

OPERATIONS MANUAL

Urbandale Police Department

“Service Built on Integrity”





Operations Manual Index

- 1.1.1 Oath of Office/ Oath of Honor/ Code of Ethics
- 1.1.3 Diversion Programs
- 1.1.4 Consular Notification & Immigration Law Compliance
- 1.2.1 Legal Authority
- 1.2.3 Constitutional Requirements
- 1.2.4 Search and Seizure/ Impound & Inventory
- 1.2.5 Arrest
- 1.2.7 Officer Discretion
- 1.2.8 Strip Searches
- 1.2.9 Unlawful or Improper Bias
- 1.2.10 Brady Disclosure Requirements
- 2.1.1 Agency Jurisdiction
- 2.1.4 Requests for National Guard Assistance
- 3.1.1 Contractual Agreements
- 4.1.1 Use of Force
- 4.3.1 Firearms
- 4.3.5 Firearms Range
- 11.1.1 Organizational Structure and Function
- 11.2.1 Accountability & Command
- 11.3.1 Authority and Responsibility
- 11.3.3 Notification to the Chief of Police
- 11.3.4 Use of Force Resulting in Serious Bodily Injury/Death
- 11.4.1 Administrative Reporting
- 11.4.2 Agency Forms
- 11.4.4 Computer Software
- 11.5.1 Temporary, Specialized, and Collateral Duty Assignments
- 12.1.2 Command Protocol
- 12.1.3 Lawful Orders
- 12.1.4 Communication, Cooperation, Coordination
- 12.2.1 Written Directive System & Issuing Authority
- 12.2.2 Operations Manual
- 12.2.3 Motto and Mission Statement
- 15.1.1 Planning and Research
- 16.3.1 Reserves
- 16.4.1 Police Chaplain
- 17.1.1 Budgeting Process
- 17.3.1 Requisition and Purchasing
- 17.4.1 Accounting
- 17.5.1 Agency Property
- 21.2.1 Classification
- 22.1.1 Compensation and Benefits
- 22.1.5 Employment Related Critical Injury or Death

22.1.6 Clothing and Equipment
22.1.6(A) Appearance Guidelines
22.1.8 Department Identification
22.1.9 Military Deployment and Reintegration
22.2.1 Physical Condition
22.2.4 Off Duty and Contracted Duty Employment
22.3.1 Collective Bargaining
22.4.1 Grievance Procedures
26.1.1 Rules and Regulations
26.1.2 Awards and Recognition
26.1.3 Sexual Misconduct
26.1.4 Disciplinary System
26.2.1 Internal Affairs
26.3.1 Complaint Procedures
31.1.1 Recruitment
31.4.1 Selection of Personnel
33.1.1 Training and Career Development
34.1.1 Promotion
35.1.1 Performance Evaluation
35.1.9 Early Intervention System
40.1.1 Crime Analysis
40.2.1 Intelligence Information
41.1.1 Patrol
41.1.3 Patrol Bicycle and Other Special Purpose Vehicles
41.1.5 Police Canine
41.2.1 Use of Emergency Vehicles
41.2.2 Vehicle Pursuits
41.2.4 First Responder Notification
41.2.5 Missing Persons
41.2.7 Response to Persons with Mental Illness
41.2.7(A) Mental Health Crisis Intervention Team
41.2.8 Alarm Response
41.3.8 In-Car & Body Worn Recording System
41.3.9 License Plate Recognition System
42.1.1 Criminal Investigation
42.2.4 Multi-Jurisdictional Investigative Task Force
42.2.5 Polygraph
42.2.6 Confidential Informants
42.2.7 Cold Case Investigation
42.2.9 Line ups and Show ups
43.1.1 Vice, Narcotics, and Organized Crime
44.1.1 Juveniles
44.2.4 School Resource Officer
45.1.1 Crime Prevention and Community Involvement
45.3.1 Volunteers
46.1.1 Critical Incidents
46.1.11 Crowd Management and Control
46.1.13 Continuity of Operation
46.2.1 Rapid and Immediate Deployment
46.2.2 Suburban Emergency Response Team

46.2.6 VIP Security
46.2.7 Special Event Planning
46.2.8 Event Deconfliction
46.2.9 Hostage/Barricade Situations
46.3.1 Terrorism
46.3.2 Hazardous Materials

46.3.5 Bomb Threats
53.1.1 Line Inspections
53.2.1 Staff Inspections
54.1.1 Public Information & Social Media
Use

55.1.1 Victim Witness Assistance

55.2.6 Emergency Notification
61.1.1 Traffic Enforcement
61.1.7 Traffic Stops
61.1.9 Operating While Intoxicated
61.2.1 Traffic Accidents
61.3.1 Traffic Direction and Control
70.1.1 Transporting Detainees
71.1.1 Processing and Temporary Detention
74.1.1 Legal Process and Arrest Warrants
74.3.1 Execution of Criminal Process

81.1.1 Communications
82.1.1 Records Administration
82.2.1 Reporting and Record Maintenance
83.1.1 Collection and Preservation of
Evidence
84.1.1 Property and Evidence Control

Tracking of paper citations
Ride Alongs
Use of Narcan
Sworn Officer Uniforms
Pink Patch Project
Notification to Area Schools
OWI Blood Draw Procedures
Patrol Division: Duty hours and breaks
Patrol Division: Hit & Run Report
Investigation Division: Work Hours
Investigation Division: Dress Code Alcohol/
Tobacco Compliance Program
Support Services: Work Hours
Support Services: Dress Code
Code of Ethics
Urbandale Map
Job Descriptions
CJIS Security Policy

Chapter 1: Law Enforcement Role, Responsibilities and Relationships

Section 1: Law Enforcement Role and Authority

Subsection 1: Law Enforcement Agency Role



Policy/Procedure #: 1

Title: Oath of Office/ Oath of Honor/ Code of Ethics

CALEA Reference#: 1.1.1, 1.1.2

I. Policy: Oath of Office/ Oath of Honor/ Code of Ethics

This policy is established to ensure all police officers for the City of Urbandale are sworn to an oath of office and an oath of honor. The policy also establishes a code of ethics to which all Department employees shall adhere.

II. Procedure: Oath of Office

- A.** All police officers of the Urbandale Police Department shall be administered the oath of office by the Mayor of the City of Urbandale.
- B.** The oath of office shall be conducted in a timely manner before an officer has assumed full duties of the position.
- C.** The signed oath of office shall be maintained in each officer's personnel file for the duration of their employment as a police officer with the City of Urbandale.

III. Procedure: Oath of Honor

- A.** A public affirmation of adhering to an oath of honor is a powerful vehicle demonstrating ethical standards. To be successful at enhancing integrity within our organization, leaders must ensure the oath is referred to frequently and displayed throughout the organization as well as ensuring ethical mentoring and role modeling are consistent and visible. The following oath of honor is recommended by the International Association of Chiefs of Police as symbolic statement of commitment to ethical behavior and shall be adopted by the Urbandale Police Department:

**On my honor, I will never betray my integrity, my character,
or the public trust.**

**I will treat all individuals with dignity and respect and that my actions
are dedicated to ensuring the safety of my community and the
preservation of human life.**

I will always have the courage to hold myself and others accountable for our actions.

I will always maintain the highest ethical standards and uphold the values of my community and the agency I serve.

- B.** Before any officer takes the oath of honor, it is important that he/she understands the meaning of the oath. An oath is a solemn pledge someone makes when he/she sincerely intends to do what he/she says.

Honor means that one's word is given as a guarantee.

Betray is defined as breaking faith with the public trust.

Integrity is being the same person in both private and public life.

Character means the qualities that distinguish an individual.

Public trust is a charge of duty imposed in faith toward those you serve.

Courage is having the strength to withstand unethical pressure, fear or danger.

Accountability means that you are answerable and responsible to your oath of office.

Community is the jurisdiction and citizens served.

- C.** Officers will acknowledge and sign the law enforcement oath of honor following an officer's oath of office. The oath of honor may be recited in unison by all Urbandale police officers present for the officer's oath of office. In addition, the oath of honor may be used but not limited to the following:

- 1.** Referred to by administrators while communicating with others.
- 2.** Placed on the back of all in-service training name cards, visible to officers throughout a training day.
- 3.** Strategically and visibly placed throughout the Urbandale Police Department.
- 4.** Signed by officers, framed and hung on the wall.
- 5.** Recited at official police ceremonies and gatherings.
- 6.** Printed on labels that are placed on equipment.
- 7.** Placed on the backside of business cards; and
- 8.** Used as a backdrop in citizens' meetings and news media events.

- D.** The signed oath of honor shall be retained by the employee.

IV. Procedure: Code of Ethics

- A.** All police officers of the Urbandale Police Department shall be informed of the code of ethics in which the Department is based. Each officer shall be required to sign their acknowledgement of and adherence to this code.
- B.** The acknowledgement of and adherence to the code of ethics shall be maintained in the Department training files for each officer.

- C.** In addition to the code of ethics for sworn officers of the Department, all employees shall be held to the code of ethics adopted by the City of Urbandale as established in the City Handbook.
- D.** At minimum, all employees of the Urbandale Police Department shall receive biennial ethics training.

Chapter 1: Law Enforcement Role, Responsibilities, and Relationships

Section 1: Law Enforcement Role and Authority

Subsection 1: Law Enforcement Agency Role



Policy/Procedure #: 3
Title: Diversion Programs
CALEA Reference#: 1.1.3

I. Diversion Programs

A policy is established to recognize the criminal justice and social service diversion programs in which the Urbandale Police Department plays an active role. All diversion type programs in which services are rendered other than pursuing a criminal charge shall be outlined to assist employees in recognition of options available.

II. Urbandale Police Department Crisis Intervention Team (CIT)

- A.** The CIT shall be comprised of a sworn police officer trained in response to individuals experiencing a mental health crisis and a mental health professional.
- B.** The CIT team shall aid persons experiencing a mental health crisis and provide the services established in Chapter 5 Section 41.2.7(A) (Crisis Intervention Team) of the Operations Manual.

III. Mobile Crisis Response Team (MCRT)

- A.** The MCRT is a social services program administered by the Polk County Health Department. The program is established to divert individuals with mental health issues to the proper service programs rather than the criminal justice system.
- B.** If an officer responds to a call where the subject is having a mental issue and the Urbandale CIT is not available, the MCRT may be called for assistance. If the subject is cooperative and would like to get help voluntarily, the MCRT may respond to the scene. Once the MCRT arrives and assess the situation, they will determine if police presence and assistance are needed. If officer assistance is no longer needed, the MCRT may relieve the officer(s).

- C. The information from the call shall be logged into the CAD; however, an officer may initiate an incident report if the situation warrants.
- D. If the subject is having a mental issue and is not cooperative and/or has shown signs to cause harm to self or others, the MCRT may be called and requested to respond to the location. MCRT will assess the situation and assist the officer with an involuntary committal if necessary or help convince the subject to submit to a voluntary evaluation.
- E. An incident report shall be filled out for any mental case where the subject is not cooperative and must be involuntarily committed.
- F. If MCRT is unable to respond to the scene, they will attempt to meet the officers at the hospital for assistance in a committal situation; however, the burden lies with the officer to take the necessary steps for an involuntary committal if warranted.

IV. Procedure: Neighborhood Mediation

- A. The Polk County Attorney's Office Neighborhood Mediation program is a voluntary, informal and confidential meeting which allows parties involved in a dispute a chance to discuss the issues and with the help of a professional mediator reach a resolution or agreement. Neighborhood Mediation is often used for neighbor or neighborhood disputes such as property line disputes, animal complaints, parking issues, etc. The goal of the program is to resolve issues before they result in criminal or civil court actions.
- B. If an officer responds to a dispute in which no criminal laws have been violated, the parties may be referred to the Neighborhood Mediation program. Officers may use discretion when referring parties to Neighborhood Mediation when there has been a violation of the law; however, both parties should be in agreement to participate in the mediation and the violation should be a minor offense. Participation in the program is strictly voluntary and neither party can be required to participate.

Chapter 1: Law Enforcement Role, Responsibility and Relationships

Section 1: Law Enforcement Role and Authority

Subsection 1: Law Enforcement Agency Role



Policy/Procedure #: 4

Title: Consular Notification and Immigration Law Compliance

CALEA Reference#: 1.1.4

I. POLICY: Consular Notification

A policy is established to ensure compliance with all United States treaty obligations on consular notification and access. The policy shall provide documentation of such notifications and access to demonstrate compliance with international treaties as prescribed by the United States Department of State. The Urbandale Police Department shall comply with federal law and guidelines established by the United States Department of State regarding the detention and arrest of Foreign Nationals as well as any state or federal law regarding immigration.

II. Definitions

- A. Arrest or Detention:** Any arrest, detention, or other commitment to custody which results in a Foreign National being incarcerated for more than a few hours triggers consular notification requirements. A brief traffic stop or an arrest resulting in a citation for a misdemeanor and release at the scene does not trigger such requirements. On the other hand, requiring a Foreign National to accompany a law enforcement officer to a place of detention may trigger the consular notification requirements, particularly if the detention lasts for a number of hours or overnight. The longer a detention continues, the more likely it is that consular notification requirements are triggered.
- B. Foreign National:** Any person who is not a U.S. citizen; same as "alien." Aliens who are lawful permanent residents in the United States and who have a resident alien registration card ("green card") are Foreign Nationals as are undocumented or "illegal" aliens.
- C. Consular Officer or Consul:** A foreign official authorized by the Department of State to provide assistance to the foreign government's citizens in the United States. Different from "counsel," which is an attorney

authorized to provide legal advice. Consuls are not authorized to practice law.

- D. Diplomat:** A foreign official at the country's embassy in Washington, D.C., assigned to represent the country. Diplomats may also perform consular functions, and should be treated the same as a consular officer.
- E. "Mandatory" Notification:** Consular notification procedures that apply when you arrest or detain a Foreign National from any of the countries that have agreed to special rules with the United States. For such a Foreign National, you must notify the consular officer regardless of whether the national requests or wants you to do so.
- F. "Upon request" notifications:** Consular notification procedures that apply when you arrest or detain a Foreign National from any country not on the "mandatory" list of countries.

III. Procedure: Consular Notification

- A.** Obligation triggered at time of booking. The notification process will begin at the time the arrested Foreign National is booked into the detention facility. The police officer who processes the arrest of the Foreign National is responsible for implementing the notification process.
- B.** Determine the Foreign National's country. In the absence of other information, assume this is the country on whose passport the Foreign National travels. Absent citizenship documentation or other evidence to the contrary, accept the Foreign National's own statement as to his or her nationality.
- C.** Determine whether or not this country is a mandatory notification ("list") country.
 - 1.** For Foreign Nationals whose country is on the list of mandatory notification countries:
 - a.** Notify the nearest consulate of the Foreign National's country via fax immediately or as soon as reasonably possible, and in no case longer than the end of the shift. Notify the consulate even if the Foreign National does not want notification. Contact information for consulates is located at:
<https://travel.state.gov/content/travel/en/consularnotification/ConsularNotificationandAccess.html>
 - b.** Inform the Foreign National that you notified his or her consulate.
 - c.** Never tell the consular officer that the Foreign National has requested asylum. If the consular officer insists on information the Foreign National does not want disclosed, contact your supervisor or the Department of State at (202) 485-7703.
 - d.** Document the notification in the case file using the Foreign National Arrest/Detention Consular Notification form and the fax confirmation sheet.

2. If the Foreign National's country is not on the list of "mandatory notification" countries, he or she is from an "upon request" country. For Foreign Nationals whose country is not on the list of mandatory notification countries:
 - a. As soon after the arrest as reasonably possible, but no later than booking, inform the Foreign National he or she may have his or her consular officers notified of the arrest or detention. Use the Foreign National Notification form. If the form is needed in a language other than English, go to:
<https://travel.state.gov/content/travel/en/consularnotification.html>
 - b. Make a note of the Foreign National's decision on the Foreign National Notification form.
 - c. If the Foreign National requests notification, notify the nearest consulate of the Foreign National's country as soon as reasonably possible but no later than 72 hours after arrest. Contact information for consulates is at:
<https://travel.state.gov/content/travel/en/consularnotification/ConsularNotificationandAccess.html>
 - d. Never tell the consular officer that the Foreign National has requested asylum. If the consular officer insists on information the Foreign National does not want disclosed, contact your supervisor or the Department of State at (202) 485-7703.
 - e. Document the notification in the case file using the Foreign National Arrest/Detention Consular Notification form and the fax confirmation sheet.

IV. Procedure: Facility Access and visitation privileges of consular officers

- A. Consular officers and diplomats visiting a detained Foreign National shall have the same access privileges as attorneys visiting a client. Consular officers and diplomats are required to adhere to the same visitation procedures as attorneys.
- B. Consular officers and diplomats must have proper identification to gain facility access. They should be carrying identification cards issued by the Department of State. If you have reason to doubt the authenticity of the identification card, call the Department at (202) 485-7703.

V. Procedure: Documentation and Record Keeping

- A. Document the offer of notification on the Foreign National Notification form. A copy of this form shall be supplied to the Foreign National.
- B. Document the consular notification on the Foreign National Arrest/Detention Consular Notification form. Make the consular notification by fax if possible, and by telephone if not. Give the Foreign National a copy of the Foreign National Arrest/ Detention Consular Notification form and fax confirmation sheet for their records.

- C. If notification must be made by telephone, note the name and location of the consulate notified, the name of the person to whom you gave the information, and the date and time of notification. Make an audio recording of the telephone call if possible and preserve it.

VI. Procedure: Death or Serious Injury of a Foreign National

- A. Standard operating procedure for death or serious injury notification shall be followed.
- B. In addition to the above procedures, when a Foreign National dies, is seriously injured, or becomes seriously ill, notify the nearest consulate of his or her country immediately or as soon as reasonably possible. Make such notification by fax if possible using the Foreign National Death/Injury/Illness Consular Notification form or by telephone if unable to fax.
- C. If notification must be made by telephone, note the name and location of the consulate notified, the name of the person to whom you gave the information, and the date and time of notification. Make an audio recording of the telephone call if possible and preserve it.

VII. PROCEDURE: Compliance with Federal and State law Relating to Immigration Laws

- A. Any lawful immigration detainer request shall be fully complied with, including any lawful instructions made in the detainer request and in any other legal document provided by a federal agency; unless compliance with such instruction will violate another duty imposed by state or federal law.
- B. All Urbandale Police Department employees shall fully comply with Chapter 27A of the Iowa Code and shall not prevent any employee from such full compliance (reference IA Code section 27A).
- C. The policies of the Urbandale Police Department shall not be interpreted to prohibit or discourage the enforcement of immigration laws (reference IA Code section 27A).
- D. No Urbandale Police Department employee or other city official shall be prohibited or discouraged from doing any of the following (reference IA Code section 27A):
 - 1. Inquiring about the immigration status of a person under a lawful detention or under arrest. Lawful detention means the detention of a person for the investigation of a public offense excluding moving traffic violations. Lawful detention excludes a detention if the sole reason for the detention is the person is a victim, witness to a public offense, or is a reporting a public offense.
 - 2. Doing any of the following with respect to information relating to the immigration status, lawful or unlawful, of any person under a lawful detention or under arrest, including information regarding the person's place of birth:

- a. Sending the information to or requesting or receiving the information from United States Citizenship and Immigration Services, United States Immigration and Customs Enforcement, or another relevant federal agency.
 - b. Maintaining the information.
 - c. Exchanging the information with other local, state, or federal governmental entities.
- 3. Assisting or cooperating with a federal immigration officer as reasonable or necessary, including providing enforcement assistance.
- 4. Permitting a federal immigration officer to enter and conduct enforcement activities at a jail or other detention facility to enforce a federal immigration law.
- 5. The Urbandale Police Department, or any person employed or under the direction or control of the Urbandale Police Department, shall not ask for or collect any information from a victim of or witness to an alleged public offense or from a person reporting an alleged public offense, including the victim's, witness's, or person's national origin, that is not pertinent to the investigation of the alleged public offense.

Chapter 1: Law Enforcement Role, Responsibilities, and Relationships

Section 1: Law Enforcement Role and Authority

Subsection 2: Limits of Authority



Policy/Procedure #: 1

Title: Legal Authority

CALEA Reference#: 1.2.1, 1.2.2

I. Policy: Legal Authority

A policy is established to define the legal authority vested in Urbandale Police Department personnel. The policy shall describe the authority vested in personnel to enforce laws and make arrests. The policy shall also state the authority of personnel to carry and use firearms.

II. Procedure: Authority to Enforce Laws and Effect Arrests

- A.** When on duty, sworn police officers of the Urbandale Police Department shall at all times, by virtue of their legally mandated authority, enforce the ordinances of the City of Urbandale and the laws of the State of Iowa relating to crimes committed within the Urbandale city limits and take appropriate enforcement action. This authority is vested in sworn police officers and is derived from Iowa State Statute 80B.3 & 804.6 and Urbandale city ordinance 30.03(10) and 33.01.
- B.** When “off duty,” officers should be prepared to act to protect life and property. Based on the circumstances they are presented with and their ability to respond, it shall be the “off duty” officers discretion whether to take action. If an “off duty” officer does take action they shall immediately be considered “on duty” and be granted the legally mandated authority to act in accordance with the policy and procedures of the Urbandale Police Department, Iowa Code and the Constitution of the United States.
- C.** Sworn reserve police officers for the Urbandale Police Department shall have the same authority as sworn police officers as provided by Iowa State Statute 80D.1A(5) and Urbandale city ordinance 33.35.
- D.** In cases where circumstances indicate that a violation of federal law has been committed, the appropriate federal agency will be notified. Sworn police officers and reserve police officers of the Urbandale Police

Department have the authority to enforce federal laws where concurrent jurisdictions exist.

- E. All officers shall perform their duties as required or directed by law, departmental rules and regulations, policies, directives or by lawful order from a supervisory officer.
- F. The United States Constitution and the State of Iowa Constitution define the scope and limits of law enforcement authority as it pertains to the enforcement of laws, statutes and ordinances.

III. Procedure: Authority to Carry and Use Weapons

- A. Iowa Statute 724.2(1), 724.4(4), and 80D.7, along with city ordinance 33.47, authorize police officers and reserve police officers to carry weapons in the performance of their duties.
- B. All Urbandale police officers and reserve police officers shall be authorized to carry and use approved weapons to perform their duties by the Chief of Police. All weapons shall be used in accordance with departmental policy and procedure and state or federal law regulating their use.

Chapter 1: Law Enforcement Role, Responsibilities, and Relationships
Section 1: Law Enforcement Role and Authority
Subsection 2: Limits of Authority



Policy/Procedure #: 3
Title: Constitutional Requirements
CALEA Reference#: 1.2.3

I. Policy: Constitutional Requirements

A policy is established by the Urbandale Police Department to make certain all employees who engage in criminal investigations or other law enforcement actions make every effort to ensure all persons are afforded the rights and protections guaranteed by the Constitution of the United States.

II. Procedure: General

- A.** All persons involved in any way with the Urbandale Police Department shall be treated fairly, without prejudice, and be extended all rights guaranteed by the United States Constitution.
- B.** Employees shall not coerce or obtain involuntary confessions from any person.
- C.** If both custody and interrogation are present as defined by a court of competent jurisdiction, an officer must advise a person of their constitutional rights according to Miranda. Officers advising a subject of their Miranda rights shall utilize one of the following procedures:
 - 1.** Miranda rights are read to the subject from a Miranda rights card issued by the Department.
 - (a)** Support Services shall issue the cards to officers as part of their equipment and replace the cards as needed.
 - (b)** Officers are required to carry the card during work hours and while appearing in court to support their testimony. Officers working administrative assignments are exempt from carrying the Miranda rights card.
 - 2.** Miranda rights are read to the subject from the Miranda rights form utilized by the Department.
 - 3.** Officers shall note in their reports when and how the Miranda rights were given.

- D. Officers shall video and/or audio record all interviews and interrogations. If an officer is unable to video and/or audio record an interview or interrogation, it is recommended another officer be present to verify any statements made by either party.
- E. Copies of all audio and video recordings of interviews and/or interrogations shall be held as evidence for the appropriate case.
- F. Except for those persons released on bond or their own recognizance, when a person is arrested with or without a warrant, the officer shall bring the arrested person before the court having jurisdiction over the offense to file the formal charge or complaint without delay.
- G. Pretrial publicity may prejudice a fair trial. All employees shall restrict the release of any information that may hinder a defendant's ability to receive a fair trial while complying with department procedures on news media relations and release of information.
- H. All persons shall be granted access to legal counsel without unnecessary delay.
- I. Officers conducting interviews or interrogations of non-English speaking persons shall ensure a competent interpreter is utilized.

III. Procedure: Field Interviews

- A. A field interview is the detainment of an individual, while on foot or in a vehicle, based on reasonable suspicion for the purpose of determining the individual's identity and resolving the officer's suspicions. It is vital officers conduct legitimate field interviews as an investigative tool as well as a crime prevention and information gathering technique. The field interview is a valuable tool in collecting, preserving and disseminating information on potential suspects or criminal activity. Officers conducting field interviews must understand the legal basis for their detainment of an individual and must be able to articulate these facts.
- B. Reasonable suspicion is articulable facts based on the totality of the circumstances that would lead an officer to believe criminal activity is being, is about to be, or has been committed.
- C. In justifying a stop, an officer must have reasonable articulable suspicion that criminal activity is afoot. This includes but is not limited to the following:
 - 1. The subject's actions indicate he is engaged in, is about to be engaged in, or has just completed some type of criminal activity.
 - 2. The hour of the day or night is inappropriate for the subject's presence in the area.
 - 3. The subject's presence in a neighborhood or location is inappropriate.
 - 4. The subject or his vehicle fits the description of a subject or vehicle wanted in connection with a crime that has occurred.
 - 5. The officer has knowledge of a subject's prior criminal history.

- 6. The subject has exhibited furtive conduct such as fleeing from the presence of an officer or attempting to conceal their person or an object from the officer's view.
- 7. The subject is in a place proximate in time and location to an alleged crime.
- D. When approaching a subject, the officer shall clearly identify himself. If not in uniform, the officer shall announce their identity and display the appropriate Urbandale Police Department identification.
- E. Officers shall remain vigilant for furtive movements to retrieve weapons, conceal or discard contraband or any other suspicious actions.
- F. Officers shall confine their questions to those concerning the subject's identity and other inquiries necessary to resolve the officers' suspicions. An officer shall only detain a subject as long as necessary to dispel or confirm their suspicions.
- G. Officers shall document all field interviews on a field intelligence report form in order to provide other officers and investigators with information concerning suspicious activities or persons.

IV. Procedure: Interview

- A. An interview is the questioning of a person who is believed to possess knowledge of official interest to the officer or investigator.
- B. Following an interview, a supplemental report shall be made as soon as possible by the interviewing officer detailing the results of the interview. This supplemental report shall be part of the case file.
- C. Interviews of juveniles shall be accomplished in a manner consistent with Urbandale Police Department policy Chapter 5 Section 44.1.1.
- D. Any person subject to an interview by the Urbandale Police Department shall be afforded all the protections guaranteed by the Constitution of the United States.

V. Procedure: Interrogation

- A. An interrogation is the questioning of persons suspected of direct or indirect involvement in a crime. The purpose of an interrogation is to obtain information which will further the investigation. Interrogation should not be simply a means of inducing an admission of guilt.
- B. Following an interrogation, a supplemental report shall be made as soon as possible by the interrogating officer detailing the contents of the interrogation. This supplemental report shall be part of the case file.
- C. Interrogation of juveniles shall be accomplished in a manner consistent with Urbandale Police Department policy Chapter 5 Section 44.1.1.
- D. Any person subject to an interrogation by the Urbandale Police Department shall be afforded all the protections guaranteed by the Constitution of the United States.

Chapter 1: Law Enforcement Role, Responsibilities, and Relationships

Section 1: Law Enforcement Role and Authority

Subsection 2: Limits of Authority



Policy/Procedure #: 4

Title: Search and Seizure/ Vehicle Impound and Inventory

Last Modified:

CALEA Reference#: 1.2.4, 61.4.3

I. POLICY: Search and Seizure

A policy is established to direct officers' actions when conducting search and seizure with and without a warrant. All search and seizure activities conducted by the Urbandale Police Department shall comply with all requirements of the Constitution of the United States and the Constitution of the State of Iowa.

II. Procedure: Search and Seizure by Warrant

- A.** Citizens shall have the right to be free from unreasonable search and seizure as afforded by the United States Constitution.
- B.** All search and seizure warrants shall be reviewed by the prosecuting attorney with jurisdiction over the matter prior to judicial review or approval.
- C.** Except in the limited occurrences when a warrant is not required, officers shall obtain a warrant to search and seize. Even when an exception to the search warrant requirement is met, officers shall strongly evaluate if obtaining a warrant would be the best course of action.
- D.** All search and seizure warrants shall be signed by a judge having jurisdiction over the matter. After service of the warrant, or if the warrant was not served, the return of service for the warrant shall be brought before a judge for review. Upon completing the return of service, the warrant shall be filed with the Clerk of Court having jurisdiction over the matter.

III. Procedure: Search and Seizure without a Warrant

- A.** Officers shall be aware of circumstances provided by federal and state law allowing an officer to search and seize without a warrant. These circumstances include but may not be limited to the following:

1. Consent searches:

- a.** Consent to search must be voluntary. At no time shall an officer coerce a person into giving consent to search.
- b.** Consent searches shall be used with the knowledge they are often subject to question after the fact, therefore obtaining consent in writing or by audio/video recording is preferred but not required. An officer obtaining a verbal consent that is not audio/video recorded shall attempt to have another officer or person witness the consent.
- c.** The scope of a consent search may be limited to specific items, areas, or times.
- d.** Withdrawal of the consent may occur at any time. At the moment the person withdraws consent, the officers shall retain any seized items they have discovered and stop the consent search. A search warrant may be required to continue the search and may include information about items already seized during the consent search.
- e.** Consent must always be obtained from a person who has authority to consent to the search.

2. Frisk or Pat Down:

- a.** An officer may make a protective, warrantless search of a person for weapons when the officer, pointing to specific and articulable facts, reasonably believes under all the circumstances the person presents a danger to the officer or to others. This search shall be limited to a "pat down" or "frisk" of the outer clothing to determine if the person is armed.
- b.** An officer who is conducting a lawful frisk for weapons and feels an item they immediately recognize as contraband or evidence may then seize the item in spite of the fact the officer knows it is not a weapon, subject to the following limitations:
 - (1)** The officer must be conducting a lawful frisk (one supported by the reasonable suspicion to believe the person has a weapon).
 - (2)** The officer's immediate recognition must amount to probable cause to believe the item is evidence or contraband.
 - (3)** The officer must immediately recognize the item as evidence or contraband without squeezing or manipulating the item.

3. Vehicle Searches:

- a.** If there is probable cause to believe evidence of a crime is in a vehicle, a warrantless search of the vehicle is allowed. This exception is allowed due to the exigent circumstances created by the mobility of the vehicle and the diminished expectation of privacy in a vehicle.

- b.** If probable cause exists to search a vehicle, all open and closed containers within the passenger compartment may also be searched.
- 4. Plain View:**
 - a.** An officer lawfully on premises may make a warrantless plain view seizure of property if it is immediately apparent to the officer the property constitutes criminal evidence.
 - b.** Except in cases involving exigent circumstances or motor vehicles, a plain view observation of contraband or evidence does not automatically justify a warrantless entry into a constitutionally protected area to seize the item.
 - c.** Officers shall be aware the search of a crime scene may require consent or a search warrant.
- 5. Exigent Circumstances:**
 - a.** Exigent circumstances make a warrantless search constitutional if probable cause exists. Exigent circumstances allow an officer to enter a structure or other area without a warrant. The situation must be one where people are in imminent danger, evidence will be destroyed, a suspect will escape, or some other consequences that will significantly hamper legitimate law enforcement efforts.
 - b.** An exigent circumstance is a situation requiring swift action. Each situation is unique and must be measured by the facts known by the officer at the time of the incident. The officer shall react based on what a reasonable officer would believe based on the facts known at the time of incident.
- B.** Officers shall be required to complete a search form when performing a search of a person, property, or vehicle based on probable cause, consent, or reasonable suspicion (stop and frisk). No later than the end of an officer's shift or assignment, the form shall be submitted to supervisor in charge. The supervisor shall review the search form to ensure proper procedures were followed. The form is not required when an arrest has occurred during the incident and the search is documented in the case reports. The form is also not required when the search has occurred due to a valid search warrant or the search is part of an on-going investigation by the Investigation Division and reason for the search is documented within supplemental reports. All search forms shall be stored on the police production server for use in the annual bias based profiling review or other supervisory reviews.

IV. Procedure: Vehicle Impound and Inventory

- A.** All vehicles impounded by the Department require a Vehicle Towing and Impound Report, a case number and a narrative account as to the circumstances surrounding the impounding of the vehicle.

- B. The decision to impound a vehicle shall be determined by the individual officer in accordance with this operating procedure. In determining if a vehicle shall be impounded, an officer shall consider the following:
 - 1. If the owner/operator wants the vehicle impounded, follow normal impound procedures.
 - 2. If the owner/operator does not want the vehicle impounded, find somewhere to park and lock the vehicle or ask the owner/operator if they wish to contact a third party to come and take possession of the vehicle. The owner/operator must grant permission before the vehicle is driven by anyone to a safe parking place or left in its current location.
- C. If a vehicle poses a traffic hazard or safety risk and cannot be moved immediately, it shall be impounded.
- D. At no time shall a vehicle be impounded solely to justify an inventory of the vehicle.
- E. If a vehicle is not impounded, an inventory of the contents is not authorized.
- F. If the officer and the owner of the vehicle are in agreement to leave the vehicle parked rather than being impounded, all control of the vehicle and the property within remains with the owner. The City of Urbandale or the Urbandale Police Department shall not be held responsible for any thefts or vandalism to the vehicle.
- G. All abandoned vehicles shall be towed directly to the designated area for storage utilized by the Department unless otherwise directed by the Support Services Division. The Urbandale Police Department shall define an abandoned vehicle as follows:
 - 1. A vehicle left unattended on public property for more than 24 hours and lacks current registration plates, or two or more wheels or other parts which renders the vehicle totally inoperable.
 - 2. A vehicle that has remained illegally on public property for more than 24 hours.
 - 3. A vehicle that has been legally impounded by the Department and has not been reclaimed for a period of 10 days.
 - 4. Any vehicle parked on the highway determined by an officer to create a hazard to other vehicle traffic.
 - 5. A vehicle that has been impounded pursuant to section 321J.4B (OWI sections) by order of the court and whose owner has not paid the impoundment fees after notification by the person or agency responsible for carrying out the impoundment order.
- H. The Department shall not impound vehicles located on private property due to abandonment. Parties requesting the removal of abandoned vehicles from private property shall be referred to a private towing service for assistance. In rare circumstances, based on a community caretaking

rationale, a supervisor may authorize impoundment of an abandoned vehicle from private property.

- I. In accordance with Iowa Code Chapter 321.89, upon impoundment of all vehicles, the register owner and all lien holders will be sent a notice of impoundment to include procedures for their vehicle's release. For any vehicles impounded by this Department, the notice shall be sent by the designated tow company after a minimum three day waiting period.
 - J. An officer who impounds a motor vehicle shall conduct an inventory of the vehicle. This shall include abandoned vehicles. The inventory shall serve to protect the owner/operator's property from theft or vandalism, protect the officer from claims of loss, damage or theft and protect the officer from any items of danger contained in the vehicle. If there are occupants of the vehicle at the time of impound, they shall be asked if there is anything of value in the vehicle they wish to retain and be allowed to do so.
 - K. Absent specific consent to search, police must inventory closed containers left behind in the vehicle as a unit (meaning you can't open suitcases, backpacks, sacks, Crown Royal bags, etc.). Officers must obtain knowing and voluntary consent before opening any closed containers. The inventory of an impounded vehicle does not include the center console, glove box or trunk area of the vehicle. If contraband is discovered during the inventory process, the officer must obtain knowing and voluntary consent or a search warrant for the vehicle before proceeding further.
 - L. An officer shall use discretion to decide when an item is of significant value that the officer believes should be removed from the impounded vehicle for safekeeping. Ask the operator whether there is anything of value requiring safekeeping and make a record of their response in order to protect the officer/department from a later claim of theft. If an item is removed from a vehicle for evidence or safekeeping, the item shall be listed on a property sheet and follow proper evidence or safekeeping procedures. All other unattached items of value contained in the vehicle shall be listed in the inventory section of the Vehicle Towing and Impound Report. Any item that is an actual part of the vehicle itself will not be considered personal property, and therefore shall not be removed from the vehicle but may be specifically noted in the inventory.
 - M. The Department shall maintain a current list of all impounded vehicles. The list shall be maintained by the Support Services Division.
- V. Procedure: Releasing Impounded Vehicles**
- A. Impounded vehicles may be released to the vehicle's registered owner upon proof of ownership, (title, registration or bill of sale) and payment of all relevant towing, storage and administrative fees. Photo identification or other proof of identity is required before the vehicle is released.
 - B. Impounded vehicles may also be released to the lien holder of the vehicle. The individual or representative of the lien holder must pay all

towing, storage, and administrative fees before the vehicle can be released.

- C. All storage fees and administrative fees collected at the police station shall be paid in cash or credit/debit card. Towing fees shall be paid directly to the designated towing company.
- D. If the impounded vehicle is stored at the towing company, the owner or lien holder shall be required to pay all fees owed to the city of Urbandale to obtain a release for the vehicle. Once all fees have been paid to the city, the owner or lien holder will be given proof of payment that must be provided to the tow company. The tow company shall be responsible for collecting their tow and storage fees from the owner or lien holder.
- E. If the impounded vehicle was classified as abandoned and is stored at the designated area for vehicle storage for the city of Urbandale, the owner or lien holder shall be required to pay all fees owed to the tow company. All fees owed to the city of Urbandale must be paid prior to releasing the vehicle. The tow company shall be responsible for collecting their tow and storage fees from the owner or lien holder.
- F. If the impound is related to an operating while intoxicated arrest, the person arrested must no longer be legally intoxicated to obtain a release for the impounded vehicle. The vehicle may be released immediately to the registered owner of the vehicle if they were not the person arrested for operating while intoxicated and are not currently intoxicated.
- G. Upon release of any impounded vehicle from police custody, the forms documenting the release shall be forwarded to the Support Services Division.
- H. Recovered stolen motor vehicles that have been impounded shall have all administrative fees owed to the department waived. If the vehicle was towed, the owner or lien holder shall be responsible for any fees owed to the tow company.
- I. Property contained in an impounded vehicle shall not be released until all fees related to the impound have been paid to the department and the tow company. Supervisors may allow exceptions on a case-by-case basis.

VI. Procedure: Abandon Vehicles

- A. Once a vehicle is impounded, the towing agency takes control of the vehicle and is responsible for all notifications, rules and regulations related to abandonment as required by Iowa Code 321.89. The towing agency shall facilitate the disposal of all abandoned vehicles. The Support Services Division shall be responsible for assisting the towing agency locate current owner information to assist in the notification process.
- B. The Support Services Division shall maintain a file of all abandoned vehicles and their disposition.

- C.** Once a vehicle is determined to be forfeited to the towing agency through the abandonment process as defined in Iowa Code 321.89, items inside the vehicle may be of significant value to warrant separate disposal through the city auction procedure. When this occurs, the item shall be placed in property/evidence until sold or converted to city use. This would not apply to small amounts of currency that would be described as loose change that has an insignificant value.

Chapter 1: Law Enforcement Role, Responsibilities and Relationships

Section 1: Law Enforcement Role and Authority

Subsection 2: Limits of Authority



Policy/Procedure #: 5

Title: Arrest

CALEA Reference#: 1.2.5, 1.2.6

I. Policy: Arrest

A policy is established to define an officer's ability to arrest with and without a warrant. The policy shall be compliant with the Constitution of the United States and the Constitution of the State of Iowa pertaining to arrest. The policy shall address when it is acceptable to exercise alternatives to arrest or continued custody.

II. Procedure: General

A. Iowa Code Chapter 804.7 states a peace officer may make an arrest under any of the following circumstances:

1. For a public offense committed or attempted in the peace officer's presence.
2. Where a public offense has in fact been committed, and the peace officer has reasonable grounds for believing that the person to be arrested has committed it.
3. Where the peace officer has reasonable grounds for believing that an indictable public offense has been committed and has reasonable grounds for believing that the person to be arrested has committed it.
4. Where the peace officer has received from the Department of Public Safety, or from any other peace officer of this state or any other state or the United States an official communication by bulletin, radio, telegraph, telephone or otherwise, informing the peace officer a warrant has been issued and is being held for the arrest of the person to be arrested on a designated charge.
5. If the peace officer has reasonable grounds for believing that domestic abuse, as defined in Iowa Code section 236.2, has occurred and has reasonable grounds for believing the person to be arrested has committed it.
6. As required by Iowa Code section 236.12 subsection 2.

B. Peace officers shall have the authority to make an arrest pursuant to subsection II (A) of this policy anywhere in the State of Iowa.

- C. Computerized warrant entries must be confirmed as valid with the originating agency prior to making an arrest.

III. Procedure: Search Incident to Arrest With or Without a Warrant

- A. All persons that have been arrested shall be thoroughly searched.
- B. The search of a person incident to arrest is permitted for the following reasons:
 - 1. To collect and preserve evidence.
 - 2. To protect the safety of the arresting officer and others.
 - 3. To prevent escape.
 - 4. To prevent weapons and contraband from entering a custodial facility.
- C. A warrantless search of a vehicle or area incident to arrest may be valid in circumstances in which the security of an arresting officer is implicated, or when the vehicle or area may reasonably be suspected to contain volatile chemicals, or when the arrested person is within reach of contraband and thus able to attempt to destroy or conceal it. Once a person is handcuffed, in control of officers, or removed from the immediate area, search incident to arrest is no longer valid.
- D. A strip search requires articulable justification and is to be completed in accordance with Chapter 1, Section 1.2.8 of the Operations Manual.
- E. A person released at the scene on a criminal signature release or traffic citation in lieu of arrest shall not be subject to search incident to arrest. The officer may be able to search the person for other reasons based on the circumstances such as a search based on probable cause.
- F. Search incident to arrest shall apply to a person who is arrested or taken into custody and later released from a detention facility on a signature release in lieu of continued custody.

IV. Procedure: Identification

- A. When taken into custody, officers shall verify the identity of a person using a variety of sources ensuring positive identification.
- B. If a person has been charged with an offense classified as a serious misdemeanor, aggravated misdemeanor, felony or any simple misdemeanor subject to an enhanced penalty for conviction of a second or subsequent offense, the person shall be fingerprinted, palm printed, and photographed prior to release. This shall include photographing other identifying features such as scars, marks and tattoos when doing so will not cause the arrested person to expose their buttock, breasts, genitals, or pubic area.
- C. Officers shall fingerprint and photograph any juvenile who has been taken into custody and charged with the commission of an offense which would be a serious misdemeanor, aggravated misdemeanor or felony if committed by an adult.
- D. Juveniles shall not be fingerprinted for a simple misdemeanor offense even if the misdemeanor is subject to enhanced penalty for a conviction of a second or subsequent offense.

V. Procedure: Reports

- A. If an adult is arrested, an incident report, an arrest report, and a detailed narrative report shall be completed.
- B. If a juvenile is taken into custody an incident report, a youth offender report and a detailed narrative report shall be completed.
- C. Regardless if an adult or juvenile has been arrested previously for a separate offense, an officer shall be required to complete all the required reports and identification procedures prescribed above as a means to accurately document the current offense and update existing records.
- D. All officers who arrest an adult for a criminal offense shall complete a preliminary complaint form or a probable cause statement depending on the jurisdiction of the prosecution. The preliminary complaint/probable cause statement shall be submitted electronically to the court having jurisdiction as soon as practical.
- E. If an adult is held for arraignment, the preliminary complaint/probable cause statement shall be delivered electronically to the courts at or near the same time custody of the person is transferred in order for the county attorney to review prior to the arraignment.
- F. If a juvenile is held for arraignment, a probable cause statement shall be delivered to the juvenile detention facility at the same time custody of the juvenile is transferred in order for the county attorney to review prior to the arraignment.
- G. If a juvenile is taken into custody and released to their parents or guardian in lieu of continued custody, the detective handling the case will be responsible for submitting a referral form if the case is referred to juvenile court.

VI. Procedure: Alternative to Arrest or Continued Custody

- A. The Urbandale Police Department shall make physical arrests when appropriate. Officers are encouraged to consider alternatives to arrest whenever possible (e.g. signature release, summonses, referral, informal resolution, and warnings) to address the variety of problems they encounter.
- B. Officers are authorized to issue a signature release in accordance with Iowa Code Chapter 805.1. Officers may release a person on a signature stating they agree to appear in court at a set time and date; however, the requirement for fingerprints, palm prints, and photographs as stated above still apply. If the arrestee meets the following criteria, they may receive a signature release in lieu of arrest or in lieu of continued custody for misdemeanor charges:
 - 1. The person can be positively identified.
 - 2. The person is a resident of Iowa.
 - 3. The person does not have an active warrant.
 - 4. The person is not charged with domestic abuse.
 - 5. The person did not use a dangerous or offensive weapon in the commission of the crime being charged.
 - 6. The person did not attempt to flee from arrest or custody.

7. The person did not resist arrest, threaten a victim, witness, or officer, and there are no reasonable grounds to believe the person will continue to commit a public offense.
8. The person does not refuse to sign a promise to appear or indicate they will not appear in court.
9. The person does not have a record of and is not currently charged with failing to appear in court or escape.
10. The offense was not committed while the person was released on bail or on their own recognizance.
11. If the person appears to be under the influence of intoxicants or drugs, a responsible person is available to take custody of the person and be responsible for the person's safety.
12. The person has sufficient ties to the jurisdiction to assure the person will appear or it reasonably appears there is a substantial likelihood the person will appear in response to a signature release.
13. Additional factors to be considered relating to the issuance of signature release when authorized shall include but not be limited to all of the following:
 - a. Place and length of residence.
 - b. Family relationships.
 - c. References.
 - d. Present and past employment.
 - e. Criminal record.
 - f. Nature and circumstances of the alleged offense.
- C. With supervisor approval, an officer may grant a signature release even if the person does not meet all of the criteria listed above. The approval and circumstances justifying the release shall be documented in a report.
- D. If a prosecuting attorney with jurisdiction over the matter has approved, a person charged with a felony may be approved for a signature release. This shall only occur in rare cases such as a serious medical condition of the offender.
- E. In the course of performing their duties, officers often encounter people in need of help more appropriately provided by another criminal justice agency, public social service agency, or private social service agency. The elderly, juveniles, alcoholics, mentally ill, substance abusers, physically sick, handicapped and transients frequently need help from resources outside of the law enforcement realm. Members of the Urbandale Police Department may, when appropriate, refer adults and juveniles to other criminal justice agencies, public social service agencies or private social service agencies within the legal parameters of state statutes. The purpose of the referral is to divert non-serious and/or social problems from the formal criminal justice system and solve individual and community problems by means of community and regional resources. Several of these programs are outlined in Chapter 1 section 1.1.3 of the Operations Manual. All referrals shall be documented.

VII. Procedure: Diplomatic Immunity

- A.** The United States Department of State issues identification documents to foreign government personnel who are entitled to immunity. Because there are different degrees of immunity, law enforcement officers should read carefully identification cards presented to them. Questions regarding an individual's status or immunity should be referred to the State Department's 24/7 Diplomatic Security Command Center at (866) 217-2089. For United Nations members call (212) 415-4444.
- B.** Any Officer having contact with a Foreign National claiming diplomatic immunity shall contact their supervisor prior to any arrest or detainment unless such arrest or detainment is necessary to prevent the loss of life or continuation of a crime. The supervisor shall make a determination as to the qualification of immunity and may by consult with the United States State Department at the phone numbers provided above.

Chapter 1: Law Enforcement Role, Responsibilities and Relationships

Section 1: Law Enforcement Role and Authority

Subsection 2: Limits of Authority



Policy/Procedure #: 7
Title: Officer Discretion
CALEA Reference#: 1.2.7

I. Policy: Discretion

A policy is established to guide officers in the use of discretion. It is unrealistic to expect officers to enforce all laws and ordinances regardless of the circumstances encountered. Instead, officers must make legal discretionary choices in arrests, issuing citations, and general enforcement to affect an equitable solution to the situation encountered. Officers shall always act in accordance with federal and state law, departmental policy, procedures, rules and regulations when employing discretion. When discretion is utilized, it must be reasonable, defensible, and accomplish a police purpose.

II. Procedure: Discretionary Process

- A.** Before officers exercise discretion, they must consider relevant factors and the overall situation. Using previously gained knowledge, training, experience, and sound judgment, the officer shall make an appropriate decision.
- B.** When utilizing discretion, officer shall consider how their actions will affect not only the situation encountered but how actions taken or not taken will affect the overall community perspective as well as general safety and order.
- C.** Officers shall be issued policy, procedures, rules and regulations and orders to define the limits of individual authority, provide guidelines for the exercise of discretion, and address actions that must be followed in certain circumstances. Discretion is based on the fact an officer is faced with a myriad of situations almost daily making it difficult for a law enforcement agency to write policies, procedures, and rules and regulations to address every conceivable situation.
- D.** The Department shall provide uniformity of decisions and action to eliminate unnecessary discretion. If the situation is beyond the officer's scope or ability, a supervisor shall be consulted on the discretionary action to be considered.

- E.** Officers shall be cognizant of laws and department policy which remove an officer's discretion and requires mandatory arrest or action be taken (e.g. domestic abuse). In these instances, officers shall comply with the applicable statute or department policy governing such situations.

Chapter 1: Law Enforcement Role, Responsibilities, and Relationships

Section 1: Law Enforcement Role and Authority

Subsection 2: Limits of Authority



Policy/Procedure #: 8
Title: Strip Searches
CALEA Reference#: 1.2.8

I. Policy: Strip Searches

A policy is established to regulate the use of strip searches. The policy shall comply with all federal and state law governing the search.

II. Procedure: Strip Search

- A.** Nothing in this policy shall restrict an officer from immediately removing a weapon from a person if the officer reasonably believes the weapon is an immediate danger to themselves or others.
- B.** A strip search is defined as requiring a person remove or arrange some or all of the person's clothing so as to permit a visual inspection or physical probe of the genitalia, buttocks, anus, female breasts or undergarments of that person or the physical probe of any body cavity.
- C.** A person arrested or detained shall not be subjected to a strip search unless there is probable cause to believe the person is concealing a weapon or contraband and written authorization of the supervisor on duty is obtained.
- D.** A strip search shall only be conducted under the following conditions:
 - 1.** Authorization of a supervisor prior to performing the search. The authorizing supervisor shall also approve the final report on the incident.
 - 2.** A search warrant supported by probable cause is obtained prior to the search.
 - 3.** A strip search of an adult in which there will only be visual inspection may be performed by an officer. A strip search in which there is a probing of any body cavity shall only be performed under sanitary conditions by a licensed physician.
 - 4.** All strip searches shall be conducted in a place where they cannot be observed by persons not conducting the search. If conducted by a physician and an officer is requested or warranted due to security

concerns, an officer of the same gender as the detainee may be present (see gender identity section below).

5. All strip searches are conducted by a person of the same sex as the detainee unless conducted by a physician (see gender identity section below).
6. When a strip search is needed involving an individual that has identified themselves as transgender or the officer is unable to determine the gender or gender identity of the individual, the following shall apply:
 - (a) Officers shall inform the individual of their right to express a preference of gender.
 - (b) Absent exigent circumstances, before performing any level of search of the individual, officers shall inform the individual of their right to request a preference of the gender of the officer that will conduct the search.
 - (c) The request and response shall be video recorded when possible and documented in the officer's report. If the request is not granted, the reason for not granting the request shall be documented.
 - (d) Absent exigent circumstances, if the individual has a preference, at least one officer of the gender requested shall conduct the search.
 - (e) If the individual does not specify a preference, at least one officer of the individual's gender expression shall conduct the search.
Example: A male officer would search an individual stating no gender preference expressing themselves as a male.
 - (f) When in doubt regarding search of a transgender individual, officer shall consult with a supervisor.
 - (g) The identified gender or the expressed gender (if failing to identify) shall be the gender utilized and applied to all processing, supervision, privacy, and separation requirements required in this or other Department policies.
- E. All strip searches of juveniles shall meet the requirements of this policy and shall only be performed by a physician regardless of the type of strip search being conducted.
- F. Subsequent to a strip search, a written report shall be prepared. The report shall contain approval of the report by the supervisor authorizing the search, the name of the person subjected to the search, the names of the person(s) conducting the search, the time, date and place of the search and a copy of the search warrant authorizing the search. The report shall also contain all facts and details that prompted the need for the search.

Chapter 1: Law Enforcement Role, Responsibilities, and Relationships

Section 1: Law Enforcement Role and Authority

Subsection 2: Limits of Authority



Policy/Procedure #: 9

Title: Unlawful Bias in Public Safety

CALEA Reference#: 1.2.9

I. Policy: Unlawful or Improper Bias

A policy is established to prohibit unlawful and improper bias by employees of the Urbandale Police Department and to provide training to agency personnel on issues related to unlawful or improper bias. The policy shall ensure employees observe, respect, and protect the constitutional rights of all persons. Law enforcement agencies shall not condone the use of any bias in enforcement programs as it may lead to violations of the constitutional rights of the citizens we serve, undermine legitimate law enforcement efforts, and lead to civil rights violations. Additionally, bias alienates citizens, fosters distrust of law enforcement by the community, invites media scrutiny, legislative action, and judicial intervention.

II. Procedure: General

- A.** Unlawful or improper bias shall be defined as the selection of individuals based solely on a common trait of a group. This includes but is not limited to race, ethnic background, gender, sexual orientation, religion, economic status, age, disability, political affiliation, national origin or cultural group.
- B.** No employee shall engage in unlawful or improper bias. The race, ethnic background, gender, sexual orientation, religion, economic status, age, disability, political affiliation, national origin, or cultural group of an individual shall not be the sole factor in determining the existence of probable cause or reasonable suspicion to take police action against an individual including custody or arrest, search or frisk, field contacts, or seizure and forfeiture of property. An individual's race, ethnic background, gender, sexual orientation, religion, economic status, age, disability, political affiliation, national origin, or cultural group alone shall not constitute probable cause or a reasonable and articulable suspicion an offense has been or is being committed so as to justify the detention of an individual or the investigatory stop of a motor vehicle. Employees must be able to articulate what constituted their reasonable suspicion or probable cause in order to support any police action.

- C. Employees shall not use any terms, language or remarks that are derogatory, tend to belittle, show contempt for or defame any individual demographic, except when necessary to include such terms, language or remarks used by another for the preparation of official reports or testimony.
- D. Employees shall not take any law enforcement action based on information from members of the public or other employees they know, or reasonably should know, under all circumstances present is the product of, or motivated by bias, based on race, ethnic background, gender, sexual orientation, religion, economic status, age, disability, political affiliation, national origin, or cultural group unless the circumstances indicate that harm is imminent or a crime has been committed.
- E. Discriminatory pretextual stops are prohibited under state and federal law and are also prohibited by this policy. Discriminatory pretextual stops are any detention of a person or a motor vehicle and its occupants for a minor violation of the law based solely on race, ethnic background, gender, sexual orientation, religion, economic status, age, disability, political affiliation, national origin or cultural group of the person(s).
- F. Employees shall attempt to reduce perceptions of bias when detaining a person. When consistent with safe practices an employee shall:
 - 1. Be courteous, polite and professional.
 - 2. Introduce one's self before asking the citizen for identification and explain to the citizen the reason for the stop as soon as practical.
 - 3. In accordance with the law, ensure the length of detention is no longer than necessary to take the appropriate action for the known or suspected offense.
 - 4. Answer any reasonable questions the citizens might have to include, if relevant, explaining options for the disposition of a traffic citation.
 - 5. When requested, provide his/her name and ID number either verbally, in writing, or on a business card.
 - 6. Offer an explanation, if it is determined reasonable suspicions were unfounded. When appropriate under the circumstances, offer an apology to the affected person.
- G. Violations of this policy shall result in disciplinary action.
- H. Supervisors shall ensure all personnel in their command are familiar with the policy requirements and are operating in compliance with the policy.
- I. Supervisors shall ensure the working environment is free of unlawful or improper bias. This oversight responsibility may include periodic inspections of body and in-car audio/video systems, traffic stop data, reports and field inspections during police/citizen interactions.
- J. Any person claiming to be aggrieved or to have witnessed unlawful or improper bias or racial profiling may file a complaint. No person shall be discouraged, intimidated, or coerced from filing such a complaint, nor shall any person be discriminated or retaliated against because he or she has filed a complaint of this nature.

III. Procedure: Reporting

- A. If an employee observes unlawful or improper bias by another employee, immediately tell the person displaying the behavior to stop. If the employee is not comfortable handling the issue, they may choose to report the incident to a supervisor rather than confronting the employee.
- B. Employees are required to promptly report any incident of unlawful or improper bias to any supervisor, commander, or the chief of police even if the employee has discussed the incident directly with the individual(s) involved.
- C. Employees shall provide the following information when reporting unlawful or improper bias:
 - 1. Date(s), time(s) and location(s) when the incident(s) took place.
 - 2. Description of each incident.
 - 3. Name(s) of anyone present during each incident.
 - 4. Anyone with whom you've discussed the incident(s).
- D. Any reports of unlawful or improper bias shall be investigated by the internal affairs unit as an internal affairs investigation as provided in the Operations Manual Chapter 3 section 26.3.1.
- E. Any employee who stops and/or reports any practice occurring in violation of this policy shall not be discriminated against in any manner for opposing such conduct, testifying, assisting or participating in any investigation, proceeding or hearing arising out of a violation of this policy.

IV. Procedure: Administrative review

- A. The Office of the Chief of Police or designee shall conduct a documented annual administrative review of agency activities with potential for bias to include but not be limited to traffic and field contacts, asset forfeiture, citizen complaints and any corrective measures taken.
- B. Annually, the internal affairs unit shall compile a statistical summary of all bias based complaints which will include the findings as to whether each case was exonerated, unfounded, substantiated, unsubstantiated. Supplemental statistical data may be obtained from other sources such as computer aided dispatch records, records management software, and TraCS.
- C. The statistical summary will be used in the documented annual administrative review for compliance with the unlawful or improper bias policy.
- D. If a pattern or significant deviation from normal activity is discovered during the review, the chief of police shall request an internal affairs investigation to determine if an employee of the department has violated the provisions of this policy or any other policies.
- E. If an employee is found in violation of this policy, the chief of police may, in addition to any disciplinary action, prescribe the following:
 - 1. Mandatory remedial or additional training designed to improve employee skills and performance.
 - 2. Informal monitoring by FTOs and/or a supervisor.
 - 3. Informal counseling by a supervisor.
 - 4. Formal counseling by a department selected psychologist.

5. Mandatory or voluntary referral to the city's Employee Assistance Program (EAP).
 6. Formal monitoring (performance improvement plan) with formal reviews and reports.
 7. Reassignment.
 8. Progressive discipline.
 9. No further action.
- F. A finding other than "no further action" shall require the division commander to provide periodic updates to the chief of police documenting employee progress.

V. Procedure: Training

- A. All employees shall receive initial training prior to assignment to full duties to recognize and prevent bias in performing their job duties. For sworn officers, initial training shall occur in the Iowa Law Enforcement Academy curriculum and the department field training program. For civilian employees, initial training shall occur during their probationary period.
- B. All employees shall receive annual refresher training on prevention of unlawful or improper bias including legal issues in order to prevent unlawful or improper bias while conducting law enforcement services which may include but will not be limited to:
1. Ethics
 2. De-escalation
 3. Motor vehicle and Terry stops
 4. Citizen contacts
 5. Probable cause and reasonable suspicion
 6. Unlawful and improper profiling

Chapter 1: Law Enforcement Role, Responsibilities, and Relationships

Section 1: Law Enforcement Role and Authority

Subsection 2: Limits of Authority



Policy/Procedure #: 10
Title: Brady Disclosure Requirements
CALEA Reference#: 42.1.6

I. Policy: Brady Disclosures

It is the policy of the Urbandale Police Department to follow Brady disclosure requirements consistent with the law. This policy provides employees with the information necessary to ensure Department personnel comply with the mandated requirements under U.S. Supreme Court decisions including *Brady v. Maryland* 373 U.S. 83 (1963) and *Giglio v. U.S.* 405 U.S. 150 (1972) and any subsequent federal and state rulings or requirements. The Department and its personnel may be subject to liability in federal and state court for failing to disclose any evidence that may be favorable to a defendant.

II. Procedure: Requirements

- A.** The Brady decision and subsequent rulings have made it a duty of all law enforcement agencies and individual personnel to:
1. Identify and provide to the prosecution any exculpatory material that would have a reasonable probability of altering the results in a trial, or any material that could reasonably mitigate the sentencing of a defendant.
 2. Provide to the prosecution any material relevant to the credibility of government witnesses, including, but not limited to police officers and other Department employees.

III. Procedure: General Provisions of Disclosure

- A.** Failure to disclose Brady information is a violation of an individual's 14th Amendment right to due process of law. All exculpatory evidence (evidence that is favorable to the accused, is material to the guilt, innocence, or punishment of the accused, and may impact the credibility of a government witness, including a police officers or other Department employees) is required to be disclosed to the appropriate prosecutor(s). Exculpatory evidence is considered material if there is a reasonable probability (probability

sufficient to undermine confidence in the outcome of the trial or sentencing of a case) that disclosure will change the outcome of a criminal proceeding. Witness impeachment material is included in the Brady disclosure requirements. There is no distinction between “impeachment evidence” and “exculpatory evidence” for Brady disclosure purposes.

- B.** The Department and all individual employees have an affirmative duty to disclose. The affirmative duty to disclose is the constitutional duty of the Department and each employee to notify the prosecutor of any Brady material. The Department and each individual employee shall exercise due diligence to ensure material of possible Brady relevance is made available to the office of the prosecutor(s) with jurisdiction over the matter.
- C.** The defense is not required to request potential Brady material. It is the Department and each individual employee’s responsibility to disclose such material as soon as reasonably possible to the prosecutor(s) with jurisdiction over the matter in time for effective use at trial. Responsibility for disclosing such material extends from indictment through the trial and sentencing process.
- D.** After disclosure, it is the prosecutor’s responsibility to establish whether material disclosed by the Department or an individual employee must be provided to the defense.
- E.** Suppression of evidence favorable to an accused violates due process when the evidence is material either to guilt or to punishment, irrespective of good or bad faith.
- F.** In general, allegations or complaints that are unfounded, unsubstantiated, or have resulted in an employee’s exoneration are not considered to be potential impeachment information and are not required to be disclosed.

IV. Procedure: Examples of Brady Material

- A.** Examples of Brady material that may be subject to disclosure include, but may not be limited to, the following:
 - 1.** Information that would directly negate the defendant’s guilt concerning any count in an indictment.
 - 2.** Information that would cast doubt on the admissibility of evidence that the government plans to offer that could be subject to a motion to suppress or exclude.
 - 3.** Any criminal record or criminal case pending against any witness whom the prosecution anticipates calling.
 - 4.** The failure of any proposed witness to make a positive identification of a defendant.
 - 5.** Information that casts doubt on the credibility or accuracy of a witness or evidence.
 - 6.** An inconsistent statement made orally or in writing by any proposed witness.
 - 7.** Statements made orally or in writing by any person that are inconsistent with any statement of a proposed government witness regarding the alleged criminal conduct of the defendant.

8. Information regarding any mental or physical impairment of any governmental witness that would cast doubt on his or her ability to testify accurately and truthfully at trial.
 9. Information that tends to diminish the degree of the defendant's culpability or the defendant's offense level under state or federal sentencing guidelines.
 10. A finding of misconduct by a Civil Service Commission that reflects on the witness's truthfulness, bias, or moral turpitude.
 11. Evidence that a proposed witness has a racial, religious, or personal bias against a defendant individually or as a member of a group.
 12. An officer's excessive use of force.
 13. An employee's untruthfulness, dishonesty, bias, or misconduct in conjunction with his or her service as a law enforcement officer or Department employee.
- B. Employee personnel files that are related to matters stated above may be provided or open to the prosecution or defense as part of a Brady disclosure as is consistent with the law.

V. Procedure: Duty to Report

- A. An employee's adherence to Department policy and rules & regulations in all matters is a requirement of their employment. Breaches of policy and rules & regulations related specifically to honesty and veracity may have direct bearing on their ability to continue serving as an employee of the Department.
- B. Employees whose history regarding integrity, honesty, credibility, veracity, and related matters have a negative bearing on their professional reputation and may be subject to Brady disclosure requirements.
- C. It is the obligation of individual employees to inform their supervisor of any elements of their employment, information contained in investigative reports, or evidence connected with a criminal indictment or trial they reasonably believe may be subject to Brady disclosure.
- D. Supervisors are equally responsible for ensuring they act with due diligence in identifying any potential Brady material connected with any criminal proceeding for which they have oversight and for bringing such material to the attention of the prosecutor in a timely manner through established reporting procedures.
- E. Employees who are knowingly and intentionally untruthful, are otherwise dishonest in the course of their employment, or use excessive force are subject to impeachment of testimony at trial. Such employees are also subject to disciplinary action up to and including termination of employment.
- F. All employees of the Department shall receive training in Brady disclosure requirements.

VI. Procedure: Unknown or Unrecognized Exculpatory Evidence

- A. If the Department becomes aware of any previously unknown or unrecognized exculpatory evidence where a person is subject to or is experiencing a significant or on-going deprivation of liberty, the Department shall thoroughly investigate any credible information that would indicate the person is innocent.

- B. Upon conclusion of the investigation, the findings and any evidence shall be submitted to the appropriate prosecuting attorney's office for review.
- C. All investigative actions including documentation of the release of the information to the prosecuting attorney's office shall be documented in the original case file and any physical evidence shall be maintained according to Department policy.

VII. Procedure: Omitted Exculpatory Evidence

- A. Claims of omitted exculpatory evidence during the original investigation shall also be thoroughly investigated. In addition to investigating the evidence presented, the Department shall also investigate and document the following:
 - 1. When was the alleged omitted exculpatory evidence received?
 - 2. Who was the officer, detective, or employee that received the information?
 - 3. If or when the information or evidence was provided to the prosecuting attorney's office.
- B. When receiving a complaint or claim of omitted exculpatory evidence, investigation into omitted evidence shall not be completed by the original investigative personnel assigned to the case.
- C. Upon conclusion of the investigation, the Investigation Division Commander or a designee appointed by the Chief of Police shall review the case to determine if there were any Department policy violations.

Chapter 1: Law Enforcement Role, Responsibilities, and Relationships
Section 2: Agency Jurisdiction and Mutual Aid
Subsection 1: Agency Jurisdiction and Mutual Aid



Policy/Procedure #: 1

Title: Agency Jurisdiction

CALEA Reference#: 2.1.1, 2.1.2

I. Policy: Agency Jurisdiction

A policy is established to clearly define the boundaries of the city of Urbandale reference police jurisdiction. The policy shall also identify and define the department's relationship with agencies having concurrent jurisdiction within the city of Urbandale.

II. Procedure: Jurisdiction

- A.** The primary area of jurisdiction for officers of the Urbandale Police Department shall be the city limits as authenticated by the city of Urbandale Engineering Department. The department shall recognize the city of Urbandale Engineering Department as the official authority for the city jurisdictional boundaries. The support service division shall be assigned as liaison with the engineering department and shall be responsible for updating jurisdictional boundaries as changes occur. A detailed official map, including jurisdictional boundaries, shall be available to officers of the department in Appendix A of the Operations Manual. Changes to the city boundaries shall be announced to officers as they become available.
- B.** The Urbandale Police Department shall provide reasonable assistance to any law enforcement agency whether municipal, state or federal who requests assistance in the investigation or enforcement of criminal laws over which the requesting agency has jurisdiction.

III. Procedure: Concurrent Jurisdiction

- A.** The department is responsible for the enforcement of Urbandale city ordinances and Iowa state statutes within the city of Urbandale. Other agencies having jurisdictional authority within the municipal boundaries of the city of Urbandale include but may not be limited to the Polk County Sheriff's Office, the Dallas County Sheriff's Office, Iowa Department of

Public Safety, Iowa Department of Natural Resources and all Federal agencies having enforcement powers by virtue of the United States Code.

- B.** It is this department's policy to offer to agencies with concurrent jurisdiction complete cooperation in the exercise of their authority within the city limits.
- C.** Effective law enforcement and investigation of criminal activity is a cooperative effort within law enforcement agencies. The Urbandale Police Department supports this effort and will fully cooperate with other agencies in the discharge of their lawful duties.
- D.** The Urbandale Police Department shall enforce the ordinances of the City of Urbandale and the laws of the State of Iowa and carry out all duties and responsibilities assigned to it by the city of Urbandale and the State of Iowa.
- E.** The Urbandale Police Department has exclusive jurisdiction and responsibility in matters concerning Urbandale city ordinances with the city boundaries.
- F.** Iowa Code 331.653 grants the Polk County Sheriff and the Dallas County Sheriff general law enforcement authority throughout Polk County and Dallas County respectively including the city of Urbandale.
- G.** Iowa Code 80.9 grants the Iowa Department of Public Safety general law enforcement authority throughout the State of Iowa including the city of Urbandale.
- H.** Iowa Code 455A.2 grants the Iowa Department of Natural Resources primary responsibility for state parks and forests, protecting the environment and managing fish, wildlife and land and water resources in the State of Iowa including the city of Urbandale.
- I.** In any situation where a question concerning jurisdictional authority with Urbandale is made, the responding officer will make every attempt to resolve the matter in the most professional manner possible. If resolution is not possible, the matter will be turned over to a supervisor for resolution. At no time shall public safety be jeopardized by the Urbandale Police Department due to a jurisdictional dispute.

Chapter 1: Law Enforcement Role, Responsibilities, and Relationships
Section 2: Agency Jurisdiction and Mutual Aid
Subsection 1: Agency Jurisdiction and Mutual Aid



Policy/Procedure #: 4

Title: Requests for National Guard Assistance

CALEA Reference#: 2.1.4

I. Policy: National Guard Assistance

A policy is established to inform officers of the process to request assistance from the Iowa National Guard during emergency situations.

II. Procedure: Requests for National Guard Assistance

- A.** In dealing with emergency situations, all officers shall be aware of state and local laws which give additional powers to government officials.
- B.** During a major emergency or incident, the shift supervisor shall notify the chain of command. The chief of police shall determine if the city manager needs to be notified. If the city manager is notified, the chief of police and the city manager shall make a decision on contacting the mayor.
- C.** The mayor shall have the following powers and duties during a time of emergency or when public danger exists in which the peace and order of the city is endangered and additional protection of life and property is necessary.

Urbandale City Ordinance 31.002 (B), Iowa Code 372.14(2)

"The mayor may take command of the police and govern the city by proclamation when a time of emergency or public danger exists. Within the city limits, he has all the powers conferred upon the sheriff to suppress disorders."

- D.** Iowa Code enables the governor to mobilize the Iowa National Guard to assist local law enforcement agencies during disasters or civil disturbances. This is generally at the request for assistance from the civil authorities.

Iowa Code 29A.7(1)

"The governor is the commander in chief of the military forces, except when they are in federal service. The governor may employ the military forces of the state for the defense of the state, to provide assistance to

civil authorities in emergencies resulting from disasters or public disorders as defined in section 29C.2 including homeland security and defense duties, and for parades and ceremonies of a civic nature.”

- E. Based on the powers of the mayor during emergency situations and the authority of the governor of the state of Iowa as the Commander in chief of the Iowa National Guard, the mayor of the city of Urbandale may request assistance from the governor of the state of Iowa to activate the Iowa National Guard during emergency situations.
- F. Although the mayor of the city of Urbandale may request assistance directly from the governor, the city of Urbandale shall normally follow the procedure established in the city’s Multi-Hazard Emergency Operations Plan. The plan establishes the following protocol:

Administration and Logistics

The EP Coordinator (Urbandale fire chief) or his/her designee may request support through the county emergency management coordinator.

The coordinator coordinates the request with the state emergency management division. The division then requests a governor's proclamation of Disaster to activate state resources. City/town and county resources must be exhausted before a governor's proclamation of disaster can be requested.

Support from federal and state agencies may be requested through the county emergency management coordinator. The coordinator coordinates the request with the state emergency management division. The division then requests a governor's proclamation of disaster to activate state resources. If local and state resources are exhausted, the governor may request a presidential declaration to activate federal resources.

State agencies and local government emergency responsibilities and support functions are described in the Iowa Emergency Plan. This plan is available in the county emergency management coordinators office.

Chapter 1: Law Enforcement Role, Responsibilities, and Relationships
Section 3: Contractual Agreements for Law Enforcement Services
Subsection 1: Contractual Agreements



Policy/Procedure #: 1

Title: Written Contractual Agreements

CALEA Reference#: 3.1.1, 3.1.2

I. Policy: Written Contractual Agreements

A policy is established to guide the Department when agreements are made between the Urbandale Police Department and other entities for law enforcement services in which a fee is paid.

II. Procedure: Written Contractual Agreements

A. All written contractual agreements will contain the following:

1. A statement of the specific services to be provided;
2. Specific language dealing with financial agreements between the parties;
3. Specification of the records to be maintained concerning the performance of services by the department;
4. Language dealing with the duration, modification, renewal and termination of the written contractual agreement;
5. Specific language dealing with legal contingencies;
6. Stipulation the Urbandale Police Department maintains complete managerial control over department personnel;
7. Specific arrangements for the use of equipment and facilities; and
8. If needed, a procedure for review and revision of the agreement.

B. The Urbandale Police Department guarantees the rights of all its employees who might be assigned under written contractual agreements for law enforcement services; this guarantee will not be abridged by the Department. The Department will honor all written contractual agreements which cover all personnel of the Urbandale Police Department.

C. The Department will not penalize or threaten the employment rights of any employee for participating in any written contractual agreement for law enforcement services authorized by the Department. The Department will honor all union and non-union agreements. This guarantee will extend to promotional opportunities, training opportunities, and other benefits.

Chapter 1: Law Enforcement Role, Responsibilities, and Relationships

Section 4: Use of Force

Subsection 1: Use of Force



Policy/Procedure #: 1

Title: Use of Force

CALEA Reference#: 1.2.10, 4.1.1, 4.1.2, 4.1.3, 4.1.4, 4.1.5, 4.1.6, 4.1.7, 4.2.1, 4.2.2, 4.2.3, 4.2.4, 4.2.5, 4.3.3, 4.3.4

I. Policy: Use of Force

A policy is established to govern the use of force and direct the review of incidents in which force is used. The policy shall clarify when deadly force may be used as well as less lethal use of force. The priority and mission of the Urbandale Police Department is to protect and serve all individuals by preserving life, minimizing harm, and utilizing force only when necessary and only to the degree required.

II. Procedure: General

- A.** Officers from the Urbandale Police Department shall only use reasonable force to accomplish a lawful objective such as overcoming resistance from a person being taken into custody, to stop an assault of a third person, in self-defense, or as reasonable and necessary to perform other police functions. Officers shall not hesitate or fail to use reasonable force when it is clearly necessary.
- B.** Iowa Code 704.1 defines "Reasonable Force" as follows: "Reasonable force" is that force and no more which a reasonable person, in like circumstances, would judge to be necessary to prevent an injury or loss and can include deadly force if it is reasonable to believe that such force is necessary to avoid injury or risk to one's life or safety or the life or safety of another, or it is reasonable to believe that such force is necessary to resist a like force or threat. Reasonable force, including deadly force, may be used even if an alternative course of action is available if the alternative entails a risk to life or safety, or the life or safety of a third party, or requires one to abandon or retreat from one's dwelling or place of business or employment.
- C.** Officers shall only use force when other viable options are exhausted or not practical. Below are options that may be available to an officer based on the totality of the circumstances encountered:
 - 1.** De-escalation by talking to the individual and attempting to gain their cooperation through calm measured communication. Officer shall

employ effective communication techniques to engage with individuals who are not compliant with orders by establishing rapport, using the appropriate tone, asking questions and providing advice to defuse conflict and achieve compliance.

2. Placing barriers between the subject and the responding officers.
 3. Containing the subject where they cannot harm officers or others.
 4. Moving to a position of safety offering cover, concealment, and distance to react while still controlling the situation.
 5. Continued communication from a safe position to gain the subjects compliance through verbal persuasion, advisements, and warnings.
 6. Avoiding physical confrontation unless necessary.
 7. Requesting additional resources such as additional officers, less lethal weapons, or mobile crisis (if safe and appropriate to do so).
- D. When able, officers shall determine whether an individual's failure to comply with an order is the result of one of the following factors and adapt or adjust the need for force or the type of force based on this information:
1. Suffering from a medical condition.
 2. Mental impairment.
 3. Developmental disability.
 4. Physical limitations
 5. Language barrier.
 6. Drug or alcohol interactions.
 7. Behavioral crisis
 8. Other factors that may be beyond the control of the individual.
- E. When an employee or reserve officer reasonably believes another Department employee, reserve officer, or any other employee of a public safety agency is using excessive force, the employee or reserve officer must intervene within their scope of authority and training to immediately stop the force and render or obtain appropriate medical assistance as needed. The witnessing employee or reserve officer must report the incident to a supervisor as soon as possible. Any complaint of excessive force including those reported by another employee shall be investigated as an internal affairs complaint and follow the procedures outlined in Chapter 6 Section 52.2.1 (Complaint Procedure) of the Operations Manual.
- F. Force shall not be used on an individual for disrespect, rudeness, cursing, or similar verbal or attitude type situations where the individual does not pose a threat to the safety of the officers or others.
- G. Any use of force by an officer shall be reported to a supervisor immediately or as soon as practical.

III. Procedure: Less Lethal Weapons

- A. Prior to authorization to carry or use a firearm or any less lethal option, an officer shall receive a copy of and instruction in the Use of Force policy. The issuance and receipt of the policy and any instruction received shall be documented.

- B.** Prior to authorization, officers shall be required to pass a proficiency test to carry a firearm or a less lethal option in an official capacity. The proficiency tests shall be developed by the Range Administrator or designee and shall conform to all state and/or federal requirements. The proficiency tests must be administered annually for each type of firearm. Except for striking instruments, instruction in the use along with practical application and proficiency testing of less lethal options shall also occur annually. Instruction in use along with practical application of striking instruments shall occur biennially (once every two years). The test must be defensible and commonly accepted in the field of law enforcement.
- C.** All less lethal training and proficiency testing shall be documented by the instructor. Copies shall be placed in the training file of each officer.
- D.** Less lethal options remedial training shall be provided to any officer identified as being deficient in a specific qualification area. Remedial training is personalized training to correct a specific deficiency identified by proficiency testing, other evaluation processes, training, or routine job performance. Remedial training for an officer may be requested by any instructor or a supervisor.
- E.** Less lethal options remedial training shall be required for any officer unable to pass proficiency testing after three (3) attempts. The remedial training shall be customized to correct the deficiencies observed by the instructor. Remedial training shall not occur on the same day as the proficiency training. A remedial training plan along with documentation of actual training shall be logged by the instructor with copies being placed in the training file of the officer.
- F.** If remedial training is needed for any less lethal option, it shall be completed within five (5) working days. If unable to pass proficiency testing after the remedial training, the Chief of Police shall determine if the officer will be assigned to restricted duties. If restrictions are implemented, they shall remain in effect until proficiency is obtained. Furthermore, it is the responsibility of all instructors to inform the Support Services Division as soon as practical of any officer's failure to pass proficiency testing within the guidelines listed in this policy.

IV. Procedure: Use of Force Paradigm

- A.** Officers shall follow the principals of the Force Management Paradigm Model. The Force Management Paradigm Model describes an escalation or de-escalation of force based on the level of threat or resistance. The more resistance a subject offers, the more force options are available to the officer. When the resistance stops, the officer must de-escalate while maintaining control. In all cases, control of an individual or situation is a perception based on reasonable force as defined in this policy.
- B.** Officers do not have to enter the paradigm at the lowest possible level. They may enter anywhere to end the threat or to control the subject. Their decisions to use a type or level of force shall be based on reasonable force as defined above.

- C. Paradigm Model: The use of force may be utilized at six general levels.
1. Presence/Appearance: An officer's presence may cause the person to change their behavior or submit to the officer. This reflects the officer's demeanor, attitude, and the legal right to be present.
 2. Voice/Tactical Communication Skills: This requires a show of authority by communication with verbal and nonverbal dialogue. The person must be informed of what is required and given a chance to comply. Nonverbal dialogue includes assuming empty hand defensive position as well as the display of a defensive weapon. Using one's voice and demeanor is paramount in de-escalation. Officers shall work towards diffusing and deescalating a situation utilizing communication skills to gain compliance from an individual while remaining tactically sound and able to respond as the need arises.
 3. Hands on Techniques: When the subject fails to respond to verbal direction or resists in a passive, defensive or aggressive manner, the officer seeks compliance by the use of physical force. This could include empty hand control, pressure compliance holds, blocking, restraining, controlling or escorting holds. When the above listed techniques are ineffective or the person becomes more aggressive, the officer may seek compliance by additional physical means. This could include strikes, kicks, stuns, or takedowns.
 4. Neutralizing Agents: This level directs the use of more aggressive techniques as well as using defensive weapons against the person's resistance. This includes chemical deterrents and less-lethal electronic control devices. The person has become an aggressor, threatens to attack, attacks, or there is fear for the safety of the officer(s) or others. Lower level techniques have been exhausted or may be ineffective.
 5. Impact Weapons: This level directs the use of more aggressive techniques as well as other defensive weapons against the person's resistance. Situations may include multiple aggressors, a person armed with clubs, chains, rocks, bottles or an unarmed subject which cannot be controlled by other means. The officer may respond with non-lethal or lethal force, depending on the situation. In an urgent situation, it is possible for many things to be used as an impact weapon. A striking instrument, extended range impact weapon and the electronic control device (E.C.D) are among impact weapons provided by the department that can be used for this purpose. Any object used to exert physical force upon a person must be justified and conform to the force paradigm.
 6. Deadly Force: The final level allows the use of additional tactics or tools against persons armed with any deadly weapon or any person capable of inflicting serious physical injury or death. This level allows for the reasonable use of less lethal and lethal force options.



V. Procedure: Deadly Force

- A.** An officer may use deadly force only when the officer reasonably believes the action is in the defense of human life, including the officer's own life, or in defense of any person in imminent danger of death or serious physical injury.
- B.** Deadly force is defined as any force which is likely to cause death or serious physical injury.
- C.** Serious physical injury is defined as a disabling mental illness or bodily injury which creates a substantial risk of death, causes serious permanent disfigurement, or causes protracted loss or impairment of the function of the bodily member or organ.
- D.** Reasonable belief is a belief that would cause others under similar circumstances to act or think in a similar way.
- E.** Imminent is defined as likely to occur at any moment.
- F.** Deadly force is only justified when a person cannot be captured any other way and either:
 - 1.** The person has used or threatened to use deadly force in committing a felony and they continue to be an imminent threat to use deadly force; or,
 - 2.** The officer reasonably believes the person would use deadly force against any person unless immediately apprehended.
 - 3.** An officer making an arrest pursuant to an invalid warrant is justified in the use of any force which the officer would be justified in using if the warrant were valid, unless the officer knows that the warrant is invalid.

- G. Due to the potential for unintended serious injury or death, the discharge of a firearm for the purpose of a warning shall be prohibited.
- H. A vascular neck restriction is a technique which causes a temporary disruption of blood flow to the brain causing incapacitation. Vascular neck restrictions are prohibited by the Department.
- I. A chokehold or stranglehold are general terms for techniques that critically reduce or prevent an individual from breathing and may also restrict blood flow through the neck. Officers are prohibited from utilizing any type of technique that critically reduces or prevents an individual from breathing and may also restrict blood flow through the neck to include a chokehold or stranglehold on a subject unless it is a measure of last resort in a situation warranting the use of deadly force. Only in extremely extraordinary circumstances may a technique that critically reduces or prevents an individual from breathing and may also restrict blood flow through the neck including a chokehold or stranglehold be used as an immediate measure of defense of life. An "immediate measure of defense of life" is defined as taking action or using any implements to defend the officer's life or safety of another with actions or implements not normally intended to be used to control a person.
- J. Techniques that critically reduces or prevents an individual from breathing and may also restrict blood flow through the neck including chokeholds and strangleholds shall not be taught as part of the defensive tactics training curriculum for the Department.
- K. When using physical force to control a subject, officers shall not place their body weight on a subject's neck unless deadly force as outlined above is justified.
- L. An officer shall not use deadly force to prevent an individual from self-harm where the individual does not pose an immediate threat to the officer or another person rising to the level that would justify the use of deadly force as outlined above.
- M. Department policy on use of force and the use of deadly force shall be reviewed annually during in-service or similar training including a review of terms used to determine when deadly force is justified.
- N. The Chief of Police may request assistance from outside law enforcement agencies to assist or lead an investigation into any use of force incident in which a person or an officer has suffered fatal injuries or serious physical injuries.

VI. Procedure: Vehicles

- A. Except under the following circumstances, discharging a firearm from or at a moving vehicle is prohibited:
 - 1. When an occupant of the fleeing vehicle is utilizing deadly force against the police officer or other persons.
 - a. In almost every situation officers shall stay out of or move out of the path of a moving vehicle. Officers shall not place themselves in the path of a vehicle thereby creating a risk of being struck by the vehicle unless it is a means of last resort to save a passenger in the

vehicle from imminent death or serious physical injury (e.g. victim being kidnapped).

- b. Moving into or remaining in the path of motor vehicle when time allows the ability to move to safety shall not be justification for using deadly force unless it is a means of last resort to save a passenger in the vehicle from imminent death or serious physical injury (e.g. victim being kidnapped).
- 2. As a last resort to prevent death or substantial harm to the officer or other persons.
- 3. As a last resort to apprehend a person who has just committed a felony resulting in death or serious physical injury and if not immediately apprehended poses an imminent threat to cause death or serious physical injury to others.
- B. The discharge of firearms at or from a vehicle that meets the above exceptions shall not be utilized when the circumstances do not provide a high probability of striking the intended target or when there is a substantial risk to the safety of other persons.
- C. Officer shall not discharge a firearm at any part of a vehicle in an attempt to disable the vehicle.

VII. Procedure: Less Lethal Options

- A. While in the performance of their duties, the Urbandale Police Department allows officers to use less-lethal options to ensure their safety, the safety of the public, and the safe control of hostile or resistive persons when lethal force may not be warranted. Only officers who have completed the prescribed course of instruction and training on the use of less lethal options and have demonstrated proficiency are authorized to use such options. Instruction shall contain a review of the use of force policies, procedures, current lawful application, and ensure the administering of proper medical aid after use. Except for striking instruments, instruction in the use along with practical application of less lethal options shall occur annually. Instruction in use along with practical application of striking instruments shall occur biennially (once every two years).
- B. Officers shall only carry/use less lethal options authorized by the Department. No additions or modifications to approved less lethal option shall be permitted.
- C. The Chief of Police shall authorize the types of less lethal options carried by the Department.
- D. All less lethal options shall be logged with the Department and inspected at least annually for proper functioning and damage. The Range Administrator or designee shall maintain the log of all less lethal options including any repairs or maintenance.
- E. If a less lethal option is deemed in need of repair, it shall be taken out of service until functioning properly. If not repairable, it shall be removed from service.
- F. **Chemical Deterrent:**

1. Approved chemical deterrent for the Department shall be Combined Tactical Systems (CTS) Model MK-4 with stream delivery at 11% oleoresin capsicum.
2. Chemical deterrent may be used against a person only when an officer reasonably believes such use is necessary to protect himself/herself or others from physical harm, prevent escape or disperse persons from an area where injury, destruction of property, or other unlawful acts are occurring.
3. Chemical deterrent may have a diminished effect on animals and people under the influence of alcohol or drugs.
4. Extreme caution must be exercised in dangerous situations where the user of chemical deterrent is under attack with firearms, knives, fists or other means of violence. In such situations, chemical deterrent may not stop the attack and the user is cautioned to employ other available means to stop the attack or retreat to a point of safety.
5. Officers shall only use enough chemical deterrents to bring a person under control.
6. Supervisors or designees are authorized to use chemical deterrent to suppress and disperse a crowd engaged in violent or illegal behavior when appropriate.
7. Chemical deterrent shall not be discharged in the vicinity of infants, elderly or the infirmed. The irritant may cause physical damage since their respiratory systems may be sensitive to vapors, etc.
8. Chemical deterrent shall not be discharged into the wind or when innocent bystanders will be affected unless authorized by a supervisor to disperse a crowd engaged in violent or illegal behavior.
9. The discharge of chemical deterrent shall be directed into the face toward the eyes, nose, and mouth. Distances of less than three feet shall be avoided unless the situation is one which presents an extreme hazard such as the immediate threat of physical harm to an officer or other person.
10. Officers shall not leave or hold a sprayed person (or any person) face down or restrict their ability to breath in any way after the person is restrained and under control.
11. Persons coming in contact with chemical deterrent shall be given an opportunity to wash the areas of their body exposed to the chemical as soon as practical.
12. Contaminated areas shall be flushed with copious amounts of cold water and exposed to fresh air as soon as possible.
13. Officers shall closely monitor the person for signs of respiratory distress. If respiratory distress is observed, immediate medical attention is required.
14. Chemical deterrent shall be carried by all officers working patrol duty or any other duty requiring a uniform.
15. Chemical deterrent shall be carried by investigators when engaged in enforcement activity.

16. Command staff and other administrative assignments not engaged in enforcement activity may choose not to carry chemical deterrent.
17. If the canister of chemical deterrent is depleted or substantially depleted, it shall be replaced as soon as possible by range personnel.
18. A variety of chemical munitions to include smoke, oleoresin capsicum, CS gas, rigid surface (glass, etc.) penetration or a combination of these munitions are authorized for use by trained personnel for specific circumstances such as crowd control/dispersion, barricaded subject, or concealment. The munitions may be deployed by hand or through the 40mm single launcher by trained personnel. Authorized and properly trained SERT personnel may also deploy the munitions with the SERT 40mm multi-launcher. The below list indicates the type of device and if the munition is authorized for officer use or restricted to SERT use only:

Manufacture	Model	Type	Authorized Use
CTS	5430/5440	Flameless CS Gas (Hand deployed)	Officer/SERT
CTS	4340/4330	40mm Liquid Barricade (OC & CS)	SERT Only
CTS	9594	Sting Ball Grenade (OC)	SERT Only
CTS	1441	Pepper Spray	Officer/SERT
CTS	5211	White Smoke Grenade (Triple Phaser)	SERT Only
CTS	5231	CS Smoke Grenade (Triple Phaser)	SERT Only
CTS	5210	White Smoke Grenade	SERT Only
CTS	5230	CS Canister Grenade	SERT Only
CTS	6210	White Smoke Grenade	SERT Only
CTS	6330	CS Vapor Grenade (Indoor)	SERT Only
CTS	6340	OC Vapor Grenade (Indoor)	SERT Only
CTS	4441	40mm OC Powder	SERT Only
CTS	4213	40mm Multi Smoke 4.8"	SERT Only
CTS	4233	40mm Multi 2 (CS)	SERT Only
CTS	4556	40mm Frangible Impact O.C. powder	SERT Only
CTS	4530	40mm Frangible Impact C.S. powder	SERT Only
CTS	6231	CS Smoke	SERT Only
CTS	6343	OC/CS Aerosol Grenade (Indoor)	SERT Only
Def Tech	1083	HC Smoke	SERT Only
Def Tech	MK9	Pepper Spray (Fogger)	Officer/SERT
CTS	6210G	Green Smoke Grenade (field searches/landing zone marking)	SERT Only

G. PepperBall launching system:

1. The PepperBall launching system is a less lethal force alternative that utilizes compressed air to deliver a non-pyrotechnic plastic projectile containing chemical deterrent. The approved delivery system for the chemical deterrent projectiles for use by Urbandale Police Department personnel is the PepperBall FTC launcher. SERT personnel may also utilize the PepperBall VKS launcher utilized by other SERT agencies after receiving proper training and certification.
2. The below list is the only approved PepperBall projectiles to be utilized by the Urbandale Police Department.

Manufacture	Model	Type	Authorized Use
PepperBall	Live-X	Round 5% PAVA Powder (red/black)	Officer/SERT
PepperBall	Inert	Round Inert powder training round (purple/white)	Officer/SERT
PepperBall	VKS Live-X	Shaped 5% PAVA Powder (red/black)	SERT
PepperBall	VKS Inert	Shaped Inert powder training round (purple)	SERT

3. Officers using the PepperBall launching system shall comply with all limits and stipulations provided in training and certification.
4. The PepperBall launching system may be utilized as a chemical deterrent or as a combination chemical deterrent and light impact weapon.
5. Use of the PepperBall launching system as a chemical deterrent shall be classified at the same level on the use of force continuum as Oleoresin Capsicum.
6. Use of the PepperBall launching system as a combination chemical deterrent and a light impact weapon shall be classified at the same level on the use of force continuum as empty hand techniques "Hard".
7. The PepperBall launching system is not intended to cause death or serious physical injury.
8. Justification for use of the PepperBall launching system:
 - a. In situations in which a person appears to be a danger to himself/herself or others.
 - b. To control a dangerous or violent person when deadly force does not appear to be justified and/or necessary.
 - c. When other attempts to control or subdue the person by conventional tactics have been or likely will be ineffective.
9. The PepperBall launching system shall not be used on persons who are passively resisting or who are not posing a threat to persons/property to include persons fleeing the scene.

- 10.** The PepperBall launching system may be utilized as a chemical deterrent for ground or area saturation in the following situations:
 - a.** When it is unsafe for an officer to approach a subject within contact range, or,
 - b.** When higher use of force options may be justified, but an opportunity exists for the use of PepperBall launching system saturation before other options are employed.
 - c.** Saturation to disperse unruly or rioting crowds threatening unlawful property damage or physical force. With PepperBall launching system usage, the primary target area when encountering crowds will be the ground. If ground saturation is determined not to be a viable option, or has proven to be ineffective, the wall, building or other fixed object behind or adjacent to a crowd may be considered as a secondary target area; however, if an officer decides to fire projectiles at a wall area or fixed object behind or adjacent to a crowd, the officer must ensure the projectiles are fired well above the heads of individuals in the crowd. In saturation deployment, officers must ensure that the rounds do not make direct contact hits with any of the persons involved.
 - d.** Inside a building, after verbal warning, if a person refuses to comply with a lawful order, and/or the person takes an aggressive posture (e.g. clenched, fists, fight stance, etc.,).
 - e.** In addition, the PepperBall launching system may be used for area saturation when:
 - (1) Deemed necessary to effect the arrest (officer and/or citizen safety)
 - (2) The use will prevent the escalation of violence of a person(s) against another or;
 - (3) When use will avoid escalation of force, or,
 - (4) To stop or subdue an animal that is aggressive.
- 11.** The PepperBall launching system may be utilized as a chemical deterrent and a light impact weapon utilizing direct contact hits in the following situations:
 - a.** When a subject exhibits violent behavior that threatens the safety of self and/or others (Note: Officers must be able to articulate the violent behavior and the perceived threat to self or others).
 - b.** Officers may utilize direct contact strikes with the projectiles on subject(s) involved active aggression. Active aggression includes assault on officers or others and/or the destruction of property.
 - c.** Officers may only utilize the PepperBall launching system for direct contact hits when meeting the criteria outlined above and when they are sure of their target and background. Deploying the PepperBall launching system projectiles into a crowd indiscriminately with the intent for direct contact hits to non-specific members of the crowd is prohibited. If a crowd creates an immediate danger of injury to persons or damage to property, a

supervisor may authorize the deployment of other less lethal tools, such as indirect saturation deployment of PepperBall Launching system projectiles, OC Spray, CS gas, or other chemical agents.

12. The PepperBall launching system shall never be used to intentionally target the head, neck, face, eyes, and spine unless deadly force is justified. Under no circumstances will the PepperBall launching system be applied after resistance has ceased.
13. The maximum distance for PepperBall launching system deployment shall be 150 feet for saturation deployment and 60 feet for light impact deployment.
14. The PepperBall launching system shall not be discharged in the vicinity of infants, elderly or the infirmed. The irritant may cause physical damage since their respiratory systems may be sensitive to the powdered deterrent.
15. Officers electing to use the PepperBall launching system to disable a potentially violent suspect should do so with at least one additional officer at the scene other than the officer deploying the PepperBall launching system. The backup officer shall be safely positioned to monitor the actions of the officer and the suspect and be prepared to respond with alternative force options to include deadly force if necessary.
16. Persons that receive direct contact hits of PepperBall launching system projectiles shall be treated and evaluated by EMS personnel or transported to a medical facility for treatment and evaluation.
17. Persons exposed to the chemical deterrent of the PepperBall launching system through a direct contact hit or through area saturation shall receive the following care:
 - a. The exposed person shall not be left or held face down or restrict their ability to breath in any way after the person is restrained and under control.
 - b. Persons coming in contact with chemical deterrent shall be given an opportunity to wash the areas of their body exposed to the chemical as soon as practical.
 - c. Contaminated areas shall be flushed with copious amounts of cold water and exposed to fresh air as soon as possible.
 - d. Officers shall closely monitor the person for signs of respiratory distress. If respiratory distress is observed, immediate medical attention is required.
18. PepperBall launching system shall not be used for any of the following:
 - a. Coercion of any type.
 - b. Escorting or prodding individuals.
 - c. Waking unconscious or intoxicated individuals.
 - d. Individuals operating a moving motor vehicle; however, the PepperBall launching system may be used on subjects within a vehicle when the vehicle is immobilized or the vehicle is parked and the driver is not actively attempting to operate the vehicle.

- e. Horseplay or practical jokes.
 - f. Subjects on elevated platforms, or where immediate immobilization of the subject will cause death or serious bodily injury.
- 19.** Prior to firing the PepperBall launching system, when possible and practical, the officer should give loud verbal commands to the targeted suspect ordering him to comply with the officer's instructions. Other officers on the scene must be made aware of the use of the PepperBall launching system to ensure officers do not mistake the sound of the PepperBall launching system as gunfire causing officers to fire their weapons.
- 20.** When deploying the PepperBall launching system officers shall consider environmental effects such as wind and rain and be aware of accidental contamination of other officers and bystanders.
- 21.** Deploying officers must always be aware of their target and background and are responsible for every round fired. A use of force incident with the PepperBall launching system may require 1 to 6 PepperBall projectiles. After each use of force application, officers shall reassess the effectiveness and gauge compliance. Officers may need to utilize alternate target areas compliant with this policy or other force options should compliance not be achieved. Each use of force incident utilizing the PepperBall launching system must be justified and documented.
- 22.** Certified instructors for the PepperBall launching system will have the following responsibilities:
- a. Ensure the PepperBall launching system is set to proper operating standards as provided by PepperBall. Officers shall not alter, adjust, or modify the PepperBall launching system in such a way as to change the pressure, the velocity of the rounds, or the basic design of the launcher.
 - b. Documented annual inspection of the launchers to ensure they are maintained in a state of operational readiness. NOTE: Before doing any cleaning or maintenance, remove the air bottle from the launcher system.
 - c. Documented annual visual inspection and hydrostatic testing every 5 years of the high-pressure air tank utilized to refill the PepperBall launching system air bottle. The high-pressure air tank will be secured in the armory to prevent accidental damage or rupture from falling.
- 23.** Prior to being deployed for use in the Patrol Division, the PepperBall launching system shall be inspected by one of the certified PepperBall launching system instructors. The instructor shall ensure proper functioning and verify the PepperBall Live-X projectiles are deployed with the weapon. The PepperBall launching system shall be stored with the bolt forward, magazine tube empty, and the safety "on". The PepperBall launching system shall be loaded, used, and rendered safe

in accordance with the procedures outlined in the PepperBall training course.

24. Upon completion of the inspection, the instructor shall place the weapon in its case and place a seal on the case. The case shall not be able to open without breaking the seal. Once the seal has been broken to deploy the weapon for use, training, inadvertently, or for maintenance/inspection, it shall not be deployed again until an instructor has inspected the weapon and resealed the case. The seal does not alleviate the requirement of the deploying officer to do a secondary check to verify the correct projectiles are in the weapon.
25. During maintenance/inspection, the air bottle pressure shall be at a minimum of 1,000 pounds of pressure. If below the minimum, a certified instructor or a trained supervisors shall re-pressurize the air bottle to its maximum pressure utilizing the high-pressure air tank. A second air bottle shall be deployed within each protective case. As with any high-pressure system, caution must be exercised to prevent a hazardous situation. The high-pressure air tank for refilling bottles to power the PepperBall launching system will be kept in the armory. For increased safety, those assigned to refill the air bottle shall wear the safety glasses when recharging.
26. The PepperBall launching system assigned to SERT shall be stored in the UPD armory.

H. Electronic Control Device (E.C.D.):

1. The E.C.D. is a hand held, battery operated electronic control device that delivers low electrical amperage which dominates the neuromuscular system causing involuntary muscle contractions and in most cases, temporarily incapacitates a person. It can be discharged using a single use dart cartridge or through direct contact. It is designed to temporarily immobilize a violent or potentially violent person. It is an additional police tool and is not intended to replace firearms, striking instruments, chemical deterrents, extended range impact s, or self-defense techniques.
2. Approved E.C.D. for the Department shall be a Taser Model X26P deploying a Taser 25 ft. cartridge.
3. Officers carrying and using the E.C.D. shall comply with all limits and stipulations provided in training and certification.
4. The E.C.D. is not intended to cause death or serious physical injury.
5. Justification for use:
 - d. In situations in which a person appears to be a danger to himself/herself or others.
 - e. To control a dangerous or violent person when deadly force does not appear to be justified and/or necessary.
 - f. When other attempts to control or subdue the person by conventional tactics have been or likely will be ineffective.

6. If the person is not an immediate threat, do not immediately resort to the E.C.D. without first attempting to use de-escalation techniques, negotiation, commands, or physical skills.
7. Second or subsequent discharges of power from the E.C.D. may be initiated if the person appears to be recovering from the prior power application and they have once again become a threat to themselves or others.
8. The E.C.D. shall not be aimed at the head, neck, or groin area.
9. When able, officers shall have back-up present to prepare to secure the suspect and assist if the E.C.D. is not effective.
10. If at any time during the application of the E.C.D., the operator or supervisor determines that further cycles of power will not effectively incapacitate the person, use of the E.C.D. shall cease.
11. Unless it is an immediate life-threatening situation, the E.C.D. shall not be used on persons that are actually or perceived to be mentally ill, young children, elderly persons, women known to be pregnant, visibly frail persons, or individuals that are known to have heart ailments or pacemaker implants and other elevated risk population members.
12. The E.C.D. shall not be used to gain compliance from persons who are exhibiting passive resistance, unless there is a reasonable expectation that it will be unsafe for officers to approach within contact distance of the person and all other options are not practical or effective. The E.C.D. is not a first choice option with persons who are passively resisting.
13. If appropriate the E.C.D. may be used on animals.
14. The E.C.D. shall not knowingly be discharged or tested near flammable or explosive materials.
15. E.C.D. shall not be used against suspects in physical control of a vehicle in motion unless exigent circumstances exist.
16. Unless it is a situation where deadly force is justified, E.C.D. shall not be used when a subject is in a location where a fall is likely to cause serious physical injury or death.
17. All persons receiving a discharge from the E.C.D. shall be treated and evaluated by certified EMS personnel or transported to a medical facility for treatment and evaluation.
18. It is the officer's discretion, based on where the probes are lodged, if police, EMS, or other medical facility personnel will remove the probes. If the police remove the probes, the officer will follow the safety procedures detailed in department training.
19. If circumstances dictate that pain is reasonably unlikely to be effective, (usually due to drug, alcohol, or mental illness causing elevated pain tolerance), officers shall avoid using pain compliance to attempt to gain control of the subject.
20. After deploying the E.C.D. on or at a person, the air cartridge and probes shall be retained as evidence in the manner shown in the Department's training course. If the E.C.D. is accidentally

discharged or used on an animal, the incident will be documented and forwarded to the officer's supervisor on an interdepartmental report or an incident report.

21. The E.C.D. shall be carried on the officer's body on the opposite side of the officer's firearm. The midline of the body shall be used to determine opposite side of the officer's body. This is intended to avoid the accidental drawing and/or firing of an officer's firearm while attempting to deploy the E.C.D. The E.C.D. shall be carried in an approved holster on the external vest carrier or the duty belt. Officers may choose from a cross draw or support hand draw configuration. An exception to the opposite side carry requirement is allowed only if the E.C.D. is carried on an external vest carrier in a cross-draw holster utilizing a support hand draw.
22. Other officers on the scene must be made aware of the use of the E.C.D. to ensure officers do not mistake the sound of the E.C.D. as gunfire causing officers to fire their weapons.
23. Available E.C.D.s shall be deployed for use during uniform patrol duty or any other assignment requiring a uniform. Patrol area and supervisory assignments shall have priority over other duties (e.g. contract duty assignments, reserve officer assignments).
24. When available, an E.C.D. shall be deployed by investigators engaged in enforcement activity.
25. Command staff and other administrative assignments not engaged in enforcement activity are exempt from the requirement to carry an E.C.D.

I. Extended Range Impact Weapon:

1. The approved extended range impact weapon shall be dedicated use LMT Defense 40mm Single Launchers.
 - (a) When utilized by officers that are not part of the Suburban Emergency Response Team (SERT), the weapons shall only be used to deploy CTS 4557 Foam Baton 40mm munitions.
 - (b) A training round may be used for training and qualification as recommended by the manufacturer.
 - (c) When deployed by SERT members, the LMT Defense 40mm single launcher or multi-launcher may also be utilized by trained personnel to deliver a variety of munitions to include the following:

Manufacture	Model	Type	Authorized Use
CTS	4557	40mm Foam Baton	Officer/SERT
CTS	4553	40mm Sting Ball Rubber Pellet	SERT
CTS	4558	40mm Sting-Ball .60 Cal Rubber Pellet	SERT
CTS	4551	40mm Rubber Foam Multi-Projectile (3)	SERT
Defense Technology	N/A	40mm Reloadable Training Projectiles, Bases, and Primers	Officer/SERT

CTS	4550	40mm Marking/Training Rounds	SERT
CTS	4401	Inert Powder Barricade Penetration (Window/ rigid surface penetration)	SERT

(d) Trained SERT personnel shall also be authorized to utilize the following hand deployed munitions:

CTS	9594	Sting Ball Grenade	SERT

2. Prior to being deployed for use in the Patrol Division, the extended range impact weapon shall be inspected by one of the certified extended range impact weapon instructors. The instructor shall ensure proper functioning and verify the CTS 4557 Foam Baton 40mm munitions are deployed with the weapon. Upon completion of the inspection, the instructor shall place the weapon in its case and place a seal on the case. The case shall not be able to open without breaking the seal. Once the seal has been broken to deploy the weapon for use, training, inadvertently, or for maintenance, it shall not be deployed again until an instructor has inspected the weapon and resealed the case. The seal does not alleviate the requirement of the deploying officer to do a secondary check to verify the correct ammunition is in the weapon.
3. Trained SERT personnel are authorized to use the LMT Defense 40mm single launcher or multi-launcher assigned to SERT to deploy a variety of munitions as listed in this policy. The munitions shall be clearly identifiable to the user to prevent unintended use. The multi-launcher shall never be deployed with more than one type of munition loaded in the weapon and shall not be utilized to deploy non-impact munitions. When practical, a second officer shall verify the correct munition is loaded in the launcher.
4. The potential for causing death or serious physical injury with extended range impact weapons is possible. The potential is reduced when avoiding impacts to the head, neck, groin or other areas capable of causing serious physical injury or death. These areas will not be targeted unless deadly force is justified.
5. The force generated by extended range impact weapons is at a similar level as striking instruments and shall have the same target areas.
6. The extended range impact weapon may be deployed when distance needs to be maintained from a situation encountered. Optimum range to deploy the extended range impact weapon is ten (10) to seventy-five (75) feet. Deployment at distances closer than ten (10) feet shall be avoided as it may result in a higher risk of injury to the subject. Deployment at distances greater than seventy-five (75) feet shall be avoided as accuracy and effectiveness will be diminished.

7. The extended range impact weapon shall be placed in the Force Management Paradigm at the same level as impact weapons but shall be used at the distances prescribed above.
8. The extended range impact weapon shall be deployed for use in the Patrol supervisor's vehicle and as needed during SERT operations.
9. Use of the extended range impact weapon shall be restricted to trained personnel.
10. When available, a cover team shall be staged to quickly approach and control the subject once down or incapacitated from the extended range impact weapon.
11. Other officers on the scene must be made aware of the use of the extended range impact weapon to eliminate the confusion of gunfire causing other officers to fire their weapons.
12. When able, officer deploying the extended range impact weapon shall have another officer assigned as a cover officer ready to use deadly force if necessary.
13. All persons struck by extended range impact weapon projectiles shall be treated and evaluated by certified EMS personnel or transported to a medical facility for treatment and evaluation.

J. Striking Instruments:

1. The only striking instrument approved by the department is the straight baton utilized as part of the crowd control/civil unrest response equipment. The batons may only be used with supervisory approval.
2. The straight baton shall primarily be used as a barricade or repelling device in crowd control situations or to ward off offensive attacks from suspects/assailants during crowd control situations.
3. In deadly force situations, strikes may be directed to any area of the body to include the head, neck, and groin as a means to stop or neutralize the threat.
4. When faced with a deadly force situation, officers may be forced to use anything at their disposal as a striking instrument to neutralize a threat.

K. Noise/Light Distraction Device:

1. Although not considered a less lethal option, the use of a noise/light distraction device may cause injury and increases the risk of damage to property from detonation and fire/heat.
2. Only trained SERT personnel are authorized to deploy the following noise/light distraction devices and only when following appropriate protocol as outline the SERT standard operating procedures:

Manufacture	Model	Type	Use
CTS	7290	Flash Bang (NLDD)	SERT Only
CTS	7290 T	Training NLDD	SERT Only
CTS	7290M	Mini Flash Bang	SERT Only

CTS	7290-6	Flash Bang	SERT Only

VIII. Procedure: Medical Attention

- A.** In all incidents in which force is used by an officer, appropriate medical treatment, consistent with any injury sustained by any individual, shall be rendered as quickly as reasonably possible. Medical treatment shall be provided in the form of first aid, request for emergency medical service (E.M.S.), and if appropriate, transport to a medical facility. EMS must be summoned as quickly as reasonably possible for situations in which there are obvious severe injuries, medical distress is apparent, or the subject becomes unconscious.
- B.** Anytime a person is injured by a use of force, the supervisor shall be notified immediately.
- C.** Officers shall be cognizant that injuries may not always be visible. All persons shall be closely monitored after a use of force incident for changes in their medical condition. If a person has a delayed reaction to a use of force they shall be provided first aid, medical aid from E.M.S., or transported to a medical care facility.

IX. Procedure: Reporting

- A.** In addition to case reports generated during an incident in which force is used on a person, an officer shall be required to complete a use of force reporting form when:
 - 1.** Discharging a firearm in the performance of their duties except for training purposes. When used to destroy a sick or injured animal or if accidental, the incident will be documented on an interdepartmental memorandum to the officer's supervisor. The supervisor shall forward copies to the division commander and the range administrator.
 - 2.** Any action that results in or is alleged to have resulted in injury or death of a person.
 - 3.** The use of a lethal or less lethal option. This shall include the pointing of a lethal or less lethal weapon (all less lethal weapons to include electronic control device, chemical deterrent, extended range impact weapons, PepperBall launching system, and striking instruments) as a means to gain compliance from or control of a person. When the only use of force utilized by an officer is the pointing of a weapon as a means to gain compliance or control, officers will only be required to complete the display of weapon use of force form. The display of weapon use of force form and a review by the immediate supervisor (video/audio when available) will be all that is required unless the supervisor requests additional documentation or follow up. Completed display of weapon use of force forms shall be forwarded to the Internal Affairs Administrator.
 - 4.** The use of physical force when used to gain control of a resistive person. The threshold for reporting physical force shall be anytime the force results in a person being injured (including an officer), a complaint of pain or injury even if not visible, a complaint of

excessive force, physical force likely to cause or lead to injury, or in the officer's or supervisor's opinion, sufficient physical force to warrant reporting.

- B.** The incident report and any supplemental reports associated with a use of force incident shall be submitted with the use of force reporting form. All case reports and the use of force reporting form from involved officers shall be submitted prior to the completion of the involved officer's shift unless supervisory approval is gained to delay reporting. The reports shall at minimum include the following information:

 - 1. The actions/threats by the individual that necessitated the need to use force.
 - 2. Any attempts at de-escalation prior to the use of force. If no de-escalation occurred explain why.
 - 3. Any verbal commands given. If no verbal commands occurred explain why.
 - 4. Type of force used.
 - 5. Any injuries sustained by the subject, the officer(s), or another person.
 - 6. Any information regarding medical assessment or evaluation including refusal of treatment.
- C.** The chain of command shall be immediately notified of any use of force resulting in death or serious physical injury.
- D.** Any visible injury resulting from a use of force shall be photographed and the photographs placed on the appropriate server.
- E.** Use of force reports shall be reviewed by the immediate supervisor of the officer involved. The immediate supervisor shall ensure any available evidentiary items from the use of force incident, to include audio, video, and still photography are noted (bookmark date & time or when appropriate copies attached to the report, etc.) in the use of force report for chain of command to review. Upon completion of their review, the first line supervisor shall forward the report to the division commander for review. Upon completion of their review, the division commander shall submit the report to the internal affairs administrator for review. Upon completion of their review, the Internal Affairs Administrator shall submit the report to the Chief of Police for final review. If it is determined by the Chief of Police the use of force was not appropriately applied, disciplinary action shall be determined based on Chapter 3 Section 26.1.4 (Disciplinary System) of the Operations Manual. All use of force reports shall be maintained by the Internal Affairs Administrator.
- F.** At the conclusion of all use of force reviews, supervisors from the division of the officer(s) involved shall conduct an after-action review of the use of force. At minimum the officer using force and their direct supervisor shall participate. Others may be requested to join by the commander of the affected division to include other officers, sergeants, the division commander, use of force instructors, the Internal Affairs Administrator and the Chief of Police. The after-action review shall examine the incident to include any video/audio. All involved shall discuss the incident and ways,

if any, the response may be improved and/or any lessons learned. The review may also be able to identify needs for additional training or change in tactics. The after-action review shall be documented as part of the use of force form. Any use of force resulting in death or serious physical injury to the subject or an officer shall only be reviewed as part of an after action with the approval of the Chief of Police after considering the physical and mental well-being of those involved.

- G.** The first line supervisor, division commander, and Internal Affairs Administrator shall not complete use of force review section of use of force incidents being reviewed as part of a complaint investigation or when the use of force has resulted in death or serious physical injury. When a complaint is associated with a use of force or the use of force has resulted in death or serious physical injury, the only the officers involved in the use of force shall complete the use of force form. The Chief of Police will be the only supervisor to complete the review on the use of force form utilizing the information obtained in the Internal Affairs Investigation into the complaint or the use of force resulting in death or serious physical injury.
- H.** Departmental instructors shall be allowed access to use of force reports and reviews in an effort to tailor use of force training to the specific needs of the department.
- I.** Training instructors shall be allowed to view use of force videos for internal use to improve departmental training in various use of force situations under the following restrictions:

 - 1. Training instructors shall receive the Support Services Division Commander's approval prior to reviewing any video for training purposes.
 - 2. Instructors are not allowed to share copies of the video with any other party internally or externally. The video must be reviewed by the instructor in a private setting not viewable by others.
 - 3. Any videos capturing serious physical injury or death of any party will not be allowed for viewing by an instructor without prior approval of the Chief of Police.
 - 4. If an instructor uses a use of force incident in a training setting, the lessons learned from the incident will be discussed in generalities and not specific to any employee.
- J.** Any employee whose actions or use of force in an official capacity results in the death or serious physical injury of a person shall be removed from operational assignments and placed on administrative leave with pay pending an administrative review by the Internal Affairs Unit and the Chief of Police. Based on the circumstances, the Chief of Police shall determine if the employee will be required to attend counseling.
- K.** The Internal Affairs Administrator shall submit an annual analysis of use of force activities, policies, and practices to the Chief of Police. At minimum, the analysis shall include the following information:

 - 1. Date and time of incidents

2. Types of encounters resulting in use of force
 3. Trends or patterns related to race, age, and gender of subjects involved.
 4. Trends and patterns resulting in injury to any person to include employees.
 5. Recommendations based on the findings of the analysis on policies, practices, equipment, and training.
- L. As part of the annual use of force analysis report, the Internal Affairs Administrator shall also include a section to review all assaults on sworn officers to determine trends or patterns. The review shall offer recommendations to enhance officer safety, revise policy, or address training issues.

Chapter 1: Law Enforcement Role, Responsibilities, and Relationships

Section 4: Use of Force

Subsection 3: Weapons and Training



Policy/Procedure #: 1

Title: Firearms

Last Modified:

CALEA Reference #: 4.3.1, 4.3.2, 4.3.3, 4.3.4

I. Policy: Firearms:

A policy is established to govern the types of firearms and ammunition used by officers in the performance of their duties. The policy shall establish a registration and approval process for all firearms and ammunition. Officers shall be required to demonstrate proficiency prior to being authorized to carry any firearm.

II. Procedure: Authorized Firearms:

- A.** All sworn officers shall be required to furnish their own firearm. All firearms owned by employees for use in an official capacity shall be submitted to a department range instructor for registration and authorization. The firearm shall not be carried or used in any official capacity until such authorization is obtained.
- B.** A qualified range instructor shall approve each firearm prior to the weapon being carried in an official capacity. Any firearm determined to be unsafe by a range instructor shall be removed from service until the weapon is repaired and deemed safe by a range instructor.
- C.** Each firearm authorized for use in an official capacity shall have a file containing the following:
 - 1.** Date the firearm was authorized for use in an official capacity.
 - 2.** Excluding routine cleaning, a log of all maintenance, repairs, or alteration completed on the firearm.
- D.** Officers are required to carry a semi-automatic firearm in one of the authorized calibers as their primary or special operations firearm while performing the functions of their job. Exceptions shall be granted for jails, holding facilities, court, training, or other situations where weapons are not permitted or not practical.
- E.** Officers shall be allowed no more than three (3) firearms registered with the Department for official use. At least one of the registered firearms must be a primary or special operations firearm.

- F.** Officers shall be allowed to change firearms registered with the Department with the following restrictions:
- 1.** The officer has acquired a new firearm to replace a registered firearm. Officers will be allowed one replacement per year if replaced due to personal preference.
 - 2.** The current firearm registered with the Department is not functioning properly as confirmed by a range instructor. There will be no restrictions on the number of firearms able to be replaced for this reason.
- G.** Primary firearm: The primary firearm shall be carried in a uniform capacity in an approved uniformed holster. The primary firearm shall be a semi-automatic pistol with a barrel length not less than 3.5 inches and no more than 5.5 inches. Sub-compact variations are not authorized for the primary firearm. This firearm must be carried with a minimum of three (3) magazines. Officers must complete the Department approved proficiency course for any primary firearm registered with the Department to the required standards.
- H.** Special operations firearm: The special operations firearm shall be carried in a non-uniform official capacity in an approved holster or in uniform capacity if meeting all requirements as stated for the primary firearm. The special operations firearm shall be a semi-automatic pistol and may be a sub-compact variation with a barrel length not less than 3.0 inches and no more than 5.5 inches. This firearm must be carried with a minimum of two (2) magazines. Officers assigned to administrative duties not requiring the use of a uniform duty belt may carry a special operations firearm. Officers assigned to administrative duties are not required to carry an additional magazine unless they are involved in enforcement activity. Officers must complete the Department approved proficiency course for any special operations firearm registered with the Department to the required standards.
- I.** Secondary Firearm: The secondary firearm may be carried as a back-up firearm to either the primary or special operations firearm in an approved holster. If carried in an official capacity, the secondary firearm must be carried in conjunction with the primary or special operations firearm. The secondary firearm may be a revolver or a semi-automatic pistol. The secondary firearm must be carried concealed from view. The barrel length shall not exceed five 5.5 inches. The secondary firearm must also meet standards for manufacturer, size, firing mechanisms and other criteria as established in this policy. Officers must complete the Department approved proficiency course for any secondary firearm registered with the Department to the required standards.
- J.** Duty Rifle: The duty rifle is any rifle used in an official capacity and meets the specifications listed in this policy for rifles. Prior to use, an officer assigned a duty rifle by the Department must complete the Department approved qualification course and training to the required standards.

Officers assigned to SERT may have additional qualification standards that must be met.

- K. Duty Shotgun: The duty shotgun is any shotgun used in an official capacity and meeting the specifications listed in this policy for shotguns. All officers must complete the Department approved proficiency course and training for the shotgun to the required standards.
- L. Holsters: The Department shall provide all new officers with their initial holster for their primary firearm. Any need for additional holsters shall be the responsibility of the employee. All holsters used while on duty shall meet the specifications listed below. Any alterations to the specifications must be approved by the Chief of Police or designee.
 - 1. Specifically fits the make and model of the weapon.
 - 2. Appropriately accommodates all accessories to include weapon light, optics, and sights.
 - 3. Holster allows the weapon to be holstered and secured with one hand.
 - 4. Holster allows strong hand draw.
 - 5. Holster must securely hold the weapon during strenuous physical activity (e.g. running or use of force situations).

In addition to the above requirements, specific types of holsters will have the following requirements.

- 1. Uniform duty holsters shall be a black basketweave style with a minimum of a level 2 retention that attaches to the duty belt in a high, medium, or low ride configuration.
- 2. Non-uniformed duty holsters shall be attached on the belt or inside the waistband.
- 3. Holsters designed with the weapon to be worn inside the waistband must be concealed.
- 4. Secondary holsters shall be securely attached to the ankle or the ballistic vest.
- 5. Specialized holsters (thigh holsters, shoulder holsters, cross draw holsters, etc.) and their manner of attachment must be specifically approved by the Chief of Police or designee and shall only be used during specialized or collateral duty assignments that have been determined to require a specific type of holster. A specialized holster is not allowed for use as a uniform or non-uniform duty holster.

III. Procedure: Miniature Red Dot Sights (MRDS):

- A. MRDS systems are approved as a sight system option for primary, special operation, and secondary weapons utilized by officers. Officers attending the Iowa Law Enforcement Academy have the option to utilize an MRDS system.
- B. Primary, special operation and secondary weapons utilizing a MRDS system shall meet all firearms requirements in this policy for manufacturer, size, caliber, and color.
- C. Approved methods for attaching the MRDS system to the firearm:
 - 1. Existing slide milled by a reputable machinist.

2. Original Equipment Manufacturer (OEM) firearm: Glock MOS, Springfield XD OSP, or Smith and Wesson M&P CORE.
 3. Optics shall be mounted by a qualified UPD firearms instructor, an experienced gunsmith, or through an OEM installed system.
- D.** It shall be the officer's discretion as to the manufacturer of MRDS system purchased. It is recommended the MRDS system be from a reputable company such as Trijicon or Holosun which has been researched, tested, and recommended for duty use.
- E.** The holster utilized for a handgun with MRDS system must meet policy requirements regarding retention and appearance. Officers shall be responsible for purchasing their own holster if the department has already provided the officer with a holster for a firearm without an MRDS system.
- F.** Care and maintenance of the MRDS system shall be the responsibility of each individual officer. Any costs associated with the system shall be the responsibility of the individual officer. The battery for the MRDS system shall at minimum be replaced annually by the Department during weapon inspections. All firearms utilizing an MRDS system shall have back up iron sights.
- G.** Officers shall be required to successfully complete the initial training and qualification requirements established by the Range Administrator for firearms with an MRDS system prior to carrying in any official capacity. All training and qualifications shall be documented in the officer's training file. Training restrictions shall include:
1. The Range administrator shall determine requirements to be met to successfully complete training and qualification.
 2. Classroom and practical training will be instructed by UPD or outside instructors.
 3. Equipment failures that are not able to be immediately remedied shall result in removal from training session. Officer will be able to reapply for a future class.
 4. Inability to meet training and qualification requirements will result in failure of the training program. Officers failing will only be allowed one additional attempt to pass the training program per calendar year. Officers shall only be allowed into future training classes based on availability with officers attending for initial training having preference for openings.
 5. Officers will only be required to complete the training course for their initial weapon system utilizing an MRDS system. Additional MRDS systems acquired by an officer for new or additional firearms shall only require the officer to successfully complete state and/or Department qualification requirements.
 6. Officers who attend and successfully complete the Iowa Law Enforcement Academy with an MRDS system will be exempt from the Department's MRDS initial training requirements. Officers will not be exempt from qualification standards.

- H. Officers utilizing a MRDS system shall qualify annually on the state mandated qualification course with their MRDS system. Officers who do not meet annual qualification requirements with their MRDS system shall not be allowed to carry their MRDS equipped firearm for duty purposes. Officers shall follow the remedial training section of this policy if they are unable to qualify.
- I. Equipment failures during training, qualifications, or duty use shall result in the MRDS system weapon being non-operational. It shall be the individual officer's responsibility to remedy the equipment failure. Once the equipment failure is corrected, the firearm must be examined and approved for use by a department firearms instructor. After approval, the officer shall be required to qualify with the MRDS system.

IV. Procedure: Firearm Requirements:

A. Approved Manufacturers:

- 1. Glock
- 2. Smith and Wesson M&P
- 3. Springfield XD
- 4. Special Approval: Officers may request approval to carry a primary or special operations firearm that is not listed as an approved manufacturer by completing the following:
 - (1) Submit a memorandum to the Chief of Police that includes the details of the firearm: manufacturer, model, caliber, color, barrel length, magazine capacity, type of sights, firing mechanism, and the reason for the request. The officer shall also include if the firearm requires any special conditions for weapon inspection.
 - (2) Special approval firearm(s) must meet all firearm requirements specified in this policy regarding primary and special operation firearms. The special approval exception does not include secondary firearms.
 - (3) If the firearm requires special conditions for weapon inspection as determined by the Range Administrator, the weapon inspection costs shall be the responsibility of the officer (e.g., shipping to an out of area armor, increased armor cost over other approved manufacturers). The officer will be responsible for providing proof of inspection within 60 days of the inspection due date. If the firearm does not need any special conditions, it will be covered under the existing weapon inspection guidelines.
 - (4) The Chief of Police shall approve or deny a request within 30 days of receipt.

- B.** All sworn officers are required to carry semi-automatic pistols from one of the approved manufacturer's listed above as their primary, special operations or secondary firearm. In addition to manufacturer, the firearm shall meet all requirements for caliber, barrel length and firing mechanisms. The approved manufacturer list does not apply to off-duty firearms, duty rifle, or duty shotgun.

- C. If the firearm meets department requirements, officers hired prior to 03-31-2011 will be allowed to carry firearms not on the approved manufacturers list. Only firearms being utilized in an official capacity prior to 03-31-2011 will be allowed. No new firearms outside the approved manufacturers list will be accepted. If the firearm is not on the approved manufacturer list, the officer shall be responsible for providing a weapon inspection from a manufacturer certified armorer. The officer shall be responsible for paying any costs associated with the inspection and shall provide proof of the inspection. The inspection must be completed within sixty (60) days of the officer's inspection due date. The inspection shall be maintained in the officer's training file by the Support Services Division.
- D. All firearms shall be inspected biennially by a manufacturer certified armorer.
- E. All firearms used in an official capacity are required to meet original factory specifications. Installing non factory sights and grips must be approved by the range administrator prior to being placed in service.
- F. Authorized primary and special operations firearms calibers shall be 9 mm, .40 cal S&W or .45 cal ACP.
- G. Authorized firing mechanisms shall be limited to traditional double action, double action only, or safe action.
- H. No light colored, stag, bone, ivory or carved grips will be permitted. Metal finish will be blue, nickel or stainless steel. Exceptions may be made by submitting a request, in writing, to the Chief of Police.

V. Procedure: Department Shotguns

- A. The Department shall provide a limited number of shotguns for use. The shotguns shall be Remington 12 gauge model 870 pump shotguns. Officers are not allowed to provide their own shotgun for official use.
- B. Ammunition for the shotguns shall be authorized and issued by the Department.
- C. It will be the responsibility of the division commanders or their designee to ensure all shotguns within their division are cleaned and maintained.
- D. Department shotguns shall be checked for cleanliness and basic maintenance needs semi-annually by range instructors. Records of the inspection shall be maintained by the range administrator or designee.
- E. Each patrol vehicle shall be outfitted with a department shotgun. The shotgun shall be mounted in the patrol vehicle to prevent unauthorized access.
- F. Shotguns mounted in patrol vehicles shall be stored with a full magazine but an empty chamber. Additional ammunition shall be stored in the same location in all patrol vehicles. The amount of additional ammunition shall be determined by the range administrator.
- G. Shotguns distributed to other divisions shall be securely stored in a state of operational readiness with an empty magazine, empty chamber and accessible ammunition.
- H. All shotguns used in an official capacity shall be inspected biennially by a manufacturer certified armorer.

VI. Procedure: Department Rifles

- A.** The Urbandale Police Department shall provide rifles for use during uniform patrol assignments, Suburban Emergency Response Team (SERT) operations, and other enforcement activities. The department rifle program is optional to officers assigned to patrol and required by officers assigned to SERT. Officers assigned to divisions outside of patrol will not be assigned a department rifle unless they are a member of SERT. Officers issued a department rifle will be expected to meet the following requirements:
1. Officers must sign a letter of intent stating the officer has read and understands the Urbandale Police Department rifle program requirements.
 2. The officer shall be required to maintain the minimum qualification standards for the rifle and shall participate in mandatory department rifle training sessions and qualifications.
 3. The officer shall maintain the rifle and accessories in a state of operational readiness to include cleaning, maintenance, and proper storage. The officer shall be subject to periodic inspections of the rifle and accessories.
 4. Except for contracted duty assignments and excluding officers issued a .308 caliber weapon system, the officer agrees to deploy their rifle during all tours of duty. Exceptions may be granted by a supervisor for special assignments in which the officer is not utilizing a vehicle.
- B.** Except for the .308 caliber weapon system noted in this policy, department rifles shall be restricted to a Colt AR-15 model in .223 caliber.
- C.** In addition to any policy regarding the securing of weapons as stated in the Operations Manual, the following shall apply to department rifles:
1. Officers shall be responsible for the security and cleaning of their rifle. When not in use, the rifle must be secured from unauthorized personnel.
 2. While working a uniform patrol assignment, the officer shall be required to secure their rifle within the patrol vehicle by use of the weapon lock system to prevent unauthorized access and to make the rifle available for immediate deployment.
 3. Unless properly secured, a rifle shall never be left unattended.
 4. The school resource officer (SRO) shall secure their rifle within a locked safe in the SRO office unless deploying. The rifle may remain in the locked safe during non-work hours. If transporting the rifle from the school for training, maintenance, etc., the rifle will always be within a secure carrying case. At no time shall the rifle be displayed or carried within the school or on school grounds unless deploying the rifle for a call for service warranting rifle use. If removed from the locked safe at the school, the rifle must be removed from the vehicle and secured within the police facility or the SRO's residence when not working.

- D.** Prior to being authorized to carry a rifle as part of the department rifle program, officers must successfully complete the department prescribed rifle qualification course and training. In addition to the department rifle qualification course and training, SERT officers shall also be required to complete SERT training and qualification requirements.
- E.** Officers assigned a department issued rifle must agree to participate in the department rifle program for a minimum of two (2) years. Officers no longer wanting to participate in the department rifle program shall submit a written request to the range administrator.
- F.** Officers accepted into the department rifle program and receiving a department rifle shall be issued the following:

 - 1. A Colt AR-15 rifle.
 - 2. A sling system.
 - 3. Quad rail hand guard.
 - 4. Tactical light.
 - 5. Two magazines.
 - 6. Authorized duty ammunition.
 - 7. Gun case.
 - 8. Any other equipment or accessories deemed necessary by the range administrator.
 - 9. Optics.
- G.** An officer with a department issued rifle who becomes a member of SERT will continue to utilize the department rifle they have been issued.
- H.** All department owned rifles shall be inspected biennially by a manufacturer certified armorer.
- I.** Rifles shall not be modified in any way from their manufacture settings. Exceptions to modification shall include minor adjustments as need is determined by a department certified armor or adjustment by the operator of the carrying strap/sling, stock, long/short range aperture, and elevation knob. Any accessories not listed in this policy shall be approved by the Chief of Police or his designee prior to use and shall be installed by a department armorer.
- J.** The Department shall provide select officers who are part of the SERT marksman/observer unit with a scoped .308 caliber weapon system. The officers assigned these weapons shall only deploy the weapon during approved SERT operations, training, or by supervisory approval. Scoped .308 caliber weapon systems issued by the Department shall be armored annually by a manufacturer certified armorer.
- K.** Unless in use during an incident, all rifles shall be deployed with an empty chamber and a full magazine attached. Additional ammunition shall be carried as determined by the range administrator. Only department issued and approved ammunition is authorized for rifles used in an official capacity.
- L.** Rifles shall be checked for cleanliness and basic maintenance needs semi-annually by range instructors. Records of the inspection shall be maintained by the range administrator or designee.

VII. Procedure: Knives

- A.** Officers are authorized to possess and use a knife while on duty. If an officer chooses to carry a knife while on duty, the officer shall furnish their own knife. It is recognized officers may have many needs for a knife, including both general use and for limited defensive purposes. While not considered to be a primary weapon of choice in a defense of life situation, officers may, under extraordinary circumstances, use a knife in defense of their life or the lives of others.
- B.** Nothing in this policy requires any officer to carry any knife. This policy is intended to aid the officer, should the officer elect to carry a knife, in the acceptable use of the knife in common tasks and under extraordinary circumstances in the defense of life.
- C.** Officers must request to carry a knife from their division commander. The division commander shall inspect the knife prior to approval for use to ensure it meets department specifications. The specification for a knife to be carried while on duty are listed below:
 - 1. Officers may carry one knife of a folding blade or fixed blade type.
 - 2. The brand, design and style of knife will be at the officer's discretion.
 - 3. Knives shall have a blade length of five (5) inches or less.
 - 4. Except for special assignments where the use of a fixed blade is specifically provided (e.g. S.E.R.T), the possession or use of a fixed blade knife by sworn personnel is permitted only if the blade is contained in a protective scabbard or carrier and the entire knife is concealed from view.
- D. General Use:**
 - 1. The carrying and use of any knife by officers shall be carried out as unobtrusive as possible so as not to alarm any bystanders.
 - 2. It is the individual officer's responsibility to use the duty knife as a tool in a safe and responsible manner.
 - 3. Officers shall use reasonable care in the general use of a knife as a tool to prevent injury to themselves and others.
 - 4. Officers shall use reasonable care in the general use of a knife as a tool to prevent damage to property.
- E. Defensive use of any knife:**
 - 1. It is recognized an officer during his or her duties may require the use of the duty knife as a means of defense under extraordinary circumstances.
 - 2. Officers shall be aware the duty knife is primarily a cutting tool to assist them in their daily duties and not intended by the Department to be a primary weapon of defense. Extraordinary circumstances may dictate the duty knife be used as an immediate measure of defense of life. An "immediate measure of defense of life" is defined as taking action or using any implements to defend the officer's life or safety of another with implements or devices not normally intended to be a weapon or issued as public safety equipment.

- F. Medical assistance shall be obtained as soon as practical for subjects who have sustained injury, expressed any complaint of injury, or the officer feels he or she has been injured in any use of force including incidents involving use of a duty knife.
- G. Supervisory notification and a use of force report shall be made as soon as practical following the application of use of force involving a duty knife.

VIII. Procedure: Ammunition

- A. Ammunition carried in an official capacity must be approved and issued by the Department. Off-duty firearms, not registered with the department as a primary, special operations, or secondary weapon, shall not carry department issued ammunition. Duty ammunition will be replaced annually. The table below lists all authorized ammunition information types:

380 caliber	Speer Gold Dot 90 GR HP
.38 special	Speer Gold Dot 125 GR HP
.357 caliber	Speer Gold Dot 125 GR GDHP
9 mm	Speer Gold Dot 147 GR
.40 caliber	Speer Gold Dot 180 GR
.45 caliber	Speer Gold Dot 230 GR
.223 caliber	Federal 55 GR Tactical Bonded
.308 caliber	Federal Match 168 GR, Boat Tail HP
.308 caliber	Federal Tactical Bonded 165 GR
12 Ga Buckshot	Federal Tactical 9 pellet
12 Ga Slug	Federal Tactical

IX. Procedure: Storage and Security of Firearms:

- A. Except when utilizing the firearm loading/unloading device or within the designated firing range, officers shall not clean, repair, load or unload firearms any place in the police building. The loading/unloading device shall be assigned to the range observation room.
- B. All sworn officers shall have a secure storage or locking device for each department approved weapon. Officers without access to secure storage or a locking device shall request a cable-style gunlock through the Support Services Division. When not in use, every officer shall secure and safely store their weapons.
- C. Firearms of any type shall not be left unattended. When the firearm needs to be stored, it will be secured by ensuring the firearm is not accessible or in view of non-departmental personnel who may enter the building, separating it from access to common areas, or rendering the firearm unusable. Unusable shall mean a firearm broken down into its component parts. When not in use, department shotguns, rifles and other firearms shall be secured in the department armory.
- D. During public presentations where citizens/children are allowed access to any department vehicle, rifles and shotguns shall be removed from their interior vehicle racks, unloaded, and placed into a gun case and secured

within the vehicle's trunk or rear storage compartment. In lieu of securing in the trunk or rear storage compartment of the vehicle, the rifle and shotgun shall be removed from the vehicle and properly stored within the Department.

- E. If a department vehicle is in need of repairs, new equipment, or any other service, all weapons will be removed from the vehicle and properly stored within the Department prior to releasing control of the vehicle to a third party.
- F. Civilian employees of the Department, who carry firearms under the authority of a valid weapons permit, are prohibited by the City of Urbandale's workplace non-violence policy from carrying weapons onto city property unless authorized by the Chief of Police.
- G. Any lost or stolen firearm shall be reported immediately by the officer through their immediate supervisor to their division commander. When appropriate, a report shall be filed with the police agency having jurisdiction over the lost or stolen firearm.
- H. Department issued less lethal weapons or firearms shall never be stored overnight in a vehicle unless the vehicle is equipped with a department provided weapon securing mechanism. Officers without a weapon securing mechanism must remove less lethal weapons or firearms from the vehicle and secure them within the police facility or the officer's residence at the end of their tour of duty. Unless being deployed, officers utilizing a department issued less lethal weapon or firearm in a non-uniform assignment (e.g. investigations) shall secure the less lethal weapon or firearm in the police facility or in their vehicle outside of the public view during their tour of duty.

I.

X. Procedure: Request for Variation, Change or Amendments

- A. Any officers requesting changes, amendments, variations, additions or deletions to any of the elements of this policy governing authorized firearms, ammunition or calibers shall submit a formal detailed proposal through channels to the range administrator. It shall be the requesting officer's responsibility to prepare this proposal in the below listed format:
 - 1. Detailed memorandum covering the reasoning and justification for the requested change.
 - 2. Detailed explanation/narrative as to why or how current authorizations do not meet the mission requirements.
 - 3. Detailed comparison as to how this change significantly improves capabilities over current authorizations.
 - 4. Cost analysis and impact statement for the implementation of the change; training cost, ammunition and equipment cost and maintenance/sustainment cost must be addressed.
 - 5. Background data supporting the enhancement of capabilities.
 - 6. Survey data detailing consensus for the proposal.

XI. Procedure: Training

- A. Prior to authorization to carry or use a firearm or any less lethal option, an officer shall receive a copy of and instruction in the Use of Force

policy. The issuance and receipt of the policy and any instruction received shall be documented.

- B.** All officers shall receive firearms training from the Department's range instructors specific to the type of firearm they are carrying.
- C.** Department policy on use of force and the use of deadly force shall be reviewed annually during in-service or similar training including a review of terms used to determine when deadly force is justified.
- D.** Firearms training with a proficiency test shall occur annually.
- E.** Officers shall be required to pass a proficiency test before being allowed to carry a firearm in an official capacity. The proficiency test shall be developed by the range administrator and shall conform to State of Iowa requirements. The proficiency test used for each type of firearm must be defensible and commonly accepted in the field of law enforcement.
- F.** All firearms training and proficiency testing shall be documented by the range administrator or designee. Copies shall be provided to the Support Services Division to be placed in the training file of each officer.
- G.** Remedial firearms training shall be provided to any officer identified as being deficient with a specific firearm. Remedial firearms training is personalized training to correct a specific deficiency identified by proficiency testing, other evaluation processes, and training or routine job performance. Remedial firearms training for an officer may be requested by any range instructor or supervisor.
- H.** Remedial firearms training shall be required for any officer unable to pass proficiency testing after three (3) attempts. The remedial training shall not occur on the same date as the failed proficiency testing. The remedial training shall be customized to correct the deficiencies observed by range instructors. A remedial training plan along with documentation of actual training shall be logged by the range administrator or designee with copies being forwarded to Support Services Division to be placed in the training file of the officer.
- I.** If remedial training is needed for a firearm, it shall be completed within five (5) working days. If unable to pass proficiency testing after the remedial training, the Chief of Police shall determine if the officer will be assigned to restricted duties. If restrictions are implemented, they shall remain in effect until proficiency is obtained. Furthermore, it is the responsibility of all instructors to inform the range administrator as soon as practical of any officer's failure to pass proficiency testing within the guidelines listed in this policy.
- J.** If the officer is unable to obtain proficiency after remediation, the Chief of Police shall determine how to proceed based on the recommendations of the range administrator.
- K.** Officers unable to meet proficiency requirements with a secondary firearm or rifle will not be required to meet the five (5) day remediation requirement and will not be assigned to restricted duty. If unable to meet proficiency requirements, officers will be restricted from utilizing/carrying the secondary firearm or rifle while on-duty.

Chapter 1: Law Enforcement Role, Responsibility, and Relationships
Section 4: Use of Force
Subsection 3: Weapons and Training



Policy/Procedure #: 5
Title: Firearms Range
Last Modified:
CALEA Reference#: 4.3.5

I. Policy: Police Firearms Range

It is the policy of the Urbandale Police Department to utilize a variety of shooting ranges operated by the Department or outside agencies in a safe manner while developing the skills and abilities of officers to use firearms and other weapons to perform the functions of their duties in a safe and effective manner. The safety of all personnel shall be a primary concern and all individuals are expected to adhere to the highest standards of safety during firearms range activities.

II. Procedure: Safety

- A.** The following rules of weapon safety shall be adhered to during any firearms or applicable less lethal training. Applicable less lethal training shall be any less lethal training in which a gun or a gun type device is utilized to fire a projectile (e.g. less lethal shotgun, Taser, any weapon utilizing simulated munitions, etc.).
1. Treat all weapons as though they are loaded.
 2. Point the muzzle in a safe direction at all times.
 3. Keep your finger outside the trigger guard until you are on target to fire.
 4. Be sure of your target and what is beyond.
- B.** The following safety rules shall be utilized during any firearms or applicable less lethal training. Firearms/less lethal instructor(s) shall be in charge of the training; however, everyone has the responsibility to ensure the following rules and safety procedures are followed. Any violations of the following rules shall be reported to a training instructor or supervisor and immediately corrected.
1. All participants, instructors, and observers utilizing a shooting range are required to use available safety equipment to include protective body armor, as well as eye and ear protection. Additional safety equipment may be required depending on the type of training or as required by the instructor.

2. Upon taking control of a weapon, lock the slide back or open the cylinder. Visually and physically check to see if the weapon is unloaded. Check the weapon a second time. This shall be completed utilizing a firearm loading/unloading device or by pointing the weapon down range when safe to do so.
 3. Never give or take a weapon unless the slide is locked back or the cylinder is open.
 4. Load only after position is taken on the firing line and the command to load by the firearms or less lethal instructor is given.
 5. Unload, re-load, de-cock, or unlock as instructed by the firearms or less lethal instructor.
 6. When not holstered or secured in a case, weapons shall be pointed down range at all times.
 7. While on the range, never draw your weapon from the holster unless instructed to do so.
 8. Never draw or holster with your finger in the trigger guard.
 9. Never holster a cocked weapon.
 10. Never leave your firing point unless instructed to do so by a firearms or less lethal instructor.
 11. Never go forward of the firing line unless instructed to do so by a firearms or less lethal instructor.
 12. Never bend over to retrieve dropped items on the firing line until instructed to do so by a firearms or less lethal instructor.
 13. No talking on the firing line except by or with an instructor.
 14. Pay strict attention to the firearms or less lethal instructor.
 15. Never anticipate a command.
 16. Never permit the muzzle of a weapon to touch the ground.
 17. Conduct a safety check on your weapon before and after training.
 18. Never dry fire your weapon on the range unless instructed to do so by a firearms or less lethal instructor.
- C. Acknowledgement of the above stated safety rules shall occur before each use of a range in at least one of the following manners:
1. Each participant shall review and sign a printed copy of the safety rules. Signed acknowledgement shall be required of outside agency instructors and officers utilizing the indoor range.
 2. Instructors may review the safety rules with a group documenting the review in the training outline or lesson plan.
 3. A copy of the rules shall be posted in a prominent location within the indoor range and be reviewed prior to use. The instructor in charge of the training shall ensure the rules are reviewed by all participants prior to use.
- D. Any firearms or applicable less lethal training shall require a certified instructor in the applicable weapon system being present, controlling the training, and ensuring all required safety procedures as outlined in this policy are being followed.

- E. All firearms and applicable less lethal instructors shall be required to maintain certification in First Aid/CPR. In addition, all firearms and applicable less lethal instructors shall receive additional training in "Stop the Bleed" or traumatic injury first aid that addresses initial treatment of firearm type injuries.
- F. During any range use, a first aid kit with specific supplies capable of treating a traumatic injury (e.g. tourniquet, blood stoppers, etc.) shall be on hand at all times. It shall be the responsibility of the instructor to ensure the kit is on-site and has proper supplies prior to any range use.
- G. Any injury sustained on any firearms range shall be immediately reported to the firearms or less lethal instructor. The instructor shall determine the need for immediate medical treatment and request the appropriate medical response as needed. As soon as practical, the instructor shall report the incident to the Range Administrator or if unavailable, a Support Services Division supervisor. If injuries are severe enough to require outside medical treatment, the Range Administrator or supervisor shall notify the Chief of Police as soon as practical.
- H. Based on the severity of the incident causing injury, the Range Administrator may request documentation from the instructor and/or the injured party. The documentation shall assist the Department in determining policy/procedure violations as well as a means to prevent future safety incidents.
- I. The Department may provide the ability for officers and reserves to utilize a private range during their off duty hours by providing a membership to the range and/or limited department ammunition as a way to increase their firearm skills. Any use of a privately owned range by department employees while not on duty shall be voluntary and at the employees own risk as it will not be controlled by department personnel.

III. Procedure: Urbandale Police Department Indoor Range Use

- A. The main purpose of the indoor range at the Urbandale Police Department is to train sworn personnel and reserve officers in the safe and proper use of weapon systems utilized as part of their job duties. Occasionally, the indoor range may be utilized to assist in community relation activities as stated in this policy.
- B. When accompanied by a certified instructor in the weapon system being utilized, the following persons are authorized to use the Urbandale Police Department indoor range (indoor range). When using other ranges, the controlling entity shall determine range restrictions and rules.
 - 1. Sworn officers and reserves of the Urbandale Police Department.
 - 2. Sworn law enforcement officers or reserves from other agencies.
 - 3. Retired Urbandale police officers if eligible to receive and as a means to meet the requirements of the Law Enforcement Officers Safety Act (LEOSA).
 - 4. Civilians with prior approval of the Range Administrator or the Chief of Police. Civilian use shall be rare and sufficiently restricted to ensure safe use.

- C. Any party utilizing the indoor range that is not an Urbandale police officer or Urbandale reserve police officer shall be required to read and sign the Firearms Range Use Waiver, Range Safety and Rules form, and adhere to all safety requirements and rules each time they utilize the indoor range.
- D. Outside law enforcement agencies utilizing the Urbandale Police Department indoor range shall be required to provide a certified instructor in the weapon system being utilized. Any outside certified instructors shall be required to read and sign the Firearms Range Use Waiver for Certified Firearms Instructors and the Range Safety and Rules form prior to range use as well as adhere to all safety requirements and rules. If needed, outside law enforcement agencies may request an Urbandale Police Department certified instructor to assist through the Range Administrator. Requests to utilize the indoor range shall be directed to and approved by the Range Administrator, the Chief of Police or designee.
- E. The following rules will apply to the indoor range:
 - 1. The door to between the range and the range observation room as well as the exterior door leading to the administrative hallway shall be securely closed during any live firing in the range.
 - 2. Weapons shall only be fired towards the ballistic wall in the north end of the range.
 - 3. A maximum of 3 shooters on the range during any live fire training. Under normal circumstances, observers shall be required to be in the range observation room during live fire unless specifically being allowed in the room by a range instructor as part of the training.
 - 4. Paper targets only. No metal, clay, rubber, plastic or other types of material targets are allowed.
 - 5. Permitted weapons:
 - (a) All handguns utilizing the following calibers: 380, .38 special, .357, 9 mm, .40, .45.
 - (b) Shotguns including less lethal shotguns are not allowed.
 - (c) AR-15 type rifles firing .223 caliber ammunition are allowed but limited due to the need for increased hearing protection measures. Rifles may only be utilized after obtaining Range Administrator approval.
 - (d) No automatic weapons of any type.
 - (e) No less lethal shotguns or other less lethal weapons that fire a projectile that will not penetrate the ballistic wall as the projectile may ricochet and cause a danger of being struck.
 - 6. Only clean fire ammunition.
 - 7. Weapon loading and unloading shall only occur with instructor approval in the range or in the range observation room utilizing the loading/unloading device.
 - 8. The ventilation fan within the range shall be required during use of any weapon and during any cleaning of weapons.

9. Any use of additional equipment such as portable barricades, lighting etc. shall be approved by the Range Administrator.
 10. The Range Administrator, supervisor, or firearms instructors shall ensure any outside agency use of the indoor range are aware of and adhere to all of the indoor range requirement and restrictions.
- F.** Key access to the indoor range shall be limited to the following:
1. Firearms instructors
 2. Supervisors
 3. Support Services Division personnel for cleaning and maintenance needs.
 4. Temporary access may be granted to outside agency certified instructors as needed to complete authorized training and to maintenance personnel to complete needed repairs.
- G.** If an employee notices damage or equipment in need of repair or replacement, a repair/service request form shall be forwarded to the Support Services Division with a copy or notice being provided to the Range Administrator.
- H.** Only sworn officers, reserves, and Support Services Division personnel shall have key access to the range observation room.
- I.** Upon completion of training, all ammunition and weapons shall be properly stored in the ammunition vault, gun lockers, or other designated storage. Weapons and ammunition assigned to a specific officer or reserve officer shall be secured as stated in Chapter 1 Section 1.3.9 (Firearms) of the Operations Manual.
- J.** Individuals or groups utilizing the indoor range or range observation room shall ensure the room(s) are clean upon completion of use to include the following tasks:
1. All equipment is picked up and organized.
 2. Debris is cleaned up.
 3. All supplies and material are stored in their appropriate place.
 4. All equipment is returned (e.g. eye and ear protection, ammunition, targets)
 5. Brass is picked up and floor is swept (as needed)
 6. If trash is full, it is emptied in an outside receptacle (cleaning personnel do not have access to the range or range observation room)
 7. Ventilation and lights are turned off.

Chapter 2: Organization, Management and Administration
Section 11: Organization and Administration
Subsection 1: Organizational Structure



Policy/Procedure #:1

Title: Organizational Structure and Function

CALEA Reference#: 11.1.1

I. Policy: Organizational Structure and Function

A policy is established to describe the Urbandale Police Department organizational structure and the functions of the various divisions within the organizational structure. The organizational structure of the Department shall be based on function, unity of command, delineation of responsibility, accountability, and the delegation of authority. The organizational structure of the Department shall be structured to maximize communication, cooperation and coordination of police functions.

II. Procedure: Organizational Structure

A. Urbandale Police Department shall be composed of officers and civilian employees as provided by budgetary appropriation or as directed by the City Manager and the City Council. At any time, officers and civilian employees may be relocated to different positions and/or assignments within the Department in order to accomplish goals and satisfy needs of the Department. The current organizational structure and function of the Department shall be available to all employees by publishing this policy in the Operations Manual and through the Power DMS document management system. The organizational structure shall also be available to the public through our website where all department policies are published. The Urbandale Police Department shall be divided into the Office of the Chief of Police and three (3) divisions. Each division may be further divided into watches or units. The Office of the Chief of Police shall have authority over each of the divisions.

B. Office of the Chief of Police:

The Office of the Chief of Police shall be comprised of the following positions listed in descending authority:

1. Chief of police

2. Administrative specialist

C. Patrol Division:

The Patrol Division shall be comprised of the following positions listed in descending authority:

1. Patrol captain
2. Patrol sergeants
3. Patrol officers

D. Criminal Investigations Division:

The Criminal Investigations Division shall be comprised of the following positions listed in descending authority:

1. Criminal investigations captain
2. Criminal investigations sergeants and narcotics investigations sergeant
3. Detectives

E. Support Services Division:

The Support Services Division shall be comprised of the following positions listed in descending authority:

1. Support services captain
 - (a) Support services sergeants
 - (b) Support services officers (Community relations)
 - (c) Community service officers
 - (d) Crisis Intervention Team
2. Support services captain
 - (a) Support Services Supervisor/CALEA manager
 - (b) Administrative Specialists
 - (c) Administrative Technicians

III. Procedure: Functional Responsibilities

A. The Urbandale Police Department is tasked with numerous functions in order to accomplish its mission in the community. The responsibilities of these functions shall be assigned to each of the divisions as well as the Office of the Chief of Police. The Chief of Police shall assign functional responsibilities to each respective division or the Office of the Chief of Police to maximize efficiency and effectiveness. The Chief of Police may assign functional responsibility to the Office of the Chief of Police, a division, a unit within a division, a position, or a specific person within a division. Except for instances in which Chief of Police has made a specific assignment, the division commanders or their designee shall assign functional responsibility within the division. Functional responsibilities for each division and the Office of the Chief of Police shall include but not be limited to:

1. Office of the Chief of Police:

- Planning
- Research and development

- Program evaluation
- Professional development
- Policies and procedures
- Rules and regulations
- Budget administration
- Payroll
- Personnel administration
- Accounts payable
- Payroll management
- Meetings organization
- Purchasing
- Document creation/formatting/maintenance
- Petty cash fund
- Alarm ordinance billing
- Grant management

2. Criminal Investigation Division:

- Person crimes
- Property crimes
- Juvenile crimes
- Victim/witness services
- Fraud/forgery
- Cyber crimes
- Intelligence
- Crime analysis
- Narcotics/vice
- Crime scene investigation
- Probation- parole liaison
- Professional standards
- Tobacco and alcohol compliance
- Range Administration

3. Patrol Division:

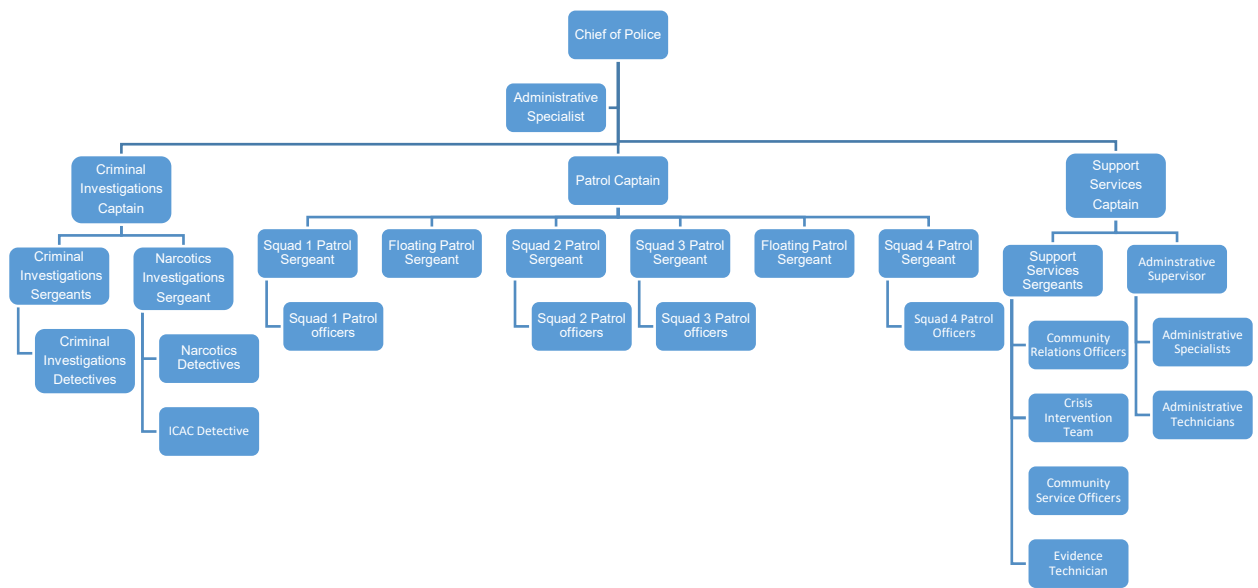
- All patrol shifts
- Patrol bicycle
- Police reserves
- Traffic enforcement and control
- Accident investigation
- Governor's Traffic Safety Bureau liaison
- Initial response to calls for service
- Vacation house checks
- K-9 unit
- Radar speed signs
- Field training officer program
- S.E.R.T. (Suburban Emergency Response Team)

4. Support Services Division:

School resource officers
School crossing guard liaison
Community relations
Press information
Technology support
Animal control
Honor guard
Police chaplains
Building maintenance
Fleet management
Uniform/equipment administration
Departmental inventory
CALEA accreditation
Emergency management liaison
Major event planning
Fees and licensing
Records
Mail distribution
Human resources
Internship program
Training
Property/evidence
Crisis Intervention

IV. Procedure: Organization Chart

- A.** When changes are made in the Urbandale Police Department affecting the organizational structure, the organizational chart shall be reviewed. Changes shall be made to the organizational chart as necessary to reflect the new structure. If the organizational chart is changed, an updated version shall be distributed to all personnel and the public.
- B.** The organizational chart for the Urbandale Police Department shall be as follows:



Chapter 2: Organization, Management and Administration
Section 11: Organization and Administration
Subsection 2: Unity of Command



Policy/Procedure #: 1

Title: Accountability and Command

CALEA Reference#: 11.2.1

I. Policy: Accountability and Command

A policy is established to clarify employee accountability in order to promote efficiency and responsibility. The policy shall establish clearly defined supervisory command and control for every level of the Urbandale Police Department.

II. Procedure: Accountability and Command

- A.** Each employee will be accountable to only one supervisor at any given time. Each employee will be accountable to the supervisor directly above them in the Urbandale Police Department chain of command. The chain of command shall follow the format outlined below and in the Urbandale Police Department organizational chart. Situations may arise requiring a supervisor to issue an order to an employee outside the supervisor's immediate chain of command. Nothing in this procedure prevents such action.
- B.** Employees shall not bypass their immediate chain of command unless urgent or immediate circumstances dictate a departure.
- C.** The Chief of Police shall establish the Office of the Chief of Police within the Department. The Office of the Chief of Police shall have the Chief of Police in command.
- D.** The Chief of Police shall establish divisions within the Department. Each division shall have one captain in command. Each captain shall be accountable to the Chief of Police.
 - 1.** If the captain from a division is absent, the senior sergeant from the division shall be in command. All rights, privileges and responsibilities of a captain assignment shall be temporarily adopted by the sergeant assuming command of a division except for those which by the nature are unique to the rank of captain.
 - 2.** The captain from a division may designate a specific officer to be in command of a division during any planned absence. Any

officer assuming command of a division shall be the rank of sergeant or above.

3. In the event the captain and all of the sergeants from a division are absent, the Chief of Police or the captain of the division shall designate a captain from another division to assume command of the division.
- E.** Captains may establish various watches, units, or subdivisions within each division. Each watch, unit or subdivision shall have one supervisor in command. If a watch, unit or subdivision has a sergeant assigned, the sergeant shall be in command. If more than one sergeant is assigned, the senior sergeant shall have command unless otherwise designated by the captain or the Chief of Police. Seniority shall be determined by time of service in grade. Each sergeant shall be accountable to the captain of their respective division.
1. Patrol shifts shall be scheduled to ensure a patrol sergeant is assigned to all shifts. If a patrol sergeant is absent, the patrol captain shall assume responsibility for the duties of the sergeant. The patrol captain may delegate these duties within the division.
 2. If the Criminal Investigation Division sergeant is absent, the Criminal Investigation Division captain shall assume responsibility for the duties of the sergeant. The Criminal Investigation Division captain may delegate these duties within the division.
 3. During the absence of the narcotics investigations sergeant, Mid Iowa Narcotics Enforcement (MINE) Task Force policy and procedure shall determine command for detectives assigned to MINE. If there are any incidents or situations for Urbandale detective(s) involving the Urbandale Police Department, the Criminal Investigation Division captain shall assume responsibility for the duties of the narcotics sergeant.
 4. If either or both of the Support Services Division sergeants are absent, the Support Services Division captain shall assume responsibility for the duties of the sergeant. The Support Services Division captain may delegate these duties within the division.
 5. The Chief of Police may place any officer in command of a division, subdivision, watch, or unit.
- F.** Each watch, unit, or subdivision of a division may have officers assigned. If a watch, unit or subdivision has an officer(s) assigned they shall be accountable to the sergeant of their respective watch, unit, or subdivision. If no sergeant is assigned to a watch, unit or subdivision, any officers assigned shall be accountable to the division captain.
- G.** The administrative supervisor/CALEA manager shall be accountable to the Support Services Division captain.
- H.** The administrative specialists and administrative technicians assigned to the Support Services Division shall be accountable to the administrative supervisor/CALEA manager. If the administrative supervisor/CALEA manager is not available, the administrative specialist and administrative technicians shall be accountable to the Support Services Division captain.

- I.** The administrative specialist assigned to the Office of the Chief of Police shall be accountable to the Chief of Police.
- J.** Each community service officer shall be accountable to a specific sergeant within the Support Services division as directed by the captain of the Support Services Division.
- K.** Each division, subdivision, watch or unit shall be under the direct command and operational control of only one supervisor as explained above and as depicted in the organizational chart.

Chapter 2: Organization, Management and Administration
Section 11: Organization and Administration
Subsection 3: Authority and Responsibility



Policy/Procedure #: 1

Title: Authority and Responsibility

CALEA Reference#: 11.3.1, 11.3.2

I. Policy: Authority and Responsibility

A policy is established to provide the department with guidelines on authority and responsibility.

II. Procedure: Authority and Responsibility

- A.** The Chief of Police shall be responsible for the performance of the Urbandale Police Department. Employees are vested with the authority necessary to perform the duties of their assignment in an effort to assist the Chief of Police in accomplishing the mission, goals and objectives of the Department. Authority to execute the required activities of a particular task in the Department is delegated by the Chief of Police through the command structure to individual employees. Such authority is found in state law, city ordinance, policy and procedures, rules and regulations, orders, and memorandums.
- B.** The success of the Department requires responsibility be accompanied by commensurate authority. At every level of the organization, employees shall be given the authority to make decisions necessary for the effective execution of their responsibilities. Employees shall not be given responsibility for a function without the commensurate decision-making authority to carry it out.
- C.** Accountability for the use or failure to use delegated authority attaches to each employee. Each employee shall be held accountable for their overall performance and the use or failure to use delegated authority in accomplishing the responsibilities of their position.

III. Procedure: Supervisory Responsibility

- A.** Supervisors shall be held accountable for the activities and performance of employees under their control. A supervisor may delegate authority to a subordinate to perform specific tasks or duties; however, ultimate

responsibility and accountability for the accomplishment of a required task or objective shall not be delegated.

- B.** The supervisor shall provide adequate guidance and supervision to subordinates for the mission, goals, and objectives of the Department to be achieved.
- C.** Each employee will be accountable to only one supervisor at any given time. Each employee will be accountable to the supervisor directly above them in the Urbandale Police Department chain of command. The chain of command shall follow the format outlined in policy and in the Urbandale Police Department organizational chart. Situations may arise requiring a supervisor to issue an order to an employee outside the supervisor's immediate chain of command. Nothing in this procedure prevents such action.
- D.** Nothing in this policy/procedure shall make a supervisor liable or responsible for acts of their subordinates when such acts are outside the course and scope of the subordinate's employment unless the supervisor ordered, approved, or ratified such acts.

Chapter 2: Organization, Management, and Administration
Section 11: Organization and Administration
Subsection 3: Authority and Responsibility



Policy/Procedure #: 3

Title: Notification to the Chief of Police

CALEA Reference#: 11.3.3

I. Policy: Notification

A policy is established to provide guidance as to when it is necessary to make immediate notification to the Chief of Police.

II. Procedure: Notification

A. The Chief of Police shall be notified immediately when certain incidents have taken place in the City of Urbandale or involve an employee(s) of the Urbandale Police Department. Any incident that may result in increased department criminal or civil liability or may produce a heightened community interest shall be immediately reported to the Chief of Police.

B. Listed below are items that shall be brought to the immediate attention of the Chief of Police by the division commander, watch commander, acting watch commander, or highest ranking officer. These incidents include but are not limited to:

1. All fatal accidents.
2. Homicide.
3. Any suspicious death.
4. Hostage situation.
5. Death or serious injury of an employee or employee's immediate family.
6. Officer involved shootings.
7. Patrol vehicle accidents with injuries.
8. All forcible felonies.
9. Emergency medical services personnel tripped to Urbandale Police Department.
10. Any disaster in which life has been lost or major property destruction has occurred.
11. Incidents which may be of significant media interest.

- 12.** An in custody death.
- 13.** Any criminal charge against a police department employee, other City of Urbandale employee, or City of Urbandale elected official.
- 14.** Any other incident not herein described that in the highest ranking officer's judgment should be reported immediately.

Chapter 2: Organization, Management, and Administration
Section 11: Organization and Administration
Subsection 3: Authority and Responsibility



Policy/Procedure #: 4

Title: Use of Force Resulting in Serious Physical Injury or Death

CALEA Reference#: 11.3.4

I. Policy:

Competent and responsible use of force investigations are critical for maintaining the public's confidence. This is especially true when the police action results in death or serious injury or has significance within the broader community. Due to the implications of such incidents, investigations into the circumstances and facts surrounding such events shall not rely solely on the general criminal investigative process but shall also include administrative procedures to be followed in regards to public information release, investigative authority, and training.

II. Procedure: General

- A.** Any use of force resulting in death or serious physical injury shall trigger the procedures outlined in this policy. Serious physical injury is defined as a disabling mental illness or bodily injury which creates a substantial risk of death, causes serious permanent disfigurement, or causes protracted loss or impairment of the function of the bodily member or organ.
- B.** If there is a question whether injuries qualify as serious physical injury, the Chief of Police or the Investigation Division Commander shall make the final determination.
- C.** In the event of a use of force incident resulting in death or serious physical injury, the following personnel shall be notified:
 - 1. The Chief of Police
 - 2. All Division commanders
 - 3. Peer support supervisor (or specific peer support members)
 - 4. Chaplain (if requested by an involved officer)
 - 5. Department Public information officer (PIO)

III. Procedure: Investigation Types

- A.** Use of Force investigations resulting in death or serious physical injury involve several types of investigations which may include:

1. A criminal investigation of the suspect's actions.
 - (a) The investigation of any criminal conduct by the suspect is controlled by the agency with jurisdiction over the crime that occurred. If crimes have been committed in multiple jurisdictions, identification of the agency controlling the investigation may be reached in the same way as with any other crime where agency capabilities and manpower are factors for consideration. The Investigation Division Commander and the Chief of Police shall be involved in determining the lead agency assigned to investigate when there are multiple jurisdictions involved.
 - (b) If an Urbandale police officer is involved a use of force resulting in death or serious physical injury from an incident within the jurisdictional boundaries of Urbandale, the Chief of Police or designee shall request the Iowa Department of Public Safety Division of Criminal Investigation (DCI) conduct the investigation. The Investigation Division Commander shall assign at least one detective or supervisor to assist the DCI in the criminal investigation of the suspect's actions as a liaison representing the Department in the investigation.
 - (c) Regardless of jurisdiction, when an Urbandale officer is involved in a use of force resulting in death or serious physical injury, the Investigation Division Commander shall assign at least one detective or supervisor as a liaison representing the Department in the investigation to assist the investigating agency in the criminal investigation of the suspect's actions.
2. A criminal investigation of the involved officer's actions.
 - (a) The investigation of the involved officer's actions is controlled by the agency with jurisdiction over the incident that occurred. If the incident involves multiple crimes committed in multiple jurisdictions, identification of the agency controlling the investigation may be reached in the same way as with any other crime where agency capabilities and manpower are factors for consideration.
 - (b) If an Urbandale police officer is involved a use of force resulting in death or serious physical injury from an incident within the jurisdictional boundaries of Urbandale, the Chief of Police or designee shall request the Iowa Department of Public Safety Division of Criminal Investigation (DCI) conduct the investigation. The Investigation Division Commander shall assign at least one detective or supervisor to assist the DCI in the criminal investigation of the officer's actions as a liaison representing the Department in the investigation.
 - (c) Regardless of jurisdiction, when an Urbandale officer is involved in a use of force resulting in death or serious physical injury, the Investigation Division Commander shall assign at least one detective or supervisor as a liaison representing the Department in

the investigation and assist the investigating agency in the criminal investigation of the officer's actions.

- (d) Regardless of jurisdiction, the Chief of Police or designee may request the DCI investigate the incident in regards to the actions of any Urbandale officer.
- 3. An administrative investigation of policy compliance by involved employees.
 - (a) Regardless where the incident occurs, when an officer is involved in a use of force resulting in death or serious physical injury, the administrative investigation will be completed by the Urbandale Police Department.
 - (b) The Internal Affairs Administrator or designee shall investigate the incident to determine policy compliance.
 - (c) The administrative investigation may be delayed by the criminal investigative process. Any delay in the administrative investigation shall be approved by the Chief of Police.
- 4. A civil investigation to determine potential liability.
 - (a) Regardless of where the incident occurs, the City of Urbandale may utilize internal or external investigators, legal counsel, or other liability experts to investigate a use of force incident resulting in death or serious physical injury.
 - (b) The City Manager shall make the decision to conduct any investigation to determine liability exposure for the City.

IV. Procedure: Investigative Process

- A. Command protocol as established in Chapter 2 Section 12.1.2 of the Operations Manual shall apply to the scene of a use of force incident that has resulted in death or serious physical injury. Officers and supervisors directly involved in the incident shall not be considered in the chain of command once able to be relieved by uninvolved personnel. Supervisors directly involved may assist any officer placed in command until additional supervisory staff arrive.
- B. The officer or supervisor in command of the incident shall immediately implement the following:
 - 1. Secure the scene while identifying and mitigating any hazards.
 - 2. Administer and/or request emergency medical attention for any injured parties.
 - 3. Request additional resources from the Department or other agencies.
 - 4. Coordinate a perimeter and if applicable, pursue any known suspects.
 - 5. Evacuate injured parties as quickly and safely as possible.
 - 6. Brief supervisory relief upon arrival.
- C. Upon arrival at the scene, the first uninvolved Urbandale supervisor shall be responsible for coordinating all aspects of the incident until they are relieved by a Division Commander or the Chief of Police. The first uninvolved supervisor shall complete the duties outlined above and also do the following:

1. Take command until relieved by another supervisor or an assigned investigator.
 2. Attempt to obtain a brief overview of the situation from any uninvolved officers. If no uninvolved officers are available a brief overview shall be obtained from one involved officer.
 3. If necessary, the supervisor may order any officer to provide public safety information necessary to secure the scene, identify injured parties, pursue suspects, and ensure the public's safety. The initial on scene supervisor shall not order involved officers to provide any information other than public safety, scene security type information.
 4. If appropriate for officer and public safety, provide information to WestCom for broadcast to affected personnel or agencies. If possible, sensitive information shall be communicated over secure networks.
 5. As soon as practical, remove involved officers from the scene. If feasible, involved officers shall be transported separately. Officers shall be transported to the Urbandale Police Department or other law enforcement agencies if occurring outside of Urbandale.
 - (a) Involved officers shall be ordered not to discuss the incident with other officers pending further direction from a supervisor.
 - (b) If an officer's handgun is taken or left at the scene for evidentiary purposes. Ensure the officer has an assigned officer escort until the handgun can be replaced.
- D. Responsibility of the Patrol Division Commander:
1. If the incident occurred in Urbandale, the Patrol Division Commander shall respond to the scene as soon as practical to coordinate scene security and any other immediate needs.
 2. If occurring outside of Urbandale and involving Patrol Division personnel, the Patrol Division Commander shall respond to the location of the involved officers to offer needed support to the officers and ensure Urbandale policy and procedure are being followed.
 3. Ensure proper manpower is available to cover any scene specific duties as well as maintain call for service response.
- E. Responsibility of the Investigation Division Commander:
1. If the incident occurred in Urbandale, the Investigation Division Commander shall respond to the scene as soon as practical to ensure the investigation of the incident is progressing as required by Urbandale policy and procedure.
 2. Initially, the Investigation Division Commander shall serve as the contact point for DCI investigators. This duty may be delegated to other division personnel after initial contact and coordination has been established.
 3. If occurring outside of Urbandale, the Investigation Division Commander shall respond to the location of the incident to offer support to the investigating agency and ensure Urbandale policy and procedure as well as proper investigative techniques are being utilized.

4. If Investigative Division personnel are involved in the incident, the Investigation Division Commander shall respond or shall assign an uninvolved supervisor to respond to the location of the officers to offer needed support and ensure Urbandale policy and procedures are being followed.

F. Responsibilities of the Support Services Division Commander:

1. If the incident occurred in Urbandale, the Support Services Division Commander shall respond to the location of the involved officers to offer needed support and ensure Urbandale policy and procedure are being followed.
2. Contact division personnel to respond as needed to fill assigned duties such as staying with involved officers, completing emergency contact notifications, etc.
3. If the incident occurred outside of Urbandale and involves Support Services Division personnel, respond to the location of the officers and offer needed support and ensure Urbandale policy and procedures are being followed.
4. If the incident occurred outside of Urbandale and does not involve Support Services Division personnel, contact the commander of the division involved and offer needed support to include manpower, emergency notifications, etc.

V. Procedure: Involved Officers

- A.** Involved officers shall remain separated from other involved officers and shall not discuss the incident with other involved officers prior to providing an interview or a report detailing the incident.
- B.** Any request by an officer for a union representative or a legal representative shall be accommodated.
 1. Due to the need for separation, involved officers will not be permitted to meet collectively with an attorney or union representative prior to providing an interview or report detailing the incident.
 2. Requests for representation by legal or union representatives from officers outside the Department shall be accommodated but referred to the employing agency for direction and coordination.
- C.** Any discussions with a licensed attorney shall be considered privileged attorney- client communication.
- D.** Discussions with peer support personnel or department chaplains shall be considered privileged to the extent provided in Iowa Code 622.10.
- E.** A mental health professional shall be provided by the Department to each involved officer upon request by the officer or the Chief of Police.
 1. Meetings with mental health professionals shall be considered privileged.
 2. A meeting with a mental health professional may take place prior to the officer providing a formal interview or report; however, the restriction of meeting collectively or in a group shall still apply until after providing an interview or a report detailing the incident.

- F. Any officer involved in a use of force resulting in serious physical injury or death shall be given reasonable paid administrative leave.

VI. Procedure: Criminal Investigation

- A. The county attorney's office with jurisdiction over the incident has the authority to conduct an investigation into the circumstances of any use of force involving serious physical injury or death.
- B. As stated above, investigative personnel from the Department shall be assigned to partner with investigators from outside agencies and the county attorney's office to avoid duplicating efforts in related criminal investigations.
- C. Once public safety issues at the scene have been addressed, criminal investigators shall be given the opportunity to obtain a voluntary statement from involved officers and to complete their interviews. The following procedures shall be followed for the involved officer:
 - 1. UPD supervisors and Internal Affairs personnel shall not participate directly in any voluntary interview of involved officers. This will not prohibit UPD supervisors and Internal Affairs personnel from monitoring interviews or providing the criminal investigators with information.
 - 2. If requested, any involved officer shall be afforded the opportunity to consult individually with a representative of his/her choosing or an attorney prior to speaking with criminal investigators; however, in order to maintain the integrity of each involved officer's statement, the officer shall not consult or meet with a representative or an attorney collectively or in groups prior to being interviewed.
 - 3. If any involved officer is physically, emotionally, or otherwise not in a position to provide a voluntary statement, the officer shall be given a reasonable period of time to schedule an alternate time for the interview.
 - 4. Any voluntary statement provided by an involved officer shall be made available for inclusion in any related investigation including administrative investigations.

VII. Procedure: Involved officer Reporting

- A. In the event a suspect(s) remains outstanding or subject to prosecution for related offenses, the Department shall retain the authority to require involved Urbandale officers to provide sufficient information for related criminal reports to facilitate the apprehension and prosecution of those individuals.
- B. While the involved officer may write the report, it is generally recommended such reports be completed by assigned investigators. Under most circumstances, assigned investigators shall interview all involved officers and draft a report based on the interview. Since the purpose of the reports will be to facilitate criminal prosecution, statements of involved officers shall focus on evidence to establish the elements of criminal activities by suspects.

- C. Nothing in this section shall be construed to deprive an involved Urbandale officer of the right to consult with legal counsel prior to completing any such criminal report.
- D. Reports related to the prosecution of criminal suspects will be processed according to normal procedures but shall also be included in the investigation of the use of force.
- E. Officers shall be required to complete the Department use of force reporting form. The review sections of the form shall be completed as outlined in Chapter 1 Section 4.1.1 (Use of Force) in the Operations Manual.

VIII. Procedure: Witness Identification and Interviews

- A. A potential witnesses to a use of force resulting serious physical injury or death may become unavailable or the integrity of their statements compromised with the passage of time; therefore, a supervisor or investigator shall take reasonable steps to utilize available law enforcement personnel for the following:
 - 1. Identification of all persons present at the scene and in the immediate area.
 - 2. When able, a recorded statement shall be obtained from those present during the incident but claiming not to have witnessed anything.
 - 3. Any potential witness who is unwilling or unable to remain available for a formal interview shall not be detained absent reasonable suspicion to detain or probable cause to arrest. Without detaining the individual for the sole purpose of identification, attempts to identify the witness prior to his/her departure shall be made when feasible.
- B. Witnesses who are willing to provide a formal interview shall be asked to meet at a suitable location where criminal investigators may obtain a recorded statement. When necessary, witnesses may be transported by a member of the Department. A written, verbal or recorded statement of consent shall be obtained prior to transporting a witness. If available, the parent or guardian of a witness that is a minor shall consent to the transport.

IX. Procedure: Investigative Personnel

- A. Once notified of a use of force resulting in serious physical injury or death, it shall be the responsibility of the Criminal Investigation Division Commander or designee to assign appropriate personnel to handle the investigation of related crimes. Department investigators shall be assigned to work with attorneys or investigators from the appropriate county attorney's office and may be assigned to separately investigate any related crimes not being investigated by the county attorney's office.
- B. All department reports on the incident shall be forwarded to the Criminal Investigation Division Commander or designee for approval. Any administrative reports shall be forwarded to the Internal Affairs Administrator or designee coordinating the administrative investigation for approval and filing.

X. Procedure: Administrative Investigation:

- A. In addition to all other investigations associated with a use of force resulting in serious physical injury or death, the Department will conduct an internal administrative investigation of involved Urbandale officers to determine conformance with department policy. The investigation shall be classified as an internal affairs investigation and conducted by the Internal Affairs Administrator or designee as established in Chapter 6 Section 52.2.1 (Complaint Procedure) of the Operations Manual.
- B. Administrative investigations shall be completed as soon as practical but may be delayed to ensure they do not interfere with any ongoing criminal investigation. Any delay shall be approved by the Chief of Police.
- C. All interviews conducted shall be subject to department policies and applicable laws.
- D. If any officer has voluntarily elected to provide a statement to criminal investigators, the assigned administrative investigator shall review the statement before proceeding with any further interview of that involved officer. The involved officer shall be provided with a copy of his/her prior statement before proceeding with any subsequent interviews.
- E. In the event that an involved officer has elected not to provide criminal investigators with a voluntary statement, the assigned administrative investigator shall conduct an administrative interview to determine all relevant information.
 - 1. Although this interview should not be unreasonably delayed, care should be taken to ensure that the officer's physical and psychological needs have been addressed before commencing the interview.
 - 2. If requested, the officer shall have the opportunity to select an uninvolved representative to be present during the interview; however, in order to maintain the integrity of each individual officer's statement, involved officers shall not consult or meet with a representative collectively or in groups prior to being interviewed.
 - 3. The officer shall be informed of the nature of the investigation and ordered to provide full and truthful answers to all questions. The officer shall be informed that the interview will be for administrative purposes only and that the statement cannot be used criminally.
 - 4. Internal Affairs Administrator shall compile all relevant information and reports necessary for the Department to determine compliance with applicable policies.

XI. Procedure: Civil Liability

- A. A supervisor or investigator for the Department may be assigned to work exclusively under the direction of the legal counsel for the Department to assist in the preparation of materials deemed necessary in anticipation of potential civil litigation.
- B. All materials generated in this capacity shall be considered attorney work product and may not be used for any other purpose. The civil liability response is not intended to interfere with any other investigation but shall be given reasonable access to all other investigations.

XII. Procedure: Audio and video recordings

- A. Any officer involved in a use of force resulting in serious physical injury or death may be permitted to review available in-car video, body-worn video, or other video or audio recordings prior to providing a recorded statement or completing reports.
- B. Any in car video, body-worn video, and other known video or audio recordings of an incident shall not be publicly released during an ongoing investigation without consulting the prosecuting attorney. The Chief of Police or designee shall determine if audio or video of the incident controlled by the Department will be released.

XIII. Procedure: Debriefings

- A. Under most circumstances, a critical incident stress debriefing as well as other services such as peer support as outlined in Chapter 3 Section 22.1.1 (Compensation & Benefits) of the Operations Manual shall occur as soon as practicable. The Support Services Division Commander shall be responsible for organizing the debriefing.
- B. The debriefing is not part of any investigative process. Care should be taken not to release or repeat any communication made during a debriefing unless otherwise authorized by policy, law or a valid court order.
- C. Attendance at the debriefing shall only include those members of the Department directly involved in the incident, which can include support personnel (e.g., dispatchers, civilian personnel). Other support personnel may attend with the concurrence of those involved in the incident.
- D. A tactical debriefing shall take place to identify any training or areas of policy that need improvement. The Chief of Police shall identify the appropriate participants. Unless deemed necessary due to immediate officer or public safety concerns, the debriefing shall not be conducted until the criminal and administrative investigations have been completed.

XIV. Procedure: Media Relations

- A. Any media release related to a police action death investigation shall be prepared with input from the Chief of Police or designee. When possible, media releases shall be coordinated with other involved organizations as established in Chapter 6 Section 54.1.1 (Public Information & Social Media Use) in the Operations Manual.
- B. No officer shall make any comment to the media unless they are authorized by the Chief of Police or a Division Commander.
- C. Department members receiving inquiries regarding use of force resulting in serious physical injury or death occurring in other jurisdictions shall not make any public comment and will direct the inquiries to the agency having jurisdiction and primary responsibility for the investigation.

XV. Procedure: Training

- A. Process training will be conducted for Department personnel responsible for managing such incidents.
 - B. Awareness training will be conducted for all Department personnel potentially impacted.

Chapter 2: Organization, Management and Administration
Section 11: Organization and Administration
Subsection 4: General Management and Administration



Policy/Procedure #: 1

Title: Administrative Reporting

CALEA Reference#: 11.4.1, 11.4.3

I. Policy: Administrative Reporting

A policy is established to provide the Urbandale Police Department with guidelines to ensure a uniform administrative reporting system establishes an efficient and accurate flow of information. A properly functioning reporting system provides department managers information regarding agency activities in a timely manner. An administrative reporting system shall establish purpose, frequency, and accountability of all departmental reports, reviews, and activities. An administrative reporting system shall provide information regarding performance of the department and all its components. All applicable reports, reviews, and activities mandated by CALEA accreditation standards shall be included in the administrative reporting system.

II. Procedure: Administrative Reporting System

- A.** A comprehensive list of all agency reports, reviews, and activities including any required by CALEA accreditation standards shall be maintained by the support services division. The list shall include the following:
 - 1. Name of the report, review or activity
 - 2. Person or position responsible for formulation
 - 3. Purpose
 - 4. Frequency
 - 5. Distribution
- B.** The chief of police or designee shall determine the person or position responsible for the formation of a report, review, or activity. All reports, reviews, and activities shall be completed in the time frame allocated by the chief of police and in compliance with any applicable CALEA standards. Failure to comply with the requirements established by the

administrative reporting system shall be the responsibility of the person or position assigned the task by the chief of police.

- C.** The support service division shall manage all reports, reviews, and activities needed to satisfy CALEA accreditation standards. The support services division may use the comprehensive list of agency reports, reviews, activities, Power DMS software, and any other available means to determine all reports, reviews, and activities are completed as needed.
- D.** In the event a report, review, or activity is not completed as scheduled, the support services division shall notify the person required to submit the respective work and request it be submitted within 10 working days. If the activity, report or review is not completed within 10 working days, the support services captain shall notify the direct supervisor of the person responsible for the report, review, or activity. The supervisor may grant an extension for the report, review, or activity to be completed and submitted or may take other action, including disciplinary action, as deemed appropriate.

Chapter 2: Organization, Management and Administration
Section 11: Organization and Administration
Subsection 4: General Management and Administration



Policy/Procedure #: 2
Title: Agency Forms
CALEA Reference#: 11.4.2

I. Policy: Agency Forms

A policy is established to develop, modify, approve, review and purge all agency forms. The policy shall standardize department forms in appearance and functionality. By controlling agency forms, the department shall realize and increase efficiency by reducing redundancy of information and avoiding duplication of effort. Employees are encouraged to develop new forms and recommend revisions and improvements to existing forms to enhance the efficiency and productivity of the department.

II. Procedure: Control

- A.** The office of the chief of police shall have control over all agency forms. If the form is part of the police records management system the appropriate software vendor shall control the forms with input from the department.
- B.** Forms used by the Urbandale Police Department shall have an assigned name, version number, revision date or date of implementation. The revision date shall be the date the form is placed into service. When part of the police records management system, the form shall be exempt as the programming will include the version number and revision dates.
- C.** A master list of all forms used by the Urbandale Police Department shall be maintained by the office of the chief of police. The list shall include form name, version number, revision date or date of implementation.
- D.** The chief of police or designee shall approve all forms for use at the Urbandale Police Department.
- E.** The division commanders shall ensure only current and approved forms are utilized. Division commanders shall ensure any forms needed in their division are included on the master list of forms and are available for use.

III. Procedure: Development, modification, Purging, Approval

- A.** When the need is identified to create, revise, or purge a form, the following procedure will be followed:
 - 1.** Employees shall utilize the chain of command to notify the division commander of their respective division explaining the need.

2. The captain shall conduct a needs assessment, including an examination of current forms, to determine the best course of action to include form development, revision, or purging. When the division commander feels there is a need for a new form, revision of an existing form, or purging of an existing form, they shall bring the form adoption, revision, or purging as a topic of discussion at a command staff meeting. At the conclusion of discussion, the chief of police shall approve or deny the creation, revision, or purging of a form.
 3. When creation, revision, or purging of a form is denied by the chief of police, the division commander of the employee making the original request shall ensure the employee is informed and the denial explained.
 4. When the creation, revision or purging of a form is approved by the chief of police, the division commander or designee shall meet with the administrative specialist assigned to the office of the chief of police for formatting or purging. If the form is part of the police records management system, the appropriate software vendor shall be included in any formatting or purging discussion as to the capability of making the changes with current software.
 5. When a form has been approved by the chief of police for purging, the administrative specialist assigned to the office of the chief of police shall remove the form from the police production server. Any paper copies shall also be removed. If the form is part of the police records management system, the appropriate vendor shall remove the form from the appropriate program.
 6. When a form is new or revised, the administrative specialist assigned to the office of the chief of police shall submit the final draft to the chief of police for approval. If the form is part of the police records management system, the appropriate software vendor shall assist in presenting the final draft to the chief of police for approval.
 7. Once a form has been approved by the chief of police it shall be implemented. The completion of the process will require that any new form is assigned an Urbandale Police Department form name, version number and implementation date. Any revised form shall be assigned a new version number and revision date.
- B.** When possible, all new and revised forms approved for use shall be placed in the police production server in a location known to all employees. All forms shall be consistently formatted and compatible to the records management system of the Urbandale Police Department.
- C.** When a form involves a legal issue, the chief of police may request the form be reviewed by legal counsel prior to implementation.

IV. Procedure: Outside Agency Forms

- A.** Forms developed outside the department may have associated instructions detailing their use. These instructions may be adopted or modified in order to meet the needs of the Urbandale Police Department.

- B.** The office of the chief of police shall be identified as the controlling division regarding the use of forms developed by other departments, agencies, or levels of government outside the Urbandale Police Department.

V. Procedure: Review

- A.** The administrative specialist assigned to the office of the chief of police shall review and evaluate each department form with the respective division commanders as needed.
- B.** The review and evaluation shall ensure that each form fulfills its intended purpose, is not duplicated and is sufficiently useful to warrant continuance.
- C.** The chief of police may order periodic reviews of department forms for the purpose of recommending adoption, revision, or elimination of forms.

Chapter 2: Organization, Management and Administration
Section 11: Organization and Administration
Subsection 4: General Management and Administration



Policy/Procedure #: 4

Title: Computer Software and Usage Requirements

CALEA Reference#: 11.4.4, 41.3.7

I. Policy: Computer Software Restrictions

A policy is established to govern the use of department computers and the introduction of data files, software, applications, data storage devices, or programs into agency controlled computer systems. The policy shall address security issues as well as a procedure to gain approval to add legitimate data files, software, applications data storage devices, or programs needed for departmental use. Proper use of approved data files, software, data storage devices, applications or programs shall also address licensing restrictions.

II. Procedure: Security

- A.** All data files, software, applications, data storage devices, or programs used by the Department will be maintained by the City of Urbandale Information Technology Department (City IT). This maintenance generally will include control of software distribution, tracking of license usage, security maintenance, and periodic backup of application produced data.
- B.** Except where noted below, no data files, software, applications, data storage devices, or programs shall be installed, downloaded, or utilized on department owned computers, laptops or cell phones without the permission of the Chief of Police, a division commander, or City IT.
- C.** All department computers shall have sufficient security features to restrict access to only authorized users. Security features shall restrict the ability to install data files, software, applications or programs on a department computer to City IT.
- D.** Except personal work files, an employee must never add, alter, copy, or delete data files, software applications, data storage devices, or programs from any department computer system without proper authorization from a division commander, the Chief of Police, or City IT. Examples of personal work files include various word processing and spread sheet data or

database files the employee uses as part of their maintenance responsibilities.

- E. Security relating to criminal justice information services is addressed in Chapter 9 section 81.1.1(Communications) of the Operations Manual.

III. Procedure: Software Approval

- A. Except where noted below, without prior authorization from a division commander, the Chief of Police or City IT, it shall be prohibited to install data files, software applications, data storage devices, or programs on any department owned mobile, desktop, or handheld computer. This specifically includes the downloading of software from the internet.
- B. Without proper authorization from a division commander, the Chief of Police or City IT, it shall also be prohibited to manipulate or alter current software running on department owned mobile, desktop, or handheld computers.
- C. Except where noted below, when an employee needs data files, software applications, data storage devices, or programs installed or altered on a department owned computer, they shall submit a repair/service request form to the Support Services Division detailing the request. Prior to submission, the repair/service request must be approved by the employee's division commander. Support Services Division shall contact City IT and inform them of the request. City IT shall review the request and if no issues exist, install the program or make the alteration. If City IT denies the request, a reason shall be supplied to the appropriate division commander and forwarded to the employee. If not satisfied with the outcome, the employee shall consult their chain of command for resolution through the Chief of Police. This procedure does not apply to any installation or upgrade of the computer systems provided by City IT.
- D. Due to the numerous amount of software applications and programs needed to perform a forensic examination of a computer, the department's forensic computer examiner shall be exempt from the approval process stated above for any equipment used in the forensic examination process.
- E. Employees must receive approval from the Chief of Police prior to any data files, software applications, data storage devices, or programs being purchased in which the department will incur a cost.
- F. Any approved data files, software applications, data storage devices, or programs utilized by the department shall be maintained and stored by City IT. If applicable, this shall include the original data disks, license agreement, and other documentation.
- G. The department shall abide by all licensing agreements of utilized data files, software applications, data storage devices, or programs. City IT shall assist the department in meeting licensing requirements.
- H. Data storage devices may be utilized and maintained by employees to store or move data. Prior to installing data storage device on any

department owned device, the employee must be confident the data storage device does not contain any files that could potentially harm the department's computer systems. If an employee is unsure of the contents on a data storage device, they shall consult City IT before use. Use includes the act of plugging the data storage device into a department owned computer system or device.

IV. Procedure: Computer Use

- A.** City of Urbandale owned mobile, desktop, or handheld computers are intended to facilitate department operations and are city property. Employees shall utilize mobile, desktop, or handheld computers in accordance with all department and City of Urbandale policies.
- B.** Mobile, desktop, or handheld computers shall be used by employees in the performance of their job duties for the following purposes:
 - 1. Run all functions of the Iowa/NCIC data base through the Shield Software System.
 - 2. Electronic communications.
 - 3. Computer Aided Dispatch
 - 4. Facilitate the completion of department reports
 - 5. Provide needed or required information within the department
 - 6. Provide needed or required information to outside agencies or the public.
 - 7. Access and operate various approved software applications.
 - 8. Additional uses may be approved at the discretion of the Chief of Police or City IT.
- C.** Only department employees or City IT shall be authorized to utilize department owned mobile, desktop, or handheld computers. Each employee shall be granted access based on the functional responsibilities of their position. Reserve officers, interns, and chaplains may be granted limited access based on the needs of their position as determined by the Chief of Police or a division commander. Any verification, certification, or training requirements shall be met prior to granting access (e.g. Iowa/NCIC system).
- D.** Any usernames and passwords for utilizing department owned mobile, desktop, or handheld computers shall be kept confidential and not shared with unauthorized persons.
- E.** Employees shall adhere to all rules and regulations regarding access and dissemination of information in the Iowa/NCIC system.
- F.** Outside of the Urbandale Police Department building, the physical security of all department owned mobile, desktop, or handheld computers shall be the responsibility of the employee assigned the device.
- G.** All transmissions from department owned mobile, desktop, or handheld computers may be reviewed by a supervisor as part of a complaint investigation or as a means to review the productivity of an employee. If

there is a need to utilize City IT to retrieve the transmissions or data, prior approval of the Chief of Police or designee shall be obtained.

V. Procedure: Wireless Handheld Device Security

- A.** The department shall follow the below procedures for securing physical devices capable of accessing the Iowa/NCIC computer data bases through the Shield Software system.
 - 1.** Each shield system enabled wireless device will be labeled with the owning agency's name, address, and phone number. This will assist in their returning if lost.
 - 2.** All shield system enabled wireless devices shall be secured from unauthorized access when not in use.
- B.** Any shield system enabled wireless devices which is misplaced or lost must be reported to an employee's direct supervisor immediately. As soon as possible the device will be "locked out" from the shield system and be unable to complete Iowa or NCIC system queries.
- C.** Any department employee holding valid certification with the State of Iowa shall be authorized to use shield system enabled wireless devices.
- D.** The password for shield system enabled wireless devices shall follow the rules defined in the U.S. Department of Justice CJIS Security Policy. The user of the device shall be responsible for maintaining the password standards listed below:
 - 1.** Password minimum length is 8 characters.
 - 2.** Password must contain alphanumeric and special characters.
 - 3.** Password must be changed at a minimum of every ninety (90) days.
 - 4.** Password can be reused every tenth (10th) change.
- E.** City IT shall be responsible for "locking out" any shield enabled wireless device as deemed necessary by any department supervisor.

Chapter 2: Organization, Management, and Administration
Section 11: Organization and Administration
Subsection 5: Temporary/Rotating Assignments



Policy/Procedure #: 1

Title: Temporary, Specialized, and Collateral Duty Assignments

CALEA Reference#: 11.5.1

I. POLICY: Assignments

The Urbandale Police Department utilizes temporary assignments, specialized assignments, and collateral duty assignments to address specific conditions or problems in the community or within the Department. Periodic reviews of these positions and the conditions that lead to their creation shall be conducted. Selection for the temporary, specialized, and collateral duty assignments shall be standardized and should include the announcement of an opening, length of the assignment, eligibility, application process and criteria for selection.

II. PROCEDURE: Temporary Assignment

- A.** The Chief of Police may utilize a temporary assignment of personnel to handle specific conditions in the community or within the Department. Temporary assignments shall be one year or less in duration unless extended by the Chief of Police. Once assigned, the temporary assignment shall be the employee's primary responsibility.
- B.** The Chief of Police, through review of allocation of personnel reports, workload assessments, specialized assignment reviews, requests from command staff, and other documentation shall determine the need for temporary assignments.
- C.** When a temporary assignment is needed, the command staff shall review all qualified personnel and offer recommendations based on current workload assessments, experience, knowledge, skills, and any other factor deemed relevant during a commanders meeting. The meeting minutes shall document the selection process. Once completed, the Chief of Police shall allocate personnel to the mission. The selection shall be announced to the Department by personnel order including the expected duration of the temporary assignment. Any extension of the temporary

assignment beyond the original estimate shall be made by personnel order.

- D. Positions available for temporary assignment shall include all sworn positions and specialized assignment positions within the Department.

III. PROCEDURE: Specialized Assignments

- A. The Department shall designate particular assignments as specialized assignments. Specialized assignments shall be positions within the department that require specific skills or abilities beyond the requirements of a uniformed patrol officer. Once assigned, specialized assignments shall be the employee's primary responsibility.
- B. When a specialized assignment becomes vacant, a notice shall be sent to all employees in the Department. The notice shall include details of the specialized assignment such as length of assignment, eligibility, criteria for selection and instructions on how to apply. The notice shall be made on command staff memorandum from the Chief of Police or designee.
- C. The minimum qualification for a specialized assignment shall be two years of service with the Urbandale Police Department by the date established in the notice. The minimum qualifications for specialized assignments shall remain stable; however, changes in qualifications may be made if based on valid justification. Additional qualification requirements may be required for some specialized assignments. The additional requirements shall be clearly stated in the notice.
- D. After being transferred from a specialized assignment, an employee may not apply for that specific specialized assignment for one year from the last date worked in the assignment.
- E. Specialized assignment positions shall be designated as rotating or non-rotating by the Chief of Police. The intent of non-rotating positions is to retain valuable training and experience within a division for a longer period of time. The intent of rotating positions is to offer job diversity, training, and career development opportunities to a greater number of employees while strengthening the overall organization.
 - 1. Employees selected for non-rotating positions shall serve in the specialized assignment with no set time limit. The Chief of Police may reassign an employee from a non-rotating position at any time. Reasons for removal from a non-rotating position include but are not limited to the following:
 - a. Poor job performance
 - b. Needs of the Department
 - c. Discipline related issues
 - d. Request by the employee to be reassigned
 - e. Promotion
 - 2. Employees selected for rotating positions shall serve in the specialized assignment for a period of three (3) years. The Chief of Police may reassign an employee from a rotating position at any time. Reasons for removal from a rotating position include but are not limited to the following:

- a. Poor job performance
 - b. Needs of the Department
 - c. Discipline related issues
 - d. Request by the employee to be reassigned
 - e. Promotion
- 3. An exception to the three (3) year rotation may be made by the Chief of Police. The reasons for the exception include but are not limited to the following:
 - a. No other qualified employee is interested in the position
 - b. Interested employees are not eligible based on tenure in the Department, poor performance in their current duties, discipline related issues, or other indicators the employee is not a good fit for the position as determined by the Chief of Police with input from other staff members.
 - c. A special project or event needs to be completed by the employee currently assigned.
 - d. Other special circumstance as determined by the Chief of Police.
- F. When the Chief of Police determines an employee will no longer be assigned to a specialized assignment, they will be reassigned by the issuance of a personnel order. The personnel order shall include where and when the employee is to be reassigned.
- G. Specialized assignments for the Department include but are not limited to the following:
 - 1. Investigator
 - 2. Narcotics Investigator (MINE)
 - 3. School Resource Officer
 - 4. Community Relations Officer
 - 5. Canine Officer
 - 6. Crisis Intervention Team Officer

IV. Procedure: Selection for Specialized Assignment

- A. Employees pursuing a specialized assignment must submit a memorandum expressing interest by the deadline established on the notice. The memorandum may also contain the employee's knowledge, skills and abilities that have prepared them for the assignment. This would include any prior specialized assignments, temporary assignments or collateral duties in which the employee has participated.
- B. A panel of three (3) supervisory staff appointed by the Chief of Police shall be assembled to conduct an interview of the applicant list.
- C. The number of questions and the scoring procedures for the interview process shall be determined based on the position being filled. The details, such as number of questions and scoring method, shall be established prior to testing for the specialized position.
- D. Upon completion of the interview process, the panel shall submit a command staff memorandum to the Chief of Police with the scores from the interview process. Although not required, the panel may also recommend an officer or officers for the specialized assignment.

- E. At the completion of the interview process, the Chief of Police and the division commander with responsibility over the specialized assignment shall review the interview results, overall job performance, educational background, ability to perform the specialized assignment, collateral duties, teamwork, cooperation with coworkers and supervisory staff, and experience in making a selection to fill the specialized assignment. Longevity shall only be considered if there is a need to separate two employees.
- F. Upon completion of the review with the division commander, the Chief of Police shall select an employee to fill the position.
- G. Selections for specialized positions shall be announced to the Department by personnel order. An effort shall be made to notify officers that participated in interviews for the position prior to notifying the remainder of the Department.

V. PROCEDURE: Collateral duty Assignments

- A. Collateral duty assignment shall be any assignment which is secondary or subordinate in nature to the officer's primary assignment. Specialized training is generally required to improve the officer's proficiency in performing the duties and responsibilities of the assignment.
- B. When assignment of a collateral duty is needed, the notice shall be sent to all employees in the Department. The notice shall include details of the collateral duty to include eligibility, criteria for selection and instructions on how to apply. The notice shall be made on command staff memorandum from the Chief of Police or designee.
- C. Additional requirements may be required for some collateral duty assignments. The additional requirements shall be clearly stated in the notice.
- D. The command staff shall review all qualified applicants and offer recommendations. After review, the Chief of Police shall select an employee from the list of qualified applicants to fill the collateral duty assignment. The selection shall be announced to the Department by command staff memorandum.
- E. The Chief of Police or a designee may assign any officer at any time to a collateral duty position based on the needs of the Department.
- F. Evaluations of employee's collateral duty assignments shall be included in the employee's annual performance evaluation. Evaluation of the collateral duty may include the following information:
 - 1. Performance in the collateral duty
 - 2. Workload specifically related to the collateral duty (i.e. percentage of overall duties, hours required to complete the duty daily, monthly, yearly).
 - 3. Any needed training or recertification.
- G. Supervisors conducting an evaluation of an employee's collateral duty shall consult the supervisor managing the collateral duty for the Department for input.

- H. The Chief of Police may remove an employee from a collateral duty at any time. Reasons for removal from a collateral duty position include but are not limited to the following:
 - 1. Poor job performance
 - 2. Needs of the Department
 - 3. Discipline related issues
 - 4. Request by the employee to be reassigned
 - 5. Promotion
- I. When the Chief of Police determines an employee will no longer perform a collateral duty assignment. The division commander shall notify the employee. The notice should include the date in which the employee is no longer responsible for the collateral duty assignment.
- J. Collateral duty assignments for the Department include but are not limited to the following:
 - 1. All certified instructor positions
 - 2. Firearms armorer
 - 3. S.E.R.T.
 - 4. Crime scene investigator
 - 5. Honor guard
 - 6. Bicycle officer
 - 7. Field training officer
 - 8. Drug recognition officer
 - 9. Accident investigator
 - 10. Peer Support Team member
 - 11. Peer Fitness Trainer
 - 12. Drone operator

VI. Procedure: General

- A. An employee may make a request to the Chief of Police to no longer perform a temporary assignment, specialized assignment, or collateral duty. Based on the nature of the assignment/duty and the needs of the Department, employees may be required to continue to perform the assignment/duty due to a lack of interest from other Department personnel or until replacement personnel are selected and trained. The Department will make efforts to grant a change in temporary assignments, specialized assignments, and collateral duties but reserves the right to assign employees to specific work responsibilities.
- B. Supervisory and civilian personnel shall not participate in the selection procedures for temporary assignments, specialized assignments, or collateral duties. Supervisory and civilian personnel shall be assigned work duties at the discretion of the Chief of Police based on the needs of the Department.

Chapter 2: Organization, Management and Administration
Section 12: Direction
Subsection 1: Direction



Policy/Procedure#: 2

Title: Command Protocol

CALEA Reference: 12.1.2

- I. A policy is established to direct the Urbandale Police Department in command protocol during various situations. The chief of police shall appoint a ranking position to act in his capacity during his absence. Any individual appointed shall have the authority to act on behalf of the chief of police and carry out daily activities of the department.
- II. **Procedure: Absence of Chief of Police**
 - A. In the absence of the chief of police the highest ranking captain will be in command and have the ability to act on behalf of the chief of police. The highest ranking captain will be determined by seniority of service in grade.
 - B. If the chief of police and all of the captains are absent, the highest ranking sergeant will be in command and have the ability to act on behalf of the chief of police. The highest ranking sergeant shall be determined by seniority of service in grade.
 - C. The chief of police may designate a specific officer to be in charge during any planned absence.
 - D. This policy and procedure in no way encroaches on the power of the city manager of the City of Urbandale to appoint an acting chief of police (Whenever the chief of police is out of the city or unable to act on account of sickness or for any other reason, the city manager has the power to name an acting chief of police. City Ordinance 33.20)
- III. **Procedure: Exceptional Situations**
 - A. In the event of an exceptional situation, the senior officer on the scene, determined by seniority of service in grade, shall be in command.
 - B. If an officer has assumed command of an exceptional situation, he/she shall remain in command until relieved by a sergeant, captain, or the chief of police.
- IV. **Procedure: Personnel from Different Divisions**
 - A. In incidents involving two or more divisions, the ranking officer from the division with authority over the incident shall be in command.

- B.** In incidents involving two or more divisions where the authority over the incident is not clearly defined by written directive, the highest ranking officer shall be in command.
- C.** If no sergeant, captain, or the chief of police is present, the highest ranking officer shall be in command.
- D.** The highest ranking officer shall be determined by seniority of service in grade.

V. Procedure: Normal Operations

- A.** Command protocol shall follow the chain of command during normal operations. The chain of command shall be in descending order:
 - 1.** Chief of police
 - 2.** Captain
 - 3.** Sergeant
 - 4.** Officer
- B.** During normal operations, if two officers are of equal rank, the officer with seniority of service in grade shall be designated as the higher ranking officer.

Chapter 2: Organization, Management and Administration
Section 12: Direction
Subsection 1: Direction



Rule and Regulation #:3
Title: Lawful Orders
CALEA Reference: 12.1.3

I. Lawful Order

Employees shall promptly obey any lawful order of a superior. This shall include orders relayed from a superior by an employee of the same or lesser rank or classification.

II. Conflicting Order

Employees who are given an otherwise proper order which is in conflict with a previous order, manual, or written directive shall respectfully inform the superior issuing the order of the conflict. If the superior issuing the order does not alter or retract the conflicting order, the order shall stand. Under these circumstances, the responsibility shall be on the superior. Employees shall obey the conflicting order and shall not be held responsible for disobedience of the previously issued order, manual, or written directive.

III. Unlawful Order

Employees shall not obey any order which they reasonably believe would require them to commit any illegal, immoral, or unethical act. If in doubt as to the legal, moral, or ethical status of the order, employees shall respectfully request the issuing employee to clarify the order or confer with higher authority.

Chapter 2: Organization, Management and Administration
Section 12: Direction
Subsection 1: Direction



Policy/Procedure#: 4

Title: Communication, Coordination and Cooperation

CALEA Reference#:12.1.4

- I. **Policy: Communication, Coordination and Cooperation**
A policy is established to ensure the communication, coordination and cooperation among all divisions and all levels within the Urbandale Police Department. The exchange of information is the cornerstones of efficient and effective police services increasing departmental awareness of problem areas and assist in formulating solutions to those problems.
- II. **Procedure: Communication Conducted by Supervisory Personnel**
 - A. Meetings shall be used to exchange information, provide a forum to present ideas, discuss problems, promote positive rapport between divisions, evaluate programs and performance, coordinate assignments across the divisions and throughout the Department, and foster cooperation between the divisions through open discussion and planning. Meeting formats are discretionary and are generally structured in a manner that is appropriate to the personnel involved. A pre-planned and prepared agenda should be distributed to all meeting attendees twenty-four (24) hours in advance of the meeting. Agenda distribution is not necessary if the meeting is called to address emergency or unusual situations. Minutes shall be prepared for all meetings outlined in this policy. Upon request, minutes from previous meetings shall be available at subsequent meetings to provide continuity to the informational process. If situations arise that impact the scheduling of a particular meeting, the staff person that called the meeting may cancel or reschedule. Supervisors shall be responsible for the dissemination of relevant material discussed in meetings to the employees they supervise.
 - B. The following meetings shall be held:
 1. Command Staff Meetings: Command staff meetings shall be called by the Chief of Police or designee. Command staff meetings shall include the Chief of Police, captains, and the Chief's administrative specialist. The Chief of Police or designee, may have additional

personnel attend a command staff meeting. Command staff meetings shall generally be held weekly and may discuss the following items:

- a. Major calls for service/cases
 - b. Captains items
 - c. Police schools
 - d. Open discussion
2. Staff Meetings: Staff meetings shall be called by the Chief of Police or designee. Staff meetings shall include the Chief of Police, captains, sergeants, any civilian supervisors, and the Chief's administrative specialist. The Chief of Police, or his designee, may have additional personnel attend a staff meeting. Staff meetings shall generally be held every other month and may discuss the following items:
- a. Crime analysis
 - b. Patrol Division
 - c. Investigation Division
 - d. Support Services Division
 - e. Office of Chief of Police
 - f. Open discussion
3. Divisional Staff Meetings: Divisional staff meetings shall be called by the captain of the division or designee. Divisional staff meetings shall include captains and sergeants from a particular division. If needed, an administrative specialist or technician may attend to keep the minutes; however, meeting minutes are not required. The captain or designee may have additional personnel attend a divisional staff meeting including all personnel from the division. Divisional staff meetings shall occur as needed by the division and may discuss the following items:
- a. Policies and procedures
 - b. Crime analysis and crime prevention
 - c. Cases of interest to the division
 - d. Awards and commendations
 - e. Personnel
 - f. Open discussion

III. Procedure: Other Forms of Communication

- A. The exchange of information between the divisions is vital to the success of the Urbandale Police Department; therefore, it is important that other means are established to facilitate this exchange. Information exchange may include written, oral, and electronic communications. Information exchange may be accomplished in many ways to include criminal investigation division daily case review, patrol shift briefings, administrative reports, criminal intelligence bulletins, formal and informal debriefings, bulletin board postings, e-mails, voicemail, small group or one

to one conversations and other means as may be deemed appropriate to augment the exchange of information.

- B.** Detectives shall periodically attend patrol division shift briefings and patrol officers shall occasionally attend criminal investigation division daily case reviews to facilitate the exchange information and keep communication lines open. The exchange of information may include ongoing investigations, wanted persons, criminal intelligence, vehicles, crime trends, potential dangers, and certain criminal modes of operations.
- C.** Other division staffs are encouraged to have their personnel attend patrol division shift briefings and criminal investigation division daily case reviews to exchange information and open lines of communication.

IV. Procedure: Coordination

- A.** Coordination of divisional response to incidents is critical to success. When an incident requires the response of more than one division, it is imperative that supervisors coordinate their response.
- B.** Supervisors from each division responding to an incident shall keep other supervisors apprised of any developments. Example: The Investigation Division is utilizing patrol to secure a scene until a warrant is obtained. The investigations supervisor shall keep the patrol supervisor apprised of how long patrol resources will be required.
- C.** If manpower or resources from another division may be required to respond to an incident, as much advanced notice as possible shall be given. Example: The Investigation Division will be serving a warrant and will be requesting patrol assistance for transport or uniform presence.
- D.** Special events plans as established in Chapter 5 Section 46.2.7 of the Operations Manual shall be distributed as soon as practical to allow enough time for divisional supervisors to plan resource allocation.

V. Procedure: Cooperation

- A.** All divisions within the Department shall cooperate with each other to accomplish the Department's mission.
- B.** Disagreements between the divisions as to task responsibility shall be resolved at the lowest supervisory level possible. At no time shall the safety of the public or officers be jeopardized due to a lack of cooperation between the divisions in the Department.
- C.** If it is unclear who has responsibility for a task, supervisors shall commit the resources necessary to complete the task. If needed, responsibility for the task can be determined at a later time by division commanders or the Chief of Police.

Chapter 2: Organization, Management and Administration
Section 12: Direction
Subsection 2: Written Directives



Policy/Procedure: 1

Title: Written Directive System and Issuing Authority

CALEA Reference: 12.2.1

- I. Policy: Written Directive System and Issuing Authority**

A written directive system is established to provide reasonable guidelines for police department employees to follow in the discharge of their duties. The Chief of Police or designee shall have the authority to issue, modify, approve, or rescind all written directives.
- II. Procedure: Types of Written Directives and the Authority to Issue**
 - A. Policy:** A policy is a written directive that is a broad statement of agency principles. Policy statements may be characterized by such words as "may" or "should" and usually do not establish fixed rules or set procedures for conduct of a particular activity but rather provide a framework for development of procedures and rules and regulations. Policy shall be issued by the Chief of Police or designee.
 - B. Procedure:** A procedure is a written directive providing a step by step guide to carry out the duties and responsibilities of the Police Department and its sub-units. A procedure may be made mandatory in the tone through the use of "shall" rather than "should" or "must" rather than "may". Procedures sometimes allow latitude and discretion in carrying out an activity. Procedures shall be issued by the Chief of Police or designee.
 - C. Rules and regulations:** Rules and regulations are written directives that establish a set of specific guidelines to which all employees must adhere. Rules and regulations shall be issued by the Chief of Police or designee.
 - D. Departmental general orders:** A departmental general order is a written directive to all department personnel for the purpose of announcing the adoption, purging, or revision of a written directive. Departmental general orders shall be issued by the Chief of Police or designee. Appropriate topics for general orders include but are not limited to:
 1. Rules of conduct.
 2. Establish permanent procedures, policies, and manuals related thereto. Examples: Investigative procedures, procedures relating to arrests, persons in custody, and permanent changes in the organization.

3. Installation of permanent programs which affect more than one unit.
 4. Permanent personnel policies and procedures including: rules of recruiting, hiring, training and promotion policies, but not including changes of status, such as transfers, promotion of individuals, etc.
 5. Use of public facilities, equipment or expenditure of public funds.
 6. Relationships with other agencies and citizens.
- E.** Divisional general orders: A divisional general order is a written directive to personnel assigned to a specific division for the purpose of announcing the adoption, purging, or revision of a written directive applicable only to a specific division. Divisional general orders shall be issued by the Chief of Police, a division commander, or designee. Appropriate topics for divisional general orders include but are not limited to:
1. Rules of conduct by a specific division.
 2. Use of public facilities and equipment by a specific division.
 3. Relationships with other agencies and citizens by a specific division.
- F.** Personnel order: A personnel order is a written directive that announces a change in the status of personnel. Personnel orders shall be issued by the Chief of Police or designee. Examples include, but not limited to:
1. The appointment of new personnel.
 2. The assignment or transfer of personnel.
 3. Termination by resignation or retirement
 4. Changes in employee assignments, absences, or other temporary changes employee assignments.
- G.** Special order: A special order is a written directive that affects only a specific segment of the organization or a statement of policy and procedure regarding a specific circumstance or event that is temporary in nature. Special orders shall be issued by the Chief of Police, division commanders, or designee.
- H.** Command staff memorandum: A command staff memorandum is a written directive that may or may not convey an order. It is generally used to clarify, inform, and inquire. Command staff memorandums are issued by the chief of police, division commanders, or designee. Examples may include but are not limited to:
1. Disseminate information or instructions which do not warrant a formal order.
 2. Explain and clarify existing orders or policy.
- I.** Inter-departmental memorandum: An inter-departmental memorandum is a written directive for the routine exchange of information. It may be issued by any level of the department to any other level of the department normally following the established chain of command.
- J.** All written directives, except interdepartmental memorandum, shall be issued to the appropriate personnel in the Power DMS document management system. Personnel receiving written directives in the Power DMS system shall review and acknowledge receipt of the written directive in the system within fourteen (14) calendar days of issuance. Exceptions

may be granted by a division commander for new officers in training, time off, sick leave, etc.

III. Procedure: Development, Review, and Purging of Written Directives

- A.** Departmental employees are encouraged to raise new concepts and issues, and to use any available resources in the research and development of new or revising of current written directives.
- B.** Any suggestion to change or add a new written directive will be submitted through the chain of command to the issuing authority and the accreditation manager.
- C.** Prior to adoption of a new/revised written directive or the purging of an existing written directive, the issuing authority shall ensure that they are in compliance with all applicable laws. The issuing authority shall also ensure the adoption or removal of a written directive does not contradict other agency written directives unless intending to revise, replace or purge said written directive. The issuing authority shall ensure that the adoption or removal of a written directive complies with all applicable CALEA standards. The issuing authority shall consult with the accreditation manager prior to issuing, revising or purging a written directive that affects compliance with CALEA standards.
- D.** After development of a new or revised policy, procedure, or rules and regulation, the Chief of Police or designee shall place the policy, procedure, or rules and regulation in the Power DMS document management system.
- E.** The Chief of Police or designee shall notify division commanders via the Power DMS document management system when the policy, procedure, or rules and regulation is available to review and assign a due date for comments to be submitted electronically via the collaboration function. If the policy, procedure, or rules and regulation has had minor changes to include spelling or format corrections, the division commanders are not required to review the document and it can go directly to the Chief of Police for final approval.
- F.** If comment(s) are added by the division commanders, the Chief of Police or designee shall address the comment(s) prior to publishing the document. All comments from the division commanders and the Chief of Police shall be addressed prior to publishing.
- G.** Once all comments have been addressed and the policy, procedure or rules and regulation have been reviewed by the division commanders, the Chief of Police or designee shall complete final approval through the Power DMS document management system.
- H.** All current written directives will be reviewed on an annual basis by the issuing authority or the accreditation manger to ensure compliance with any changes during the past year.

IV. PROCEDURE: Indexing and Format

- A.** The Chief of Police or designee shall format all new or revised policy, procedure, and rules and regulations to maintain consistency. All other

written directives will be formatted by the issuing authority following the guidelines established in the formatting section of this procedure.

- B.** Policies, procedures, and rules and regulations shall be formatted with the Operations Manual chapter number and title, the section number and title, and the subsection number and title centered at the top of the first page. The department logo shall also be centered at the top of the first page. Policies, procedures and rules and regulations shall be on white paper containing one column with the policy/procedure or rules and regulations reference number, title, and a CALEA reference number. Policies, procedures, and rules and regulations will be numbered to indicate the section, subsection, and policy/procedure or rules and regulations number (e.g. 12.2.1, 12 indicates the section number, 2 indicates the subsection number, and 1 indicates the policy/procedure or rule and regulation number).
- C.** Departmental general orders shall be formatted with the department logo on the left at the top of the first page followed by the designation “Departmental General Order.” Departmental general orders will be indexed according to the year they were issued followed by the sequential number of the order for the specific year it was issued (e.g. Departmental General Order #: 2010-01, Departmental General Order#: 2010-02). The departmental general order will contain one column designating the following:

 - 1. To: (To whom the order is addressed)
 - 2. From: (Issuing Authority)
 - 3. Re: (Topic to be addressed)
 - 4. Departmental General Order#: (Numerical designation of order)
 - 5. Date: (Date order issued)
 - 6. The remainder of the departmental general order will be of open text format to contain the order itself.
- D.** Divisional general orders shall be formatted with the department logo on the left at the top of the first page followed by the designation “Divisional General Order.” The order will then indicate in which division the order will be issued (e.g. Patrol, Investigations, Administrative Services, and Support Services). Divisional general orders will be indexed according to the year they were issued followed by the sequential number of the order for the specific year it was issued (e.g. Divisional General Order/ Patrol #: 2010-01, Divisional General Order/ Patrol #: 2010-02). The divisional general order will contain one column designating the following:

 - 1. To: (To whom the order is addressed)
 - 2. From: (Issuing Authority)
 - 3. Re: (Topic to be addressed)
 - 4. Divisional General Order#: (Numerical designation of order)
 - 5. Date: (Date order issued)
 - 6. The remainder of the divisional general order will be of open text format to contain the order itself.

- E.** Personnel orders shall be formatted with the department logo on the left at the top of the first page followed by the designation "Personnel Order." Personnel orders will be indexed according to the year they were issued followed by the sequential number of the order for the specific year it was issued (e.g. Personnel Order #: 2010-01, Personnel Order#: 2010-02). The personnel order will contain one column designating the following:
1. To: (To whom the order is addressed)
 2. From: (Issuing Authority)
 3. Re: (Topic to be addressed)
 4. Personnel Order#: (Numerical designation of order)
 5. Date: (Date order issued)
 6. The remainder of the personnel order will be of open text format to contain the order itself.
- F.** Special orders shall be formatted with the department logo on the left at the top of the first page followed by the designation "Special Order." Special orders will be indexed according to the year they were issued followed by the sequential number of the order for the specific year it was issued (e.g. Special Order #: 2010-01, Special Order#: 2010-02). The special order will contain one column designating the following:
1. To: (To whom the order is addressed)
 2. From: (Issuing Authority)
 3. Re: (Topic to be addressed)
 4. Special Order#: (Numerical designation of order)
 5. Date: (Date order issued)
 6. The remainder of the special order will be of open text format to contain the order itself.
- G.** Command staff memorandum shall be formatted with the department logo on the left at the top of the first page followed by the designation "Command Staff Memorandum." The command staff memorandum will contain one column designating the following:
1. To: (To whom the memorandum is addressed)
 2. From: (Issuing Authority)
 3. Re: (Topic to be addressed)
 4. Written Directive Reference #: (Numerical designation of associated written directive if applicable)
 5. Date: (Date memorandum issued)
 6. The remainder of the command staff memorandum will be of open text format to contain the message being conveyed.
- H.** Interdepartmental memorandum shall be formatted with the department logo on the left at the top of the first page followed by the designation "Interdepartmental Memorandum." The interdepartmental memorandum will contain one column designating the following:
1. To: (To whom the memorandum is addressed)
 2. From: (Issuing Authority)
 3. Re: (Topic to be addressed)

4. Written Directive Reference #: (Numerical designation of associated written directive if applicable)
 5. Date: (Date memorandum issued)
 6. The remainder of the interdepartmental memorandum will be of open text format to contain the message being conveyed.
- I. Grammatical construction of written directives shall be in accordance with the following:
 1. Tense Usage shall be interchangeable with the past, present and future.
 2. Gender Usage of the masculine or feminine shall be interchangeable to include members of both sexes unless otherwise specified.
 3. The Usage of singular terms shall also include the plural unless other specified.
 4. The words "SHALL" and "WILL" are mandatory words. The words "MAY" and "SHOULD" are considered permissive.
- V. Procedure: Purging and Archive**
- A. Except for an interdepartmental memorandum, when a written directive is revised, replaced, or purged, the original version of the written directive shall be archived in the Power DMS document management system.
 - B. Notice shall be given to all affected personnel when a current written directive is revised, replaced, or purged. The notice shall be in the form of a departmental memorandum, general order, divisional general order, or through notice in the Power DMS document management system.
 - C. Purging a written directive shall be performed by the issuing authority; however, any supervisor shall have the ability to purge a written directive issued by personnel under their command and control.

Chapter 2: Organization, Management and Administration
Section 12: Direction
Subsection 2: Written Directives



Policy/Procedure #: 2

Title: Operations Manual/Dissemination and Storage

CALEA Reference: 12.2.1/12.2.2

I. Policy: Operations Manual

An operations manual is established for the purpose of organizing and storing Urbandale Police Department written directives and other important documents in a system that allows ease of use and accessibility for all personnel. A system of distribution and storage of written directives allows for accountability from all personnel. Responsibility for distribution, inspection and maintenance is established to ensure the latest revisions of the operations manual are available in a timely manner.

II. PROCEDURE: Indexing of Operations Manual

- A.** The operations manual shall be divided into chapters. Each chapter shall contain a general subject matter to be covered. Each chapter shall be given a numerical designation. (e.g. Chapter 1: Role, Responsibility and Relations, Chapter 2: Organization, Management and Administration).
- B.** Each chapter of the operations manual may be divided into sections. Each section shall contain a topic related to the subject matter of the chapter to which it is assigned. Each section will be given a numerical designation (e.g. Chapter 1: Role, Responsibility, and Relations, Section 1: Law Enforcement Role and Authority, Section 2: Agency Jurisdiction and Mutual Aid).
- C.** Each section of the operations manual may be further divided into subsections. Each subsection shall contain a topic related to the subject matter of the section to which it is assigned. Each subsection will have a numerical designation (e.g. Chapter 1: Role, Responsibility and Relations, Section 1: Law Enforcement Role and Authority, Subsection 1: Law Enforcement Agency Role, Subsection 2: Limits of Authority).
- D.** Each subsection of the operations manual may be further divided into individual policies and procedures or rules and regulations. Each policy

and procedure or rule and regulation shall contain a topic related to the subject matter of the subsection to which it is assigned. Each policy and procedure or rule and regulation will have a numerical designation (e.g. Chapter 1: Role, Responsibility and Relations, Section 1: Law Enforcement Role and Authority, Subsection 1: Law Enforcement Agency Role, Policy/Procedure #1: Oath of Office, Policy/Procedure #2: Code of Ethics).

- E. The operations manual shall contain a table of contents to assist users with locating specific items in the manual.
- F. One chapter of the operations manual shall be designated for orders. The orders contained in this chapter shall include, departmental general orders and divisional general orders.
- G. The operations manual shall contain an appendix. The appendix may be used for departmental information that does not readily lend itself to categorization within the operation manual chapters. Each document placed in the appendix will be designated with a letter (e.g. Appendix A: Urbandale Boundary Map, Appendix B: Code of Ethics).
- H. Indexing of the operations manual shall be the responsibility of the Chief of Police or designee.

III. PROCEDURE: Dissemination

- A. The operations manual shall be stored on the police production server. Receipt and review of the documents contained in the operations manual shall be maintained by the Power DMS document management system.
- B. If any document within the operations manual is added, removed or revised, the Chief of Police or designee will utilize the Power DMS document management system to alert personnel in the Department. If anyone experiences a problem with receiving the information or there are questions about the change, personnel shall contact their direct supervisor or the Chief of Police or designee for clarification or assistance. If necessary, the Chief of Police or designee may issue paper copies of any update. If paper copies are distributed, the Chief of Police or designee will document their receipt and review.
- C. A paper copy of the operations manual shall be kept in the library area. If any written directive within the operations manual is added, removed, or revised, the Chief of Police or designee shall update the paper copy of the operations manual.
- D. An electronic copy of the operations manual shall be kept in the police production server. The electronic copy of the operations manual shall be accessible by all personnel through the use of departmental computers. The Chief of Police or designee is responsible for the maintenance of the electronic copy of the operations manual. If any document within the operations manual is added, removed or revised, the Chief of Police or designee shall update the electronic copy stored in the police production

server. All employees shall be instructed on how to access and use the electronic copy of the operations manual as well as the ability to access a paper copy.

- E.** It shall be the responsibility of each employee to read and understand each document within the operations manual.

Chapter 2: Organization, Management and Administration
Section 12: Direction
Subsection 2: Written Directives



Policy/Procedure#:3
Title: Motto and Mission Statement
CALEA Reference: 12.2.1

- I. Policy: Motto and Mission Statement**
A motto and mission statement is established to demonstrate commitment from every member of the Urbandale Police Department to quality performance in our daily endeavors. It is critical that all members understand and accept the responsibilities established by the motto and mission statement. It provides the foundation upon which all operational decisions and organizational directives will be based. This includes all rules, regulations, policies, procedures and practices.
- II. Motto:**
Service Built on Integrity
- III. Mission Statement:**
The Urbandale Police Department is dedicated to enhancing public safety and maintaining the quality of life for the community we serve.

Chapter 2: Organization, Management, and Administration
Section 15: Planning and Research, Goals and Objectives, and Crime
Analysis
Subsection 1: Planning and Research



Policy/Procedure #: 1

Title: Planning and Research

CALEA Reference#: 15.1.1, 15.1.2, 15.1.3, 15.2.1, 15.2.2

I. Policy: Planning and Research

A policy is established to outline the Urbandale Police Department's planning and research component. The policy shall address the department's commitment to planning and research as an effective management tool for evaluating current police services and projecting future needs.

II. Procedure: Multi-year plan

A. The Chief of Police shall be responsible for planning and research for the department. The planning and research function of the department shall anticipate needs through the use of a multi-year plan as well as departmental and divisional goals and objectives.

B. The Chief of Police shall produce a multi-year plan that establishes the long term goals and objectives of the department and projects the needs of the department for the next ten (10) years. The multi-year plan is designed to assist with planning and budget preparation. The multi-year plan shall include the following:

1. Long term goals and operational objectives
2. Anticipated workloads and population trends
3. Anticipated personnel levels
4. Anticipated capital Improvements and equipment needs

C. Annually, the Chief of Police shall review and revise the multi-year plan.

III. Procedure: Department and divisional goals and objectives

A. Short term departmental and divisional goals and objectives shall be established by the Chief of Police with input from the division commanders.

1. Goals and objectives shall be established for the department and each division annually.

2. The Chief of Police shall request input on goals and objectives by tasking division commanders to submit goals and objectives for their respective divisions on an annual basis. Division commanders may seek input from employees in their division to assist in formulating goals and objectives.
 3. Division commanders shall also provide performance measures which can be utilized to measure progress towards reaching the goals they have provided.
 4. The Chief of Police shall evaluate the submissions by the division commanders and finalize the goals and objectives as well as the performance measures to be utilized.
 5. The Chief shall hold annual evaluations with the division commanders to review progress towards stated departmental and divisional goals and objectives and overall performance of the division.
 6. Goals and objectives shall be made available to all agency personnel.
- D. Any employee enlisted to assist with the multi-year plan or departmental and divisional goals and objectives shall have direct access to the Chief of Police for planning, research, and direction.

Chapter 2: Organization, Management, and Administration
Section 16: Allocation and Distribution of Personnel and Personnel
Alternatives
Subsection 3: Reserves



Policy/Procedure #: 1
Title: Reserves
CALEA Reference#:

I. Policy: Reserves

A policy is established to govern the Urbandale Police Department reserve unit. The policy shall establish hiring, training, termination, uniform and equipment requirements, liability issues, and performance evaluations. The Urbandale Police Reserve Unit shall comply with all demands and restrictions of Iowa Code Chapter 80D and City of Urbandale Municipal Code.

II. Procedure: Reserve Selection Procedure

- A.** All reserve police officer applicants shall be subject to the same background investigation requirements as full-time sworn officers.
- B.** Selection criteria applicable to full-time sworn officers shall apply equally to reserve police officers.
- C.** Reserve police officer applicants shall be required to possess a high school diploma or equivalent education.
- D.** Appointments shall be made by the Chief of Police with the approval of the Mayor and City Council in accordance with the City of Urbandale Municipal Code.

III. Procedure: Reserve Training Requirements

- A.** All Urbandale reserve police officers shall be required to satisfy State of Iowa mandatory training for reserve police officers by completing Iowa Law Enforcement Academy reserve police officer training requirements.
- B.** Meeting the same requirements the Department has for sworn officers, reserve police officers shall be required to meet all in-service training requirements on the Department's use of force policy and procedure as well as complete weapons proficiency testing annually.
- C.** Reserve police officers shall receive necessary in-service training and certifications equivalent to the requirements sworn officers of the Department. The reserve coordinator, in conjunction with the Support Services Division, shall ensure all reserve training and certifications meet

the standards of the Department and the requirements of the State of Iowa.

IV. Procedure: Reserve Ranks

- A. Reserve Candidate:** Upon selection, a reserve candidate shall be required to complete the initial training modules and testing as established by the State of Iowa and the Iowa Law Enforcement Academy for reserve officer certification. Once completing the training modules and meeting the State of Iowa requirements for a reserve officer, a reserve candidate shall be required to complete the Urbandale Police Department reserve candidate field training program and a minimum of nine (9) months of observation with a certified officer. The training and the observation shall run concurrently. The reserve coordinator or the Patrol Division Commander may select any sworn officer to act as a field training officer for the reserve officer field training program.
- B. Reserve Officer:** Once completing the reserve candidate requirements and being approved to continue in the reserve program, a reserve candidate shall progress to reserve officer status.
- C. Senior Reserve Officer:** Once completing three (3) years of service as a reserve officer and being approved to continue in the reserve program, a reserve officer shall progress to senior reserve officer status.
- D. Command Reserve Officer:** Upon completing two (2) years of service as a senior reserve officer, a reserve officer is eligible to be selected as a command reserve officer. Command reserve officers shall be senior reserve officers demonstrating management and leadership abilities that will assist the reserve coordinator with the administrative duties of operating the reserve unit. Command reserve officers shall be recognized as a lieutenant or a captain. After one (1) year of service as a command reserve officer at the rank of reserve lieutenant, a reserve command officer is eligible to obtain the rank of reserve captain. Command reserve officer status shall be awarded at the discretion of the Chief of Police. The reserve unit shall be restricted to no more than three (3) lieutenant's positions and one (1) captain's position.
- E.** Progression to the next level of reserve officer shall be at the discretion of the Chief of Police. The decision shall be based on a variety of factors to include job performance and the ability to meet departmental requirements for volunteer hours and training. Any progression to a higher level shall be documented in a personnel order.

V. Procedure: Uniforms and Equipment

- A.** Reserve officers shall have the same uniforms as sworn officers with the Department. The difference in uniform shall be the reserve insignia displayed above the departmental patch and reserve insignia on departmental badges.
- B.** Reserve officers shall be supplied a bullet proof vest of the type supplied to sworn officers of the Department and be held to the same standard requiring the use of the vest as stated in Chapter 5 section 41.1.1 of the Operations Manual.

VI. Procedure: Employment Status and Benefits

- A.** As provided by City of Urbandale Municipal Ordinance, reserve police officers shall be considered employees of the City of Urbandale during those periods when they are performing police duties for the Urbandale Police Department.
- B.** As employees, reserve police officers for the City of Urbandale shall receive hospital and medical assistance and benefits as provided in Chapter 85 of the Code of Iowa to members of the reserve force who sustain injury in the course of performing official duties but shall not be included under or share any of the benefits or obligations contained in the police retirement system of Chapter 411 of the Iowa Code.
- C.** Liability and false arrest insurance shall be provided by the City of Urbandale to reserve police officers while performing official duties in the same manner as for sworn police officers.

VII. Procedure: Evaluations and Termination

- A.** The reserve coordinator or designee shall complete performance evaluations on all reserve police officers as provided for in Chapter 4 Section 35 of the Operations Manual. This shall include quarterly evaluations during the reserve candidate status as described above.
- B.** The members of the reserve police unit shall serve at the discretion of the Chief of Police and they may be removed and discharged from such positions and their city employment terminated. Such removal may be without cause and/or by recommendation of the reserve police captain, the reserve coordinator, or a division commander.

VIII. Procedure: Duty Requirements and Restrictions

- A.** All reserve officers shall work under the direct supervisory control of a certified police officer. Under normal circumstances, this will be the supervisor of a patrol shift. In addition, the following restrictions/requirements shall apply:
Reserve Candidate- During initial module training required by the State of Iowa, a reserve candidate is required to complete four (4) hours of non-uniformed observation each month with a sworn officer or command reserve officer (the vast majority of these hours shall be with a certified officer). Upon completion of the initial module training required by the State of Iowa, reserve candidates shall enter the Urbandale Police Department reserve candidate field training program. During the reserve candidate field training program, reserve candidates shall be required to complete sixteen (16) hours of uniformed observation time each month for a minimum of nine (9) months with a sworn officer. Failure to complete the required hours may result in an extension of the field training program. A reserve candidate shall only participate in uniform at special events while in the immediate presence and control of a certified officer or any non-probationary reserve officer and only after completion of the initial module training required by the State of Iowa. For the reserve candidate, participation at special events shall not be considered part of the

observation time required each month. Reserve candidates are not allowed to operate a patrol vehicle.

Reserve Officer- Required to complete approximately 100 hours of volunteer hours per calendar year. The 100 hours of volunteer time shall be distributed throughout the year (i.e. no working 100 hours the last 2-3 months due to failure to volunteer the prior 9-10 months). Volunteer hours and participation in special events shall be restricted to being in the immediate presence and control of a certified officer, senior reserve officer, or command reserve officer. A minimum of 50% of the volunteer hours shall be in observation and assistance to a certified officer.

Senior Reserve Officer- Required to complete approximately 100 hours of volunteer hours per calendar year. A minimum of 50% of the volunteer hours shall be in observation and assistance to a certified officer. The 100 hours of volunteer time shall be distributed throughout the year (i.e. no working 100 hours the last 2-3 months due to failure to volunteer the prior 9-10 months). Volunteer hours and participation in special events may be completed without the restriction of immediate presence and control of another officer; however, it is encouraged that the majority of volunteer hours be spent assigned to a certified officer. Within the restriction of department policy and with supervisor approval, senior reserve officers are restricted to operating a patrol vehicle only during a special event or a special assignment unless accompanied by a certified officer.

Command Reserve Officer- Command reserve officers shall have the same volunteer requirements and restrictions of duty as senior reserve officers with additional management duties as assigned by the reserve coordinator. Within the restriction of department policy and with supervisor approval, command reserve officers shall be allowed to operate a patrol vehicle.

- B. After receiving required training and instruction, all reserve officers may operate the department all-terrain vehicle.
- C. All levels of reserve officers are required to attend monthly reserve meetings and assigned training sessions.
- D. Except for the reserve candidate that has not completed the State of Iowa reserve training modules, all levels of reserve officers are required to volunteer during the events scheduled on or around July 4th. Exceptions may be granted by the reserve coordinator. Except for reserve candidates, reserves are also required to volunteer during at least one additional event during the calendar year. Volunteer hours working an event shall count toward reserve officers annual requirements except as noted above for reserve candidates.
- E. Failing to volunteer the required hours per month, attend monthly meetings, and complete required training shall be grounds for termination from the reserve police officer unit. The reserve coordinator may approve absences for two (2) months of volunteer hours and two (2) meetings per year. Absences shall be conveyed prior to occurrence. Volunteer hours

missed shall be completed before the end of the calendar year. Required training missed shall be rescheduled as soon as practical.

- F.** Inability to participate in monthly meetings and/or volunteer hours due to a prolonged illness or injury shall be documented by a leave of absence granted by the Chief of Police. Unlike the approved absences noted above, volunteer hours missed while on an approved leave of absence do not have to be recovered at a later time.
- G.** Requirements for scheduling of volunteer hours, monthly meetings, special events, and training shall be organized by the reserve coordinator and command reserve officers.
- H.** All volunteer hours and activities to include monthly meetings, training, and special events shall be documented by the reserve coordinator or designee utilizing the reserve database and/or other department accepted forms (e.g. agenda, meeting minutes, lesson plans, event logs, etc.).

Chapter 2: Organization, Management, and Administration
Section 16: Allocation and Distribution of Personnel and Personnel
Alternative
Subsection 4: Auxiliaries



Policy/Procedure #:1
Title: Police Chaplain
CALEA Reference#:

I. Policy: Chaplains

Chaplains provide spiritual guidance and support to members of the Urbandale Police Department, their families, and the community. Chaplains are not intended to replace an individual's own clergy and are available based on need and desire. Chaplains are non-sworn volunteers.

II. Procedure: Appointment and Qualifications

A. Applicants for police chaplain shall meet the following requirements:

1. Be an ordained member of the clergy, recognized as a member of a religious body, in either full time service or having retired from a full time ministry. It is preferable to possess an ecclesiastical endorsement from the applicant's recognized church organization.
2. Possession of a high school diploma or GED and have a certificate in clinical pastoral education.
3. Possess a valid motor vehicle operator's license issued by the State of Iowa.
4. Provide personal references attesting to the ministerial works of the chaplain.
5. Satisfactorily complete a thorough background investigation (including driving record and criminal history background).
6. Able to comply with all other requirements of the standard operating procedure governing the chaplaincy program.

B. Police chaplain applications shall be reviewed by the Chief of Police prior to appointment. Only the Chief of Police shall have the authority to appoint police chaplains to the Department.

C. Unless sworn as a regular or reserve police officer, the chaplains are not law enforcement officers and shall possess no law enforcement authority other than that of a private person.

III. Procedure: Role and scope of authority

- A. The chaplain program shall be administered by the Support Services Division; however, chaplains shall have the authority to report directly to the Chief of Police.
- B. The primary role of the police chaplain is to provide spiritual assistance, guidance, and counseling.
- C. When appropriate, the chaplain shall contact the clergy of anyone involved in a crisis and make appropriate referrals to other agencies.
- D. Without the permission of the Chief of Police, chaplains shall make no statements regarding their role with the department or reference any incident in which they participated as a chaplain for the department to the media.
- E. Chaplains' scope of authority is described in Chapter 3 Section 22.1.5 (Line of Duty Death) and Chapter 6 Section 55.2.6 (Emergency Notification) of the Operations Manual. They may also be utilized in a variety of other critical incidents. The following examples are considered critical incidents and calling upon the police chaplain to assist is highly recommended:
 - 1. Unattended Death: When there has been an unattended death, suicide, or other death investigation. Always call the police chaplain if the death is due to an accident, fire, or criminal activity. Do not ask the family if they desire a chaplain. The chaplain will make an inquiry of needed services upon arrival. If services are not needed, the chaplain will express their sympathy to the family on behalf of the city and leave.
 - 2. Victim Assistance: All traumatic events (major fires, accidents, shootings, etc.) when compassionate support is needed – the chaplain knows what the community resources are and how to make referrals.
 - 3. Confidential counseling: When an officer desires confidential counseling related to any aspect of his/her professional or personal life. Any communications an employee makes to the chaplain is strictly confidential and shall not be released to departmental members or any other person without the explicit consent of the person being counseled. Any police personnel may go to the chaplain without having to notify his/ her supervisor or anyone else that personal counseling is being sought. Only when there is imminent danger to the person seeking counseling or others shall this confidentiality be breached.
 - 4. When a chaplain is called to assist, they shall submit a report detailing their involvement in the incident to the Support Services Division Commander or designee. The report shall be shared with the command staff and Chief of Police as needed. Confidential counseling shall not be documented on a report to the Department.

IV. Procedure: Training

- A. It is expected those serving as chaplains will take the initiative to further their own education and develop skills to benefit their ministry and chaplaincy with the Department.
 - B. When able, the Department shall provide opportunities for continuing education and training for its chaplains. Continuing education and training may be found through various law enforcement agencies, hospitals, and church organizations including the International Conference of Police Chaplains (ICPC). The ICPC has regional meetings as well as a national meeting each year and offers a wide span of helpful information.
- V. **Procedure: Equipment & Uniforms**
 - A. Chaplains shall be provided the following department issued clothing and equipment:
 - 1. Department identification
 - 2. Department chaplain badge
 - 3. Department keycard to allow access to the common areas of the police department.
 - 4. Shirts with embroidered "Urbandale Police Chaplain" designation.
 - 5. Jacket with embroidered "Urbandale Police Chaplain" designation.
 - 6. Department uniform. The uniform shall clearly designate "police chaplain" by the badge and the collar insignia.
 - 7. Ceremonial uniform to be worn for formal or special events. The uniform shall clearly designate "police chaplain" status through the badge and the collar insignia.
 - B. When responding to incidents, chaplains are encouraged but not required to wear the department issued uniform or clothing. They are required to possess their department issued identification and present a professional appearance.

Chapter 2: Organization, Management and Administration
Section 17: Fiscal Management and Agency Property
Subsection 1: Fiscal Management



Policy/Procedure #:1

Title: Budgeting Process

CALEA Reference#: 17.1.1, 17.2.1, 17.2.2

I. Policy: Budgeting Process

A policy is established to outline the Urbandale Police Department budgetary process. The policy establishes the authority and responsibility for the fiscal management of the Urbandale Police Department. The policy also address responsibility for budgetary functions within the Department.

II. Procedure: Authority

- A.** The Chief of Police shall have the authority to manage the budget for the Urbandale Police Department.
- B.** The Chief of Police shall be responsible for the fiscal management of the Urbandale Police Department.

III. Procedure: Requirements

- A.** The budget shall be developed with the cooperation of all organizational components, command staff, and supervisory personnel. All personnel shall have the opportunity to submit, through the chain of command, any budget request intended to enhance the operation of their unit or division. The requests will be compiled in conjunction with the Department's overall goals and objectives and will be accompanied by written justification for the anticipated expense. The Chief of Police will determine the due date for these requests each year based on the timeline established by the City Manager.
- B.** Comprehensive written justifications shall be required for all new expenditures or expansion of existing expenditures. Written justifications shall be supported by historical information, explanation of need, and costs associated with implementation.
- C.** Unless requested by the Chief of Police, written justifications shall not be required for anticipated expenditures necessary to maintain the same levels of service as in the current fiscal year, including projected cost increases due to inflation.

IV. Procedure: Budget Process and Responsibility

- A.** The Chief of Police shall request budget justifications from all divisional commanders.
- B.** Division commanders shall inquire with division personnel to project needs for the upcoming fiscal year.
- C.** Based on discussions within the division, the division commanders shall draft budget justifications for any new or expanded expenditures. Division commanders shall be responsible for portions of the department budget related to the functions of their division to include:
 - 1.** Operating needs
 - 2.** Capital purchase needs
- D.** The budget justification form shall be utilized to submit all budget justifications to the Chief of Police.
- E.** Upon completion of budget justifications, the command staff shall present their budget justifications to the Chief of Police. The Chief of Police and the command staff shall discuss the budget justifications and decide which items will be included in the budget proposal to the City Manager and the City Finance Department. The Chief of Police shall make the final decision on all items included in the budget proposal to the City Manager and the City Finance Department.
- F.** Based on the recommendations established in the multi-year plan, the Chief of Police shall be responsible for submitting requests for additional personnel or personnel expenditures such as overtime to the City Manager and the Finance Department during the budget process.
- G.** The Office of the Chief of Police shall have responsibility for producing the final budget proposal in the format requested by the City Manager and the City Finance Department.
- H.** At the City Manager's discretion, the Chief of Police may present the budget proposal for the Urbandale Police Department to the City Manager and the City Finance Department. Division commanders will be included in the budget presentation as determined by the Chief of Police.

Chapter 2: Organization, Management and Administration
Section 17: Fiscal Management and Agency Property
Subsection 3: Purchasing



Policy/Procedure #: 1

Title: Requisition and Purchasing

CALEA Reference#: 17.3.1

I. Policy: Requisition and Purchasing

A policy is established to regulate the requisition and purchasing of equipment, supplies, and services for the Urbandale Police Department. The policy shall address, bidding requirements, the selection of submitting bids, emergency purchasing and requests for supplemental appropriations. All procedures shall be compliant with the City of Urbandale purchasing policy and procedures manual.

II. Procedure: Item Specifications

- A.** Whenever possible, an employee shall state specifications for items or services purchased. A specification is the description of the items or services to be purchased. Because quality is as important as price, the employee shall furnish the specifications that will fulfill but not exceed the requirements for which the items or services are intended.
- B.** In considering and developing specifications, it must always be considered purchases funded by public revenue cannot be expected to provide for deluxe or luxurious levels of quality. It is necessary to follow a general policy toward the purchase of goods and standard grades of merchandise which represent an optimum relationship between quality and price while consistently providing satisfactory levels of service.
- C.** Bids and vendor prices must be based upon adequate specifications. A lengthy specification designed solely for the purpose of eliminating competition must be avoided. Specifications must be free from restrictions which would tend to reduce or eliminate competition. Evaluation of bids shall be based upon specifications supplied to the vendors. The Department may give weight to life cycle costing and weighing for standard objectives whether or not stated in the prepared specifications.
- D.** The administrative specialist assigned to the Office of the Chief of Police may assist an employee in developing specifications for items to be purchased.

- E. An employee's supervisor, division commander, or the Chief of Police may deny a request to purchase based on specifications or the lack thereof.

III. Procedure: Requisition

- A. When an employee identifies a need to purchase equipment, supplies, or services in order to meet the requirements of their duties, they shall submit a request to purchase form if meeting the thresholds established below. The total cost including shipping and handling fees shall be considered when evaluating the thresholds.
- Under \$250- Exempt from the requirement to submit a request to purchase form. The item can be purchased by an employee using a vendor charge account or department credit card.
Receipts/invoices are to be turned into the administrative specialist assigned to the Office of the Chief of Police within 5 working days of the date on the receipt/invoice.
 - \$250-\$2,500- Submit a request to purchase form. Include the item or service requested, reason for the request, description or specification of the item or service, quantity needed and the actual or approximate cost of the item or service.
 - \$2,500- \$10,000- Submit a request to purchase form. Include the item or service requested, reason for the request, description or specification of the item or service, quantity needed and 3 written quotes.
 - \$10,000- \$25,000- Competitive bid process. Submit a request to purchase form with the 3 lowest bids received.
 - \$25,000 and above- Competitive bid process and City Council approval.
 - Note: The above thresholds are excerpts from the city's purchasing policy and shall be utilized as a guide. The city's purchasing policy shall be referred to for specifics regarding purchasing requirements.
- B. An employee will submit the request to purchase form to their immediate supervisor for approval. If the supervisor approves the request, they will forward the request to purchase form to the division commander. If the division commander approves the request to purchase they shall forward the request to the Chief of Police. If the Chief of Police approves the request to purchase, the form will be forwarded to the administrative specialist assigned to the Office of the Chief of Police.
- C. The administrative specialist assigned to the Office of the Chief of Police shall notify the employee their request to purchase has been approved and assist the employee to ensure requirements of the city purchasing policy and procedures manual are followed.
- D. The administrative specialist assigned to the Office of the Chief of Police shall document all purchases made through request to purchase

forms and submit all needed documentation to the city finance department.

- E. If a request to purchase is denied by an immediate supervisor, division commander or the Chief of Police, the reason for the denial will be entered on the form and returned to the employee originally requesting the purchase.
- F. The Chief of Police shall be exempt from the requirement to submit a request to purchase form on equipment, supplies or services in which a direct request is made to the City Finance Department, the City Manager or the City Council.

IV. Procedure: Purchasing

- A. All employees shall follow the purchasing policy and procedures manual for the City of Urbandale. When following the procedures outlined in this policy and the City of Urbandale purchasing policy and procedures manual, all employees of the Department are authorized to make the purchased needed to perform the functions of their position.
- B. For items or services under \$100.00, an employee may purchase the item or service with personal funds and retain the receipt in order to be reimbursed. Reimbursement can be submitted through the City Finance Department or through the departmental petty cash fund administered by the administrative specialist assigned to the Office of the Chief of Police.
- C. The administrative specialist assigned to the Office of Chief of Police can assist with ordering equipment, supplies, and services for the Department.
- D. A request to purchase form shall not be required for travel costs. All costs associated with travel shall be submitted in accordance with the City of Urbandale's travel policy guidelines.

V. Procedure: Emergency Purchasing

- A. An employee may circumvent the purchasing procedure if a situation requiring an expenditure of funds is an emergency. An emergency situation shall be classified under emergency exemptions in the city purchasing policy and procedure manual.
- B. If an employee purchases goods or services under the emergency exemptions of the city purchasing policy and procedure manual, they shall submit a request to purchase form with an attached memorandum detailing their justifications for the expenditure and the need to circumvent the standard requisition and purchasing procedure. All receipts and documentation of the expenditure shall also be attached. The submission of documents shall be made as soon as practical after the emergency situation has been resolved.
- C. The request to purchase form and the attached memorandum shall be submitted through the chain of command to the Chief of Police for review. After review, the Chief of Police shall submit documentation to the

City Manager for approval under the emergency exemptions section of the city purchasing policy and procedure manual.

- D. If approved by the City Manager, the request to purchase form and a copy of the attached memorandum shall be submitted to the administrative specialist assigned to the Office of the Chief of Police for documentation and payment.

VI. PROCEDURE: Supplemental or Emergency Appropriation and Fund Transfer

- A. In the event the Department would require supplemental or emergency funds in a specific line item of the budget, the Chief of Police has the authority to transfer funds within the department budget. The Chief of Police shall notify the City Finance Director of the transfer for accounting purposes.
- B. In the event the operating budget for the department is exceeded, the Chief of Police shall request supplemental or emergency funds through the City Finance Director and the City Manager. If the supplemental or emergency funds cannot be subsidized through funds appropriated to the public safety function or the contingency fund established in the Urbandale city budget, Iowa state law governing the budget amendment process must be followed in requesting additional funds.
- C. The administrative specialist assigned to the Office of the Chief of Police shall be informed of any approved supplemental or emergency appropriations in order to maintain accurate records within the Department.

Chapter 2: Organization, Management, Administration
Section 17: Fiscal Management and Agency Property
Subsection 4: Accounting



Policy/Procedure #: 1

Title: Accounting

CALEA Reference#: 17.4.1, 17.4.2, 17.4.3

I. Policy: Accounting

A policy is established to ensure appropriate and approved accounting of all funds administered by the Urbandale Police Department. The policy shall address all accounts and authorize use of cash funds. The policy shall also establish an independent audit mechanism for department fiscal activities. Any accounting procedure utilized by the Department shall comply with all the requirements of the city of Urbandale Finance Department (Finance Department).

II. Procedure: Account Management

- A.** As part of the budgetary process prescribed by the Finance Department, the Chief of Police shall approve and be responsible for all accounts utilized by the Urbandale Police Department.
- B.** The Chief of Police shall review monthly status reports on all department accounts. The monthly status report shall include the following:
 - 1. Initial appropriation for each account.
 - 2. Balances at the commencement of the monthly period.
 - 3. Expenditures and encumbrances made during the period.
 - 4. Unencumbered balance.

III. Procedure: Cash Accounts

- A.** The Department shall maintain various cash accounts in order to perform specific duties. Maintenance and record keeping of each cash account shall be assigned to one employee within the division with functional responsibility for the account. The employee shall submit quarterly reports to the administrative specialist assigned to the Office of the Chief of Police for review. If the cash account is administered by the administrative specialist assigned to the Office of the Chief of Police, the quarterly report shall be submitted to the Support Services Division Commander for review.
- B.** A cash account reporting form shall be utilized to report quarterly cash account activities. The cash account reporting form shall include a

balance sheet indicating initial balance, credits(cash income received), debits (cash disbursed), and the ending balance.

- C. The review of quarterly cash account reporting shall include a review of all credits, debits, and verification of the ending balance in the account. Once the review is complete the quarterly reports shall be electronically stored in the Department's record system.
- D. Receipts or other documentation shall be created for the acceptance or disbursement of any cash.
- E. The Chief of Police shall authorize any cash expenditure in excess of \$1,000.00.
- F. Employees assigned to the Support Services Division shall be authorized to disburse cash as necessary to complete transactions in which the Department is accepting fees. Disbursement of funds through Support Services Division shall be limited to making correct change during a transaction. Any other disbursement of funds through the accounts managed by Support Services Division must have supervisor approval.
- G. The administrative specialist assigned to the Office of the Chief of Police is authorized to disburse cash from the Department petty cash account for reimbursement of items or services incurred by employees costing less than \$10.00.
- H. An employee must have supervisor approval to disburse cash from the investigation expense fund. Any disbursements of cash shall follow written directives governing the investigative expense fund.
- I. Only employees authorized to administer the alcohol and tobacco compliance checks shall have the authority to disperse cash from the alcohol and tobacco compliance fund. Any disbursements of cash shall follow written directives governing the alcohol and tobacco compliance fund.
- J. All officers and other employees designated by the Support Services Division Commander are authorized to disperse cash in the form of gift cards from the fuel assistance fund. Only the Support Services Division supervisor or designee is authorized to accept funds to replenish the fuel assistance account. Any receipt of or disbursement from the fuel assistance fund shall follow the written directives governing the fund.

IV. Procedure: Audit

The Urbandale Police Department shall be audited on an annual basis as part of the independent audit conducted on the City of Urbandale as required by Iowa State Code 11.6 (1)(2). The results of the independent audit shall be reviewed by the Chief of Police.

V. Procedure: Petty Cash Account

- A. For items or services under \$10.00, an employee may purchase the item or services with personal funds and retain the receipt in order to be reimbursed. Reimbursement may be submitted through the departmental petty cash fund administered by the administrative specialist assigned to the Office of the Chief of Police.

- B. An employee need not obtain prior approval from a supervisor when submitting for reimbursement through the petty cash fund, however, only items or services needed to perform police functions shall be reimbursed. If there is a question as to need, a supervisor shall be consulted prior to the purchase. If disputed, the Chief of Police shall have the final decision on reimbursement.
- C. To obtain reimbursement through the petty cash account, an original receipt shall be submitted to the administrative specialist assigned to the Office of the Chief of Police. Once received, the administrative specialist shall reimburse the employee at the earliest convenience.
- D. At all times, the cash remaining in the account and the receipts that have been reimbursed must total \$50.00.
- E. When the administrative specialist determines the petty cash account needs to be replenished, a memorandum shall be addressed to the City Finance requesting reimbursement to cover all submitted receipts. Attached to this memorandum shall be the original receipts for which reimbursement is being sought. The City Finance shall then issue a check to the Urbandale Police Department for the encumbrances submitted. The check shall be taken to a financial institution and cashed. The cash received shall be placed in the petty cash account.
- F. The petty cash account shall be secured at all times when not in use.

VI. Procedure: Support Services Cash Account

- A. The Support Services Division shall maintain a cash account to facilitate the collecting of various fees. The support services cash account shall maintain \$150.00 in cash and change to facilitate cash transactions for fees and services.
- B. A cash register shall be utilized by the support services division to track all fees collected and maintain by the support services cash fund during business hours. Any proceeds and the support services cash fund shall be secured in the support services safe or the secured register at the close of business each day.
- C. At the beginning of each business day (Monday through Friday), the cash register transactions from the previous day shall be reconciled.
- D. Once every business day, the receipts from the previous day along with any required documentation shall be deposited with City Finance. The employee depositing shall obtain a signature from a member of City Finance on the cash account reporting form indicating the amount deposited. A receipt shall also be obtained from the City Finance indicating the amount of the deposit.
- E. Any U.S. currency (dog at large, bond, impound administrative fee, etc.) collected during non-business hours shall be sealed in an envelope and placed in the secure drawer near the departmental mailboxes. The outside of the envelope shall contain two verifying officers' signatures on the seal and the total amount of currency within the envelope. Accompanying paperwork shall be attached to clearly indicate the appropriate incident number relating to the collection of the currency.

Normal property/evidence procedures will apply to any currency seized during an investigation or turned over as found property.

VII. Procedure: Fuel Assistance Fund

- A.** The Support Services Division shall maintain a cash account to assist local churches and support groups with providing fuel and other needed items to indigent persons. The cash account shall be maintained in the form of Hy-Vee gift cards.
- B.** During normal business hours, Monday-Friday 0800-1630 hours, Support Services Division personnel shall administer assistance to those requesting. After hours requests shall be handled by the Patrol Division.
- C.** The gift cards and corresponding ledger of transactions shall be maintained in a secure drawer near the department mailboxes. The key to the drawer shall be available on the key board in the range observation room. Officers and other employees designated by the Support Services Division Commander shall have access to the drawer and be authorized to disperse the gift cards as established in this policy.
- D.** Upon completion, any employee utilizing a gift card for an indigent person shall notify Support Services Sergeant by email of the transaction. Upon receiving the email notification, the Support Services Sergeant or designee shall inspect the fund to ensure the transaction was properly documented as required by this policy.
- E.** Any gift cards donated to the fund by area churches or other support groups shall only be accepted by the Support Services Sergeant or designee. A receipt shall be provided to the party donating the cards. A copy of the receipt shall be attached to the cash account report.
- F.** The following procedure shall be utilizing when providing assistance with a gift card:
 - 1.** Check the requesting subject's driver's license and record the recipient's name, date of transaction, officer name, and amount of transaction on the cash account report (located in the drawer with the cards). Under most circumstances, assistance shall only be provided once every three (3) months.
 - 2.** Authorized employees shall take one gift card and meet the person requesting at Hy-Vee Gas. Employees shall enter the store and authorize the clerk to provide fuel for the requesting person utilizing the gift card to pay. Ensure a receipt is obtained for the amount of fuel/items purchased. Unless permission is obtained from a supervisor, no more than \$20.00 in assistance shall be given to each requesting party. Under no circumstances is the gift card to be turned over to the requesting party to obtain their own fuel/items.
 - 3.** Return the receipt to the secured drawer attached to the used gift card. Enter the exact amount of the transaction on the cash account report.

4. The gift cards shall only be utilized for fuel and other automotive needs (washer fluid, oil, antifreeze). Any person requesting food assistance shall be referred to the Urbandale Food Pantry for assistance.
- G. It shall be the responsibility of the Support Services Division to maintain an adequate number of gift cards and to contact local churches and support groups when additional donations are needed to continue the program.

Chapter 2: Organization, Management and Administration
Section 17: Fiscal Management and Agency Property
Subsection 5: Agency Property



Policy/Procedure #: 1

Title: Agency Property

CALEA Reference#: 17.5.1, 17.5.2, 17.5.3

I. Policy: Agency Property

A policy is established to ensure agency property is inventoried and controlled. The policy shall address the issuance of agency property and the tracking of said property through its lifespan. The policy shall address operational readiness of all stored agency property.

II. Procedure: Inventory

- A.** All departmental property with a value at time of acquisition of more than \$500.00 shall be recorded utilizing the Department's inventory system. Division commanders or the Chief of Police may require other department property be included in inventory system regardless of value.
- B.** Inventoried property shall be issued a departmental identification number. When practical, the departmental identification number shall be placed on the property to assist in the inventory process.
- C.** The inventory system shall be maintained by the Support Services Division. The inventory system shall include the following (if applicable to the item):
 - 1. Department issued identification number.
 - 2. Item description.
 - 3. Item identification (make, model, serial number, etc.).
 - 4. Date issued/acquired.
 - 5. Location of item.
 - 6. Division or employee to whom the item is issued.
 - 7. Date removed from service.
 - 8. Disposition.
- D.** Uniform and equipment issued specifically to one employee shall be inventoried regardless of value. The inventory system shall document the issuance of all uniform and equipment items supplied by the Department

for use by an individual employee to perform their duties. Items purchased by the employee utilizing the clothing allowance stipend shall not be placed on the inventory.

III. Procedure: Operational Readiness

- A.** All stored department property shall be maintained in a state of operational readiness. Operational readiness shall include maintenance, repair, cleanliness, and workability.
- B.** Operational readiness of stored department property shall be the responsibility of the employee to which the property is assigned. If department property is not assigned to a specific individual, the Division Commander or their designee of the division the property is assigned shall be responsible for operational readiness.
- C.** An inspection of stored department property for operational readiness shall be conducted by the Support Services Division on a semi-annual basis.
- D.** Except for personal equipment items issued to each operator, Suburban Emergency Response Team (SERT) equipment stored at the Department shall be inspected as part of the operational readiness semi-annual inspections. This shall include all items stored in the rapid deployment vehicle. The Division Commander with functional responsibility over SERT shall assign an Urbandale SERT officer or supervisor to complete the semi-annual inspections and provide the information to the Support Services Division.
- E.** Departmental firearms shall be inspected semi-annually by the range administrator or designee. The status of departmental firearms shall be provided to the Support Services Division to be included in the operational readiness report.

IV. Procedure: Property Issuance and Disposition

- A.** Any property meeting the threshold to be included in the inventory system shall be recorded prior to being placed in service.
- B.** Any property, equipment, or uniforms owned by the Department and no longer useful shall be returned to the Support Services Division. The Support Services Division shall log the date removed from service and final disposition of the item.
- C.** All uniforms and equipment owned by the Department shall be returned to Support Services Division upon ending employment. All department insignia (patches, nameplates, etc.) shall be returned to the Support Services Division. Exceptions to returning insignia may be made by the Chief of Police for use in retirement memorabilia.
- D.** Any department firearms, ammunition, or munitions that are no longer useful shall be disposed of by the range administrator or designee in compliance with all applicable state and federal regulations and shall be recorded in the inventory system.

Chapter 3: The Personnel Structure
Section 21: Classification and Delineation of Duties and
Responsibilities
Subsection 2: Classification



Policy/Procedure #: 1

Title: Classification

CALEA Reference#: 21.2.1, 21.2.2, 21.2.3

I. Policy: Allocation and Distribution of Personnel

The Urbandale Police Department shall utilize a job classification plan to control and track the number, type and location of all authorized positions within the Department as well as ensure each position within the Department has designated job functions and workloads that are commensurate to the position. The goal of the classification plan is to provide an equitable, effective and efficient deployment of departmental human resources.

II. Procedure: Classification Plan

A. The Department shall operate under the classification plan adopted by the City of Urbandale for all city employees.

B. The classification plan for employees shall at a minimum contain the following:

1. Categorization of each job by class on the basis of similarities in duties, responsibilities, and qualifications.
2. Specifications for each class.
3. Provisions for relating compensation to classes.
4. Provisions for reclassification.

III. Procedure: Job Descriptions

A. Job descriptions for all full and part time positions within the Department to include reserve police officers shall be kept current and made available to all personnel through the Power DMS document management system and the appendix of the Operations Manual.

B. To ensure job descriptions are maintained, the Chief of Police or designee shall complete a documented review a minimum of once every four years.

IV. Position Management System

A. The Department shall maintain an updated position management system. The system shall contain the following information:

1. The number and type of each position authorized by the Department's budget.
 2. The location of each authorized position within the Department's organizational structure.
 3. The status of all authorized positions, filled or vacant.
- B.** The position management system shall be maintained by the Support Services Division.

Chapter 3: The Personnel Structure
Section 22: Personnel Management System
Subsection 1: Compensation



Policy/Procedure #: 1

Title: Compensation & Benefits

CALEA Reference#: 22.1.1, 22.1.2, 22.1.3, 22.1.4, 22.1.7

I. POLICY: Compensation & Benefits

The Urbandale Police Department shall offer a comprehensive compensation and benefits package to all full-time employees. The compensation and benefits shall be competitive with other police agencies in the Des Moines metro area and the State of Iowa. As part of their employment benefits and due to the stressful nature of the police environment, employees are offered several options to assist in handling stress as outlined in this policy.

II. Procedure: Compensation

- A.** Salary compensation for sworn full time police officers with the department shall be stated in the current agreement between the city of Urbandale and the Urbandale Professional Peace Officers Association represented by the International Brotherhood of Teamsters Local 238 (Teamsters Local 238).
- B.** Compensation for non-union full-time employees including full time sworn officers at the rank of sergeant or above shall be stated in city of Urbandale employment policy to include salary differential between the ranks.
- C.** Any compensation for sworn full time police officers for special skills shall be clearly stated in the labor agreement between the city of Urbandale and Urbandale Professional Peace Officers Association represented by Teamsters Local 238.
- D.** Any compensation for non-union full-time employees including full time sworn officers at the rank of sergeant or above for special skills shall be stated in city of Urbandale employment policy.
- E.** Compensatory reimbursement, overtime compensation, and any salary augmentation shall be stated in the current agreement between the city of Urbandale and the Urbandale Professional Peace Officers Association represented by Teamsters Local 238.
- F.** Employees executing duties that may result in overtime compensation, compensatory reimbursement, or other forms of salary augmentation are required to obtain supervisory approval prior to beginning such

assignments. This process ensures that all additional compensation is properly authorized and documented in accordance with city and departmental procedures.

However, there are circumstances where prior supervisory approval may not be feasible. In situations that are active or critical in nature—where immediate action is necessary and seeking approval beforehand is impractical—employees may proceed without prior supervisory authorization. Upon completion of the task, supervisory personnel shall be notified as soon as practical. These exceptions are intended to support timely and effective responses during urgent operational needs while maintaining compliance with department guidelines.

III. Procedure: Benefits

- A.** The benefits for sworn full time officers with the department shall be stated in the current agreement between the city of Urbandale and the Urbandale Professional Peace Officers Association represented by Teamsters Local 238 or the city of Urbandale employment policy.
- B.** The benefits for non-union full-time employees including full-time sworn officers at the rank of sergeant or above shall be stated in the city of Urbandale employment policy.
- C.** Retirement and/or disability/death benefits for full time sworn officers shall be administered by the Municipal Fire and Police Retirement System of Iowa. Any additional retirement and/or disability/death benefits shall be stated in the city of Urbandale employment policy or the current agreement between the city of Urbandale and Urbandale Professional Peace Officers Association represented by Teamsters Local 238.
- D.** Retirement and/or disability/death benefits for all non-sworn full-time employees shall be administered by the Iowa Public Employees Retirement System. Any additional retirement benefits shall be stated in the city of Urbandale employment policy.
- E.** The city of Urbandale offers health insurance coverage to full time employees of the department. Details of health insurance coverage and the costs to the employee shall be listed in the city of Urbandale employee benefit plan or the current agreement between the city of Urbandale and the Urbandale Professional Peace Officers Association represented by Teamsters Local 238.
- F.** All employees are protected against civil litigation as mandated by Chapter 670 of the Iowa Code when acting within the scope of their employment or duties. In addition, employees are covered by the city of Urbandale's insurance carrier.
- G.** Full-time sworn officers shall receive educational benefits as stated in the agreement between the city of Urbandale and the Urbandale Professional Peace Officers Association represented by Teamsters Local 238. Full-time sworn officers at the rank of sergeant or above and all other employees of the department shall receive educational benefits as stated in the city of Urbandale employment policy.

- H. Employees injured on the job and are unable to return to their regular job classification upon returning to work shall be afforded the benefits of the city's return to work program. The details of the program are covered by the return-to-work policy. Employees injured while outside of work shall be offered the return-to-work program on a case by case basis. The chief of police shall be responsible for administering the return to work program for the department under the guidelines established by the city of Urbandale.

IV. Procedure: Support for employees

- A. Stress can be a physical, mental, and emotional reaction to situations caused by change, confusion, danger, excitement, fear, irritation, or uncertainty. The department recognizes persons employed in police service are engaged in a high stress profession and an employee's physical or mental health may be impaired as a result of the negative effects of stress. It is the policy of the department to assist employees to understand and cope with such stress by providing counseling under certain circumstances. These circumstances may include but not be limited to:
1. Incidents resulting in serious injury or death to an employee.
 2. Incidents resulting in serious injury or death to a citizen.
 3. Incidents resulting in an employee being exposed to a potential for extreme physical harm.
- B. When an employee is involved in a duty-related incident as described above, the following procedure may be initiated:
1. Based on the incident and a supervisor's observations of an employee's reaction, the employee may be required to meet with his immediate supervisor or division commander for a debriefing and to assess the need for professional counseling. This meeting should occur as soon as practical after the incident.
 2. If the assessment determines counseling is not needed, a memorandum stating the supervisor's findings shall be forwarded to the chief of police. Periodic inquiries with the employee may be needed based on the supervisor's observations to determine if counseling might be needed at a future time.
 3. If counseling is deemed necessary, the supervisor or the division commander shall draft a memorandum to the chief of police stating their recommendation the officer visit a counselor. If other action such as a temporary change in duty assignment or time off is needed, those recommendations shall also be forwarded through the chain of command to the chief of police.
 4. The chief of police may request the counselor provide a confidential report of his findings and any recommendations to the chief of police to ensure the officer is able to return to full duty.
- C. Costs associated with required counseling from a duty related incident shall be paid by the department.
- D. Employees may have a need for counseling for reasons not associated with a duty related incident such as marital problems, financial difficulty, family health issues, etc. When a supervisor observes an employee

having difficulties for issues not associated with a duty related incident, the supervisor shall interview the employee in an effort to determine the cause and to discuss the possible need or benefit of professional counseling. Recommendations concerning counseling shall be forwarded through the chain of command to the chief of police.

- E. Recommendations will be reviewed by the chief of police, the employee's supervisor, and division commander. After review, the employee may be recommended or ordered to seek counseling.
- F. If ordered to obtain counseling, the division commander of the employee will schedule the initial appointment and determine if the city's Employee Assistance Program (EAP) can be utilized.
- G. When ordered to obtain counseling and the counseling will be obtained through EAP, the department shall be responsible for payment of the initial evaluation and any other permissible sessions as stated in the city of Urbandale's contract with EAP. Any additional sessions will be the responsibility of the employee. If unable to obtain services from EAP the employee shall be responsible for all costs associated with the counseling.
- H. If an employee is recommended to seek counseling but not ordered, all costs will be the responsibility of the employee. The employee may use the services provided in the city's EAP, which may offer initial counseling for no cost.
- I. All records concerning professional counseling ordered by the department shall be kept confidential. Such records will be maintained by city of Urbandale Human Resources Department.

V. Procedure: Employee Assistance Program

- A. The city of Urbandale and the Urbandale Police Department shall offer an Employee Assistance Program (EAP) to all employees.
- B. EAP services are offered by Employee and Family Resources and their services are described in detail on their web site. Employees wishing to utilize this service may go to the website at [Employee & Family Resources](#) and select employee assistance programs or by calling (800) 327-4692.
- C. Any request for assistance to EAP by an employee not required by the department shall be completely confidential and no records of such services shall be obtained by the department.
- D. Services offered by EAP shall be delivered appropriately in a timely manner. Any problems with the services offered by EAP may be forwarded to a supervisor. This may be done anonymously to ensure confidentiality.
- E. Cost for initial consultation, services, and counseling through EAP shall be covered by the city of Urbandale. Any cost for additional consultation, services or counseling shall be clearly stated to the employee prior to receipt.
- F. Supervisors for the department shall receive training as to the services offered by EAP, the supervisor's role and responsibility in referring employees for assistance, and how to identify employee behaviors which may indicate problems or issues affecting job performance.

VI. Critical Incident Stress Management

- A.** Critical Incident Stress Management (CISM) is a comprehensive, systematic and multi-component approach for the reduction and control of harmful aspects of stress. The department may use CISM response teams from the Red Cross that are trained and available to assist in the event of a critical incident.
- B.** Critical Incidents include, but are not limited to; life threatening events, severe injury or death of a child, family member, or coworker, traffic fatality, suicide, homicide, mass casualty incident, or any other critical incident creating traumatic stress.
- C.** All employees react differently to traumatic stress events. The differences in reactions are based on each employee's life experience, previous responses, the duration of time on scene, extent and proximity of their involvement, severity of the scene, degree of injury or loss, their individual coping mechanisms, and available family, social, or coworker support.
- D.** Any employee may request CISM services through the chain of command to the chief of police. The chief of police shall evaluate the request for CISM support and may request assistance from a CISM Team.
- E.** If contacted by the department, the CISM Team will assist command staff in evaluating the critical incident and assist in preparing a plan for providing stress management services in accordance with the circumstances of the traumatic event and those involved.
- F.** Based on the recommendations of the CISM Team, the chief of police shall determine what action to take, up to and including no action. Not all critical incidents require CISM support services.
- G.** Critical Incident Stress Management support may include, but is not limited to:
 - 1. Individual Services (One-On-One):** Services for an individual employee who experienced a traumatic event.
Timing: Anytime post event as needed. Provided by a trained peer.
 - 2. Rest Information & Transitional Services (RITS):** Services for a group of employees engaged in a large scale ongoing traumatic event or disaster, in order to share up-to-date information, provide rumor control, assess employees and provide preliminary support as necessary. RITS is not considered a standalone stress intervention.
Timing: Prior to employees being released from duty intended to increase group cohesion. Provided by command staff and may be supported by CISM trained peers or CISM Team, (30 minutes in duration). RITS is not considered a standalone stress intervention.
 - 3. Defusing:** Intended for a small group of responders directly involved in a traumatic event. The defusing is a shortened version of the Critical Incident Stress Debriefing (CISD) with three phases: Introduction, Exploration, and Information. Defusing shall not be utilized in response to a line-of-duty death.

Timing: 2-8 hours post event to mitigate the impact of the traumatic incident. Provided by trained peers or CISM Team (20-30 minutes in duration).

- 4. Critical Incident Stress Debriefing (CISD):** Intended to support those directly involved in response to a traumatic event. The CISD is a seven (7) phase process of Introduction, Facts, Thoughts, Reactions, Symptoms, Teaching and Re-entry. When utilized, CISD shall be provided by trained CISM Team. Officer(s) who discharged a weapon in a loss of life event should not take part in the CISD. The officer should see a psychologist and may participate in a one-on-one session with a CISM trained peer.

Timing: May be most effective 24-72 hours post event; however, sometimes provided 5-10 days post event. (1-2 hours in duration).

- H.** Any costs for CISM will be the responsibility of the department or the city of Urbandale.
- I.** Other groups or individuals offering critical incident stress debriefings such as Iowa COPS, individual psychologists, or other appropriate groups may be utilized in lieu of the Red Cross. The determination of which group or individual is appropriate shall be determined by the chief of police.
- J.** Except for instances in which safety for the employee or others is a concern, the content of CISM activities shall not be reported to staff members or human resources. The confidentiality of these meetings is meant to foster open and honest discussions on difficult topics and feeling.

VII. Peer Support Team

- A.** The Peer Support Team (PST) provides a confidential, safe and supportive environment for department personnel and their families. It facilitates individual families in coping more effectively with the multitude of stressors experienced during the course of their, or their loved ones, public safety professions. The PST is dedicated to the prevention and/or reduction of marital problems, substance abuse, suicide, and psychological symptoms that may be caused or exacerbated by stress related to our profession.
- B.** The PST is guided by the philosophy peers are in the best position to help other peers to recognize and acknowledge work-related stress and to facilitate an intervention before the problem becomes life or career threatening.
- C.** PST members are not licensed counselors but offer a safe and trusting opportunity for employees and their families to discuss emotional issues with someone they trust and who can understand their struggles.
- D.** Support offered by PST members includes emotional support (trust, esteem, and fellowship), appraisal support (affirmation and feedback), instrumental support (basic needs and safety), and informational support (information, advice, direction and referral).
- E.** PST members shall be considered a collateral duty and shall follow the selection process outlined in chapter 2 section 16.2.1 (Temporary, Specialized, and Collateral Duty Assignments) of the Operations Manual.

- F.** The PST shall be managed by a peer support coordinator. The peer support coordinator shall act as the primary liaison for the PST and the department's command staff and shall be appointed to the position by the Chief of Police. The peer support coordinator shall ensure the PST is functioning as intended. The peer support coordinator shall be responsible for the following:

 - 1. Oversight of the program.
 - 2. Coordination of training meetings to ensure competency of PST members.
 - 3. Assignment of PST members to incidents.
 - 4. Ensuring PST members are following up on referrals.
- G.** PST members provide support and assistance to employees and/or their immediate family in time of stress and/or crisis. The PST members shall be responsible for the following:

 - 1. Conveying trust, anonymity, and assure confidentiality within policy guidelines to employees who seek assistance from the PST.
 - 2. Providing assistance and support to peers.
 - 3. Assisting the employee(s) by referring him/her to the appropriate and viable referral resource, such as the Employee Assistance Program (EAP) or professional counseling services, when necessary.
 - 4. Being available to the employee for follow-up support.
 - 5. Maintaining contact with their peer support coordinator.
 - 6. Agreeing to be contacted and, if practical, respond at any hour.
- H.** Peer support team members may be called out in response to a critical incident. The peer support team response shall be conducted in a manner that does not interfere with an active investigation. Critical incidents where a PST response is appropriate include, but are not limited to: life threatening events, severe injury or death of a child, family member or coworker, traffic fatality, suicide, homicide, mass casualty incident, or any other critical incident that creates traumatic stress.
- I.** The PST member is authorized to use department facilities to meet with an employee while on duty with appropriate supervisory approval.
- J.** Participation as a PST member as well as a recipient of services shall be a strictly voluntary. PST members will receive appropriate compensation for any time spent completing PST assistance.
- K.** The acceptance and success of the Urbandale Police Department PST shall be determined, in part, by observance of confidentiality (See State Code 622.10(9)). It is imperative that each PST member maintain strict confidentiality of all information learned about an individual within the guidelines of this policy.
- L.** The policy of the department's PST is to maintain confidentiality. Communication between the PST members and an employee is considered confidential except for matters which involve the following:

 - 1. Danger to self

2. Danger to others
 3. Suspected child or elder abuse
 4. Narcotic offenses
 5. Domestic violence
 6. In cases where law requires divulgence.
 7. Where divulgence is requested by the employee seeking services.
- M.** A general principle for PST members to follow is to inform the person, prior to discussion, what the limitations and exceptions to confidentiality are regarding the information revealed. In cases where a concern or a question regarding confidentiality arises, the PST member shall immediately contact the peer support coordinator for further advice or action.
- N.** Personnel providing peer support services should receive training commensurate to their responsibilities. This may include access to referral resources, interview and counseling strategies, signs and symptoms of mental health distress or illness, communicating with families and significant others, confidentiality and information sharing, intervention techniques, and criteria for required action such as notification of other professional services when the subject displays suicidal behavior.
- O.** The peer support coordinator shall complete an annual report to the chief of police. The report shall document the number of contacts made (NO NAMES), general topics discussed, time allocated, and referrals made by the PST. The report shall be utilized as a means to improve the services of the program and to assist the department with identifying general trends that may need to be addressed on a department wide basis. NO NAMES OR ANY IDENTIFIABLE INFORMATION WILL BE DOCUMENTED.

Chapter 3: The Personnel Structure
Section 22: Personnel Management System
Subsection 2: Compensation & Benefits



Policy/Procedure #: 5

Title: Employment Related Critical Injury or Death

CALEA Reference#: 22.1.4, 22.1.5

I. Policy: Employment Related Critical Injury or Death

A policy is established to guide the department in the event an employee is killed or critically injured performing work-related duties. The department shall provide proper emotional care for an injured or deceased employee's family and department members through carefully planned procedures.

II. Procedure: General

- A.** The department has the responsibility to provide liaison assistance to the immediate family of an employee who is critically injured or dies while performing work-related duties. This responsibility includes providing emotional support for the employee's family during this traumatic period.
- B.** A work-related critical injury or death includes any action, felonious or accidental which critically injures or claims the life of an employee who was performing work-related functions while on or off duty. The chief of police may activate all or part of this policy for cases in which an employee is critically injured while performing work-related functions or suffers death/critical injury when not performing work-related functions.
- C.** If an officer with the department is killed performing work-related duties, officers shall be assigned to stand constant guard with the deceased officer until funeral services are concluded. The chief of police may request a guard for other employees who are critically injured or have died performing work-related duties and also for employees critically injured or who have died but not during work related duties.
- D.** Timely grief counseling shall be provided to members of the department including additional counseling services as needed provided by EAP or other services.
- E.** The surviving family should hear of the death from a department representative first, not from the press or other sources. A notification team shall be assembled as quickly as possible to deliver a work-related death notification. The following procedures shall be used:

1. The chief of police shall determine who shall be on the notification team. The chief of police and another supervisor, preferably the division commander of the employee critically injured or killed should be assigned to the team. The station is the preferred place to gather and prepare for the notification. Timeliness of the notification is of the essence. If the chief of police is not immediately available to make this designation, the responsibility shall remain with the ranking supervisor who has been notified of the injury or death.
2. When the notification involves a death, one of the Urbandale Police chaplains should be part of the notification team. When the notification involves a critical injury, a supervisor shall determine if a chaplain is needed.
3. Prior to contact with the family, the notification team shall review the information so they all know the circumstance and the parties involved. The accuracy and completeness of the information will be verified at this time. The notification team shall familiarize themselves with essential details of the critical injury or death, location of the deceased employee and their personal effects, and other pertinent information.
4. Determine who will do the sharing of information with the family. The chief of police should make the notification to the family. The chaplain may be relied upon to assist the chief of police or his designee when the chief is unavailable to make the initial notification.
5. Emergency contact information on file with the department should dictate the first family member to be notified. If no emergency contact information is on file, particular efforts should be made to locate the closest family member starting with a spouse and followed by adult children, parents, brothers, sisters, and then minor children. Family dynamics such as estrangement and divorce may be considered when locating the closest family member. Only where substantial delays would be required to make contact with the family listed above should the order of notification be altered. The chief of police shall decide when doubt exists concerning whom to notify.
6. Time is of the essence when making a notification. Delays in the notification process should not be made unless information is not sufficient to make a proper notification or an emergency situation exists. Any unusual delay in notification shall be approved by the chief of police.
7. If an employee is critically injured and not expected to survive, every effort will be made to get the family to the hospital prior to the employee's death. This will include expediting the notification process.

III. Procedure: Notification

- A. All work-related death notifications shall be delivered in person to the family. Critical injury notification may be made by other means if necessary.
- B. In the event of a critical injury or death, external monitoring of the police radio frequencies will be extensive. Whenever possible, communications

regarding notifications should be restricted to the telephone and/or person to person. The name of the injured or deceased employee must never be released to the media before immediate family living in the region are notified. If the media already has the employee's name, they should respond to a request to withhold this information, pending notification of the family.

- C. The notification team shall use the following procedure when making a work-related critical injury or death notification:
1. Go to the residence or place of employment of the family member to be notified. Check the accuracy of the location to ensure you are at the correct address.
 2. Identify yourselves and ask to be admitted to the residence. If this is a place of employment, ask for a room where you can have privacy. Request to speak to the person to whom notification is to be made. If the slightest doubt exists, ensure you have the correct person by verifying the relationship of the survivor to the employee.
 3. Every reasonable effort shall be made to make the notification in the privacy of the family's home or in another location away from public scrutiny.
 4. Prior to making notification, the supervisor or the chaplain should bring members of the family together who may be in the house or otherwise on hand. If possible, have family members seated for the notification to avoid any injuries. In calm, direct, adequate but not lurid detail, explain what has happened (e.g. "There was an accident at _____, and _____ was involved. Their injuries were so severe they were killed"). If we say, "They did not survive", the family may not grasp what we are trying to say in the emotion of the moment. Team members should be cognizant not to use police terms or jargon when making the notification. Team members should refer to the employee using his/her first name or terms reflecting the employee's relationship to the survivor (i.e. son, daughter, etc.).
 5. Wait for the information to sink in and then be ready to answer as many questions as possible. Most family will inquire for more details on exactly what happened, where it occurred, if they can go to the scene, where their family member is now, etc.
 6. In many incidents it will be necessary to say we are not sure exactly how the incident occurred, a full investigation is ongoing and we will let them know as soon as possible.
 7. Tell them "John is at the medical examiner's office in Ankeny," not "The body is at the medical examiner's office."
 8. The chaplain should ask if they have a clergy person he/she may contact (a list of all Urbandale clergy is included with the death/serious injury/illness notification information form), if there are family and friends we can call for them, or if there are neighbors they would like us to contact. Our goal is to serve the family and give them support in this very difficult time.

9. Stay with the family until you are confident they are emotionally stable and they have some support system with them. The chief of police may assign an officer to stay with the family. Under normal circumstances, no family member should be left alone. Family, friends, co-workers, neighbors, clergy, crisis counselors or other community social service agencies may also relieve the notification team (If a family member leaves the room, keep track of them. In this emotional time, we do not want anyone to harm themselves in their immediate grief.). In gauging the need for assistance, the notification team shall consider the following:
 - a. The emotional reaction and physical condition of the survivor.
 - b. The availability of other adults in the home.
 - c. Responsibility for infants or small children.
 - d. Availability of a support system (e.g. including friends, family, close friends, access to clergy, etc).
- D. If the incident dictates the need to go to the hospital, transportation shall be provided by the department. If the family refuses this service and insists on driving themselves, a representative from the notification team may ride with the family. Other members of the notification team should follow the family to the hospital. The notification team shall notify the ranking officer at the hospital when the family will be arriving (by phone if possible).
- E. Personal effects of the deceased employee shall not be delivered to family at the time of death notification.
- F. Notification team members should be prepared for unexpected responses from family to include hysteria and possible verbal or physical attack.
- G. Notification team members should remain alert to the possible need for medical assistance. When officers are aware of serious medical conditions in advance of notification, they should place a local medical response unit on alert. This includes, but is not limited to, whether families are elderly, disabled, visually or hearing impaired, or have medical issues. If possible, obtain the names of the survivor's closest relative, friend, family doctor and clergy.
- H. Similar procedure shall be used to make notifications regarding critical injury.
- I. When able, the notification team should regroup at the station following a notification in order to debrief and decompress.
- J. Written documentation of the notification shall be assigned to a member of the notification team.

IV. Procedure: Requesting Notification From Another Agency

- A. Only when it is impossible to make timely notification to the family of an employment related death shall another agency be requested to assist.
- B. When another agency must be contacted to notify the family of an employment related death for the department, supervisors shall:

1. Speak to the specific personnel that will be making the notification. This will decrease the chance for miscommunication or errors being made during the transfer of information.
2. Request the notification be made in person.
3. Request immediate verification when notification has been accomplished.
4. Furnish as much information as possible based on the incident being mindful of the confidentiality of certain investigations.
5. Exchange contact information with the personnel you are requesting to do the notification including the name, address, phone number, etc.

V. Procedure: Assistance at the Hospital

- A. The first ranking officer to arrive at the hospital shall become the hospital liaison officer until relieved of this duty. This officer is responsible for coordinating the arrival of immediate family, police officials, the press, and others.
- B. The responsibilities of the hospital liaison officer shall include:
 1. Arrangements with hospital personnel for appropriate waiting facilities. There should be segregated areas reserved for family.
 2. Ensure the waiting room for family is restricted to family, the chief of police, notification team members, and others as requested by the family.
 3. Arranging for a separate area or room for fellow officers, department staff, and friends.
 4. Designate a press staging area.
 5. Ensure medical personnel communicate pertinent information on the employee's condition to the family first.
 6. Arrange transportation for the immediate family and others from the hospital to their residence.
 7. When possible, the family should be allowed to see the employee as soon as possible. Medical personnel should make the family aware of hospital policy about visiting a trauma patient or viewing the deceased employee.
 8. A representative from the department should be present with the family the entire time at the hospital to arrange assistance as needed for the family.

VI. Procedure: Family Support during the Wake and Funeral

- A. Within twenty-four (24) hours of death, the chief of police shall designate a family liaison officer, a benefits coordinator, a family support advocate, and a department liaison (usually the appropriate division commander). These designations shall be announced to employees in writing. All referrals will be made according to areas of responsibility. The chief of police will personally notify the surviving family of the designated choices.
- B. The department liaison is normally filled by a division commander and shall have the following responsibilities:
 1. The department liaison shall direct the funeral activities of the department and visiting law enforcement agencies, according to the

wishes of the family. The IOWA Concerns of Police Survivors (COPS) and the Iowa Chiefs Association may be called upon to assist.

2. The department liaison will work closely with the family liaison officer to ensure the needs and requests of the family are fulfilled regarding the funeral arrangements.
 3. Expedient application of all needed department resources.
 4. Gather a comprehensive list of alternate churches and reception halls with seating capacities able to accommodate attendance of a law enforcement funeral. This information is given to the family as soon as possible to help them decide on a location. The final choice remains with the family.
 5. Coordinating all official law enforcement notifications and arrangements for the funeral, including honor guards, pallbearers, traffic control and liaison with visiting law enforcement agencies.
 6. Liaison with the media through the public information officers. An officer should be posted at the family's residence for security and to control the media. In the unlikely event the family decides to accept an interview, with the family's permission, a ranking officer should attend and "screen" all questions presented to the family so upcoming legal proceedings are not jeopardized.
 7. Arranging routine residence checks of the family's home for 6-8 weeks following the tragedy. This service is necessary since large amounts of money may pass through the residence and the family may be spending much time away from the home with legal matters. This may require outside liaison with other jurisdictions. Family members shall be made aware of the increased presence around their residence.
- C. The family liaison officer acts as a facilitator between the surviving family and the department during the wake and funeral. The position requires the officer to have a good knowledge of the family relationships, but not be so emotionally involved with the loss he/she would become ineffective. The family liaison officer need not be a ranking officer and may be the police chaplain.
- D. The family liaison officer shall report to the department liaison and shall have the following responsibilities:
1. Being constantly available to the family throughout the wake and funeral.
 2. Ensuring the needs of the family come before the wishes of the department.
 3. Meeting with the family and funeral director regarding funeral arrangements. Since most employees have not prearranged their wishes for the handling of their own funeral, these decisions should remain with the family. The family liaison officer should only make the family aware of what the department may offer in the way of assistance and resources based on information from the department liaison.
 4. Relaying all available information to the surviving family concerning the circumstances of death and any continuing investigation. Law

enforcement is traditionally hesitant to release this type of information, particularly in sensitive homicide cases. The family liaison officer should coordinate with investigating officers and prosecutors to ensure the family receives as much allowable information during the first few days as possible. Being "kept in the dark" is a common complaint of surviving families.

5. Determining the travel arrangements needed for out-of-town family members or other special needs during the funeral. This information must be forwarded to the department liaison.
 6. Ensure the family is fully aware of any law enforcement funeral procedure and obtaining family approval (e.g., twenty-one gun salute, presentation of the flag, playing of taps, etc.)
- E. The chief of police will designate a ranking officer to act as benefits coordinator. The benefits coordinator is responsible for:
1. Notifying the appropriate hospital personnel billing for medical services concerning employment related death shall be directed to the city of Urbandale. If an employment related death, the family should not receive any of medical bills related to the incident at their residence. The benefits coordinator should contact the hospital during normal business hours to ensure proper billing takes place. If death is a result of off-duty enforcement action a determination will be made as to where billing for such services should be forwarded.
 2. Filing worker's compensation claims and related paperwork.
 3. Gathering information and assisting the family in applying for any benefits/funeral payments available to the family, including the public safety officer's benefits act provided by the United States Justice Department.
 4. Fielding all phone calls and inquiries regarding the establishment of any special trust funds or educational funds.
 5. Communicate the distinction between benefits, (which are financial payments made to the family to ensure financial stability following the loss of a loved one) and funeral payments, (which are funds specifically earmarked for funeral expenses).
 6. Preparing a comprehensive document of the benefits/payments due to the family, listing named beneficiaries, contacts at various benefits offices and when they can expect to receive the benefit.
 7. At the family's request, filing all benefit related paperwork and following through with the family to ensure the benefits are being received. Offer information as to a potential need for consultants or attorneys and assist the family in working with benefit providers.
 8. Special attention should go to the possible loss of health benefits. The family will be assisted in securing health insurance/benefits working with the human resources department of the city.
 9. Advise the surviving family of the role of law enforcement associations and organizations such as Heroes, Inc. in making their attorney/financial counselor available to the surviving family for

whatever legal/financial counseling is necessary, (e.g. establishing trust funds, educational funding, etc.) This attorney should not be affiliated with the city of Urbandale and should work as an advocate for the family.

10. A division commander may serve as a benefits coordinator in addition to being the department liaison.
- F. The chief of police shall designate a family support advocate from the department to act as a long term liaison with the surviving family. The family support advocate should have extensive experience dealing with crime victims and witnesses. This position will normally go to the victim/witness coordinator for the department. The family support advocate's responsibilities include:
1. Constant contact with the surviving family to keep them abreast of criminal proceedings. The family should never learn of developments in the case from the press prior to learning them from the department.
 2. Accompanying the surviving family to any criminal proceedings. Introducing them to prosecutors and answering any questions they may have concerning the criminal trial.
 3. Ensuring the family has referral and contact information to all appropriate outside peer groups specific to an employment related death. The family support advocate shall facilitate any family request to contact or join these support groups.
 4. Ensuring the surviving family does not feel isolated by the department and is kept abreast of any activities honoring their family member or other department activities after the funeral.
 5. Encouraging others to make visits or help with needs of the surviving family. Care should be taken that promises are not made to the surviving family that cannot be honored.
 6. The family support advocate shall not have a set time limit for assisting the family. Each case will depend on the surviving family and how they "recover" from this traumatic event. The grief process has no timetable. Families may experience a complicated grief process.
 7. Family members should continue to feel like they are part of the "law enforcement family" for which the employee gave his/her life. The family support advocate should keep in touch with the family with phone calls through the first year. The needs of the family usually dictate the frequency of contact.
 8. The chief of police, family support advocate, and others will ensure the anniversary date of the employee's death is observed including appropriate contact to the family (e.g. visit, phone call, card, etc.) and adequate support is given to the family during the holidays particularly during the first year.

Chapter 3: The Personnel Structure
Section 22: Personnel Management System
Subsection 1: Compensations & Benefits



Policy/Procedure #:6

Title: Department Issued Clothing and Equipment

CALEA Reference#: 22.1.6, 41.3.4

- I. Policy: Department Issued Clothing and Equipment**

A policy is established to regulate and standardize the clothing and equipment issued to employees by the Urbandale Police Department.
- II. Procedure: Department Issued Clothing and Equipment**
 - A.** All clothing and equipment issued to employees by the department and available for employees to purchase shall be listed on the master clothing and equipment checklist. The Support Services Division shall be responsible for maintaining a comprehensive master clothing and equipment checklist. The checklist shall indicate the following:
 - 1. Item name.
 - 2. Quantity to be issued or maintained.
 - 3. Restrictions on issuance based on job assignment.
 - 4. Specifications for the item.
 - 5. Approved vendor (if applicable)
 - B.** If deemed a suitable replacement, an employee may request to purchase items in lieu of items specifically listed on the clothing and equipment checklist. All such requests shall be made on interdepartmental memorandum through the chain of command to the chief of police for approval. Approval shall be obtained prior to use. A sample of the item may be requested prior to purchase to ensure uniformity and quality. Approval shall only be granted if the replacement item has the same specifications, quality, and meets uniformity requirements of the item listed on the clothing and equipment checklist and there is valid reason why the department specified item is not a viable option.
 - C.** Clothing and equipment issued by the department to employees may be new or used based on departmental inventory. In order to maintain a professional appearance, supervisory personnel shall have the authority to require an employee to replace or repair worn or damaged clothing and equipment.

- D.** With approval of the chief of police, division commanders shall regulate clothing and equipment items to be worn in the performance of divisional duties. Any divisional order regulating clothing or equipment shall be administered uniformly to all employees affected.
- E.** The department shall provide newly hired or newly assigned employees with the clothing and equipment listed for their position in the master clothing and equipment checklist. Clothing and equipment provided by the department shall be placed on the department inventory system by the Support Services Division as stated in chapter 2 section 17.5.1 of the Operations Manual. Clothing and equipment items shall be issued by the Support Services Division; however, each division may have specific clothing or equipment in their control that is issued to an employee. When this occurs, the supervisor of the employee shall be responsible for reporting the issuance to the Support Services Division along with any pertinent data needed for entry in the department inventory system.
- F.** Except for personal items as noted in the police union contract, each employee shall be responsible for replacement or repair of department issued clothing or equipment items due to wear or loss. Damage or loss of department issued clothing or equipment items due to negligence may result in disciplinary action.
- G.** If clothing or equipment items are damaged while in the performance of assigned duties, they shall be replaced by the department within the boundaries established by the police union contract.
- H.** All clothing and equipment items purchased by the department, as listed on the master clothing and equipment checklist, shall be returned to the Support Services Division upon ending employment with the department. Any employee failing to return said items may receive a bill for replacement cost of the item(s) from the department or the city of Urbandale.
- I.** Any clothing or equipment provisions stated in the current union labor contract shall apply to all sworn full time personnel.
- J.** To ensure uniformity and prevent the use of substandard items, personal equipment and apparel for use by personnel shall be issued by the department upon employment. Replacement of said items shall meet the requirements listed in the master clothing and equipment checklist. Sworn employees receiving the annual clothing allowance shall be responsible for replacing clothing and equipment items as needed.
- K.** Any undergarments not visible while wearing the uniform are exempt from this policy.
- L.** Uniformed officers including reserve officers may use personally owned items and apparel if specifically approved by the patrol division commander. Unless specifically listed on the master clothing and equipment checklist, uniformed officers shall submit a memorandum to the patrol division

commander listing all personally owned items and a brief description (make, model, color, size, specifications) of the personally owned item(s) they are requesting to carry/wear while in uniform. The patrol division commander shall note his/her approval or denial of items on the memorandum and return it to the officer. A copy of the memorandum shall be kept by the patrol division commander for reference. The patrol division commander may require an inspection of the item prior to approval. Upon notice to the officer, the patrol division commander or the chief of police may revoke the approval at any time.

M. Personally owned equipment and apparel that may be approved by the patrol division commander shall be restricted to the following items and specifications:

1. Seat belt cutter- shall have a protected blade
2. Gloves- shall be black in color and allow the user to perform necessary functions including handling of weapons
3. Winter cap- shall be black or navy blue in color with no or subdued logo. Also acceptable will be a black or navy blue headband or ear muff style cover for the ears.
4. Leather jacket- shall be black leather, "Indianapolis" style with insignia the same as department issued jackets
5. Flashlight- shall be dark in color and no larger than department issued flashlights
6. Handcuffs- shall meet department specifications
7. Handcuff case- shall meet department specifications but may be a double handcuff case of the same type or a strap type holder.
8. Magazine carrier- shall meet department specifications
9. Portable radio holder- shall meet department specifications
10. Sunglasses and jewelry- shall conform to the specifications in chapter 3 section 26.1.1A (Appearance Guidelines) of the Operations Manual. Sunglasses and jewelry meeting policy requirements do not need approval from the Patrol Division Commander
11. Firearms- shall conform to the specifications in chapter 1 section 1.3.9 (Firearms) of the Operations Manual. Per policy, firearms shall be approved by a range instructor and the range administrator. No approval from the Patrol Division Commander is necessary.
12. Duty Knife- shall conform to the specifications in chapter 1 section 1.3.9 (Firearms) of the Operations Manual.
13. Secondary firearm holster- shall be concealable, securely hold the weapon, and approved by the range administrator as stated in chapter 1 section 1.3.9 (Firearms) of the Operations Manual.

N. Non uniform clothing and apparel bearing the department logo/insignia shall be approved by the chief of police. Employees are not restricted to wearing items to work functions only; however, employees shall use sound judgement about the appropriateness of wearing/using department logo/insignia items when not working. Employees wearing and using department logo/insignia items may give the appearance of representing the Urbandale Police Department to the public. Public perception will dictate representation not the employee's intention and Chapter 3 Section 26.1.1 (Department Rules and Regulations) shall apply. Employees wearing/utilizing department logo/insignia items while on or off duty shall conduct themselves at all times in such a manner as to reflect most favorably on the department. Improper conduct of an employee shall include that which impairs the morale of the department, causes the public to lose confidence or respect in the department, or impairs its efficient and effective operation.

Chapter 3: The Personnel Structure
Section 22: Personnel Management System
Subsection 1: Compensation & Benefits



Policy #: 6(A)

Title: Appearance Guidelines

CALEA Reference 22.1.6

I. Policy: Appearance Guidelines

A policy is established to mandate grooming and appearance standards for employees of the Urbandale Police Department. It is the policy of the Urbandale Police Department to require all members to present a favorable appearance to the public we serve. All department personnel shall present a well-groomed, clean and neat appearance while on duty.

II. Rules and Regulations: Grooming

Except where stated, the grooming standards shall apply to all employees.

A. Female hairstyles for sworn officers:

1. Except for a single ponytail, hair styles shall not hang below the bottom of the collar on the back and shall be no longer on the side than the back edge of the jaw bone.
2. Hair exceeding the above length may also be worn in a secure knot or bun on the top of the head accommodating the wearing of the uniform hat.
3. Hair will be worn in a neat manner which does not detract from the wearing of the uniform.

B. Male Hairstyles for sworn officers:

1. The hairstyle shall not be more than medium length and fullness.
2. Bushy hair protruding from the sides or back of the head, when the hat is worn, is prohibited.
3. A neat pattern on the rear of the neck shall be maintained; the growth must be neatly trimmed near the collar line and shall not extend over the shirt or the coat collar.
4. The hair will be cut in a neat and proper manner which does not reflect on or detract from the wearing of the department uniform.

C. Prohibited Hairstyles for all employees:

The following hairstyles are prohibited for all employees except those in specialized units with the permission of a supervisor:

1. Mohawks
2. Punk Styles (spikes, tails, unusual colors)
3. Designs engraved into the hair or scalp
4. Hairstyles deemed to be extreme or not within the norm of professional conservative standards.

D. Sideburns:

1. Sideburns will be neatly trimmed with straight lines. The base will be a clean-shaven line and the length of the hair that constitutes the sideburns will be evenly tapered in the same manner as the remainder of the hair on the side of the head.
2. The forward and rear edges will be maintained at a vertical line. The growth shall not be more than one-half (1/2) inch in depth.
3. When no beard is present, the base of the sideburn will not extend downward beyond the line parallel to the ground and drawn horizontally from the bottom of the ear lobe. The forward and rear edges will be maintained at a vertical line and shall not exceed 1 ¼ inches at the broadest point.

E. Facial hair:

1. Acceptable facial hair styles shall include a beard, moustache, and a van dyke.
2. Acceptable beard styles shall include a moustache, facial hair on the chin and a cleanly shaven neck. Other than a van dyke style, no variation other than a full beard are acceptable.
3. All beards, moustaches, and van dykes shall be neatly trimmed with straight lines and shall not present a bushy appearance. Facial hair length shall not exceed ½ inch in length.
4. When worn alone, mustaches shall extend no lower than the imaginary line drawn horizontally from the corners of the mouth. The hair from the mustache will not extend over the upper-most edge of the upper lip. The hair of the mustache will be groomed in such a manner so as not to present a projected bushy appearance.
5. Facial hair grown for special assignments shall meet the grooming standards as established by the division commander in charge of the special assignment.
6. Officers performing honor guard assignments shall be clean shaven.

F. Tattoos, brands, and intentional scarring:

1. Visible tattoos, brands, and intentional scarring are allowable for all employees. No tattoos, brands, or intentional scarring may be visible while working if the design is deemed offensive.

2. No tattoos, brands, or intentional scarring shall be applied to the face, head, or neck unless they are completely covered by the uniform or other approved clothing.
 3. Any covers utilized for tattoos, brands, or intentional scarring must be approved by the Chief of Police.
- G.** Cosmetics: Excessive cosmetics, such as dark, heavy eye shadow, false eyelashes and heavy mascara are prohibited. If worn, cosmetics shall be moderate and natural appearing.
- H.** Fingernails: Fingernails shall be kept clean and neatly trimmed. The length of the nails shall not interfere with the requirements of the employee's assignment. Female employees may wear nail polish that presents a conservative, professional appearance.
- I.** Sunglasses: Only sunglasses presenting a conservative and professional appearance are permitted. No bright colors are permitted. If cords are worn, they will be dark blue or black. Sunglasses shall not remain on once inside of a building or during night time hours.
- J.** Jewelry:
1. Neck jewelry for sworn personnel in uniform will not be visible.
 2. Sworn personnel are permitted one ring on each hand. Wedding band and engagement ring are considered one ring.
 3. Sworn personnel: Sworn personnel may wear earrings not to exceed ½ inch in diameter. No hanging earrings are permitted. No more than two earrings in each ear are permitted.
 4. No employees are allowed nose, lip, eyebrow, or facial piercings while on-duty.
 5. Large gauge style earrings or earlobes that have been stretched to accept large gauge style earrings are not permitted.
 6. Sworn personnel are permitted one wristwatch.
 7. Sworn personnel are permitted one bracelet.
 8. No jewelry deemed offensive shall be permitted for any employee.

III. Rules and Regulations: Uniform

- A.** The uniform shall be neat, clean, and pressed. Footwear, brass, and leather items will be clean and polished. When in the presence of the public and when not wearing a uniform tie, all uniform shirts must be completely fastened except the top button. Shirt sleeves will not be rolled or turned up.
- B.** All police uniforms and uniform accessories must be approved for use through the Chief of Police. Support Services Division shall maintain a current list of approved uniforms and uniform accessories.
- C.** Police uniform requirements shall be clearly stated by the commander of each division. The Chief of Police shall have final approval of any uniform directive.

IV. Rules and Regulations: Non uniform

- A.** All employees are expected to dress appropriately for their positions and to maintain reasonable standards of neatness and cleanliness. Generally, employees shall avoid extremes and strive for a neat and business like appearance on the job. When in doubt about a particular style of clothing or grooming, an employee shall refrain from wearing that style or ask their supervisor in advance whether it is appropriate.
- B.** The clothing style for non-uniform personnel shall at minimum be business casual. Exceptions may be allowed by a division commander, the Chief of Police, or for specific assignments (e.g. defensive tactics training, narcotics).
- C.** Non uniform appearance shall include training & light duty assignments.
- D.** All clothing must be neat, clean, and in good condition.
- E.** Footwear shall be worn at all times. Shoes will be clean and polished. Any footwear deemed inappropriate by a supervisor (e.g. sandals) shall not be worn.
- F.** Officers attending official court proceedings shall be dressed in full uniform, or business attire (e.g. suit, dress, collared shirt and tie, dress type sweater and slacks, etc.). Officers working a narcotics or similar assignment may be exempt from dress requirements for court based on the type of court proceeding. Officers shall comply with requests from the prosecutor for appropriate dress requirements.
- G.** All other non-uniform clothing requirements shall be clearly stated by the commander of each division. The Chief of Police shall have final approval of any non-uniform clothing directive.

Chapter 3: The Personnel Structure
Section 22: Personnel Management System
Subsection 1: Compensation & Benefits



Policy/Procedure #:8

Title: Department Identification

CALEA Reference#: 22.1.8

I. Policy: Department Identification

A policy is established to ensure the public can identify employees of the Urbandale Police Department. The ability to readily identify employees of the Department will facilitate public confidence and create accountability for employee actions.

II. Procedure: Department Identification

- A.** The Department shall issue one official identification card to all full and part time employees of the Urbandale Police Department. The front of the card shall contain the employee's rank/title, photograph, name, identification number, and department insignia. If the employee is a sworn officer, the back of the card shall contain the employee's name, identification number, and the required H.R. 218 documentation.
- B.** Based on need, the Department may issue one official identification card to volunteers. The front of the card will contain the volunteer's title, photograph, volunteer designation, name, and department insignia. The back of the card shall contain no information.
- C.** The City of Urbandale Park and Recreation Department shall issue one identification key card to each full and part time department employee. Sworn officers may request a second identification key card. The identification key card shall serve a dual function as identification as a City of Urbandale employee and a key card to allow access to various areas of the Police Department. The identification key card shall contain the employee's rank/title, photograph, name, City of Urbandale identification number, and the City of Urbandale insignia.
- D.** When on duty or when representing themselves as an employee of the Department while off duty, all employees or volunteers shall produce their police department identification for viewing upon request. When contacting any party by telephone for work related matters, employees shall verbally identify themselves as employees of the Urbandale Police

Department. Officers are exempt from this requirement when functioning in an undercover capacity.

- E.** The Support Services Division shall be responsible for issuing, tracking, and replacing official department identification cards and City of Urbandale identification key cards. Any card that is lost, stolen, or damaged shall be reported immediately to the employee's supervisor. Requests for department identification card or City of Urbandale identification key card replacement shall be completed by memorandum and submitted to the employee's supervisor. The request to replace either card shall be forwarded through the chain of command with final approval from the Chief of Police. The Chief of Police may periodically request an audit of all department identification cards or City of Urbandale identification key cards issued. If requested, supervisors shall audit their employees and/or volunteers to verify all issued cards are in their possession.
- F.** No department identification cards or City of Urbandale identification key cards shall be produced without the authorization of a division commander or the Chief of Police.
- G.** Upon ending employment or volunteer work for the Department, all cards shall be returned to the Support Services Division. Exceptions may be made by the Chief of Police for display in retirement type displays.
- H.** At the discretion of the Chief of Police, sworn full time officers retiring from the Department may be issued identification indicating they are a retired member of the Department. When approved by the Chief of Police, H.R. 218 rights may be affixed to the back of the retired officer's identification. The retired identification card will be the same format as the department identification card with exception of "retired" added to the rank/title.

Chapter 3: The Personnel Structure
Section 22: Personnel Management System
Subsection 1: Compensation & Benefits



Policy/Procedure #:9

Title: Military Deployment and Reintegration

CALEA Reference#: 22.1.9

I. Policy: Military Deployment and Reintegration

Military deployment of personnel offers unique challenges to the employee as well as the agency. The Urbandale Police Department recognizes these challenges and is committed to making the transition to and from military deployment as seamless as possible by establishing clear procedures to be followed. It is the intent of the Department to comply with all federal and state law governing employment rights during a military deployment and reintegration.

II. Procedure: General

- A.** The provisions of this policy shall only apply to personnel with military activations exceeding 180 consecutive days for pre-deployment, deployment, and post deployment.
- B.** Employment benefits afforded personnel for military leave are outlined in the City of Urbandale Employee Handbook.
- C.** The Department and the employee shall comply with all applicable state and federal regulations in regard to employee and employer rights, responsibilities, and minimum requirements.
- D.** The military deployment checklist shall be completed by the division commander of the deployed employee and submitted to the Chief of Police upon completion. A copy of the checklist shall be provided to the accreditation manager.

III. Procedure: Point of Contact

- A.** The division commander of the affected employee shall be the point of contact within the Department. It shall be the division commander's responsibility to ensure all requirements of the policy are completed by the affected employee.
- B.** The Human Resources Director or designee shall be the point of contact for the employee reference benefits related questions.

IV. Procedure: Out processing

- A. Unless the deployment is made in emergency circumstances with little or no notice, all deployed employees shall complete the following tasks.
 - B. Employees shall participate in an exit interview with the Chief of Police and their division commander. The exit interview shall include but not be limited to the following topics:
 - 1. Projected length of deployment and anticipated date of return to employment
 - 2. Anticipated assignment changes or promotional opportunities to occur while the employee is deployed.
 - 3. Establishing means of communication with the employee while deployed (e.g. phone, email, Power DMS, etc.). To the extent possible, these means of communication shall be utilized to notify the deployed employee of department news, significant events, or promotional opportunities. If means of communication change during a deployment, it shall be the employee's responsibility to notify the Department of the change.
 - C. Except for the items listed below, the division commander for the deployed employee shall determine what agency equipment shall be submitted for safekeeping and storage:
 - 1. Agency owned firearms/less lethal weapons shall be turned over to the Range Administrator for storage and safekeeping.
 - 2. Agency owned vehicles shall be turned over to the appropriate division commander.
 - D. All other equipment required to be turned in for storage and safekeeping shall be submitted to the Support Services Division for inventory. The division commander or the Chief of Police shall determine if an equipment item shall be utilized by the Department while the employee is deployed.
 - E. Prior to departure, deployed employee shall be required to meet with a representative from Human Resources Department to review work requirements and benefits provided to the employee.
- V. Procedure: In processing**
- A. Upon returning to work following a deployment, an interview with the Chief of Police and the employee's division commander shall be conducted as soon as practical. The interview shall include but not be limited to the following:
 - 1. Update on the current state of the Department and any other relevant news.
 - 2. Training requirements to be completed before the employee can return to full duty. Training requirements shall include any missed mandatory initial/refresher training, weapons recertification, and any other training deemed necessary by the Department. This shall include a review of any policy changes that occurred while absent. The Support Services Division shall assist with determining training requirements.

3. Based on the length of deployment and the ability of the returning employee, the division commander may require the employee to complete a retraining program that may include assignment to a field training officer.
 4. A review of the Department's Employee Assistance Program (EAP) and other available counseling services with the employee to ensure they are aware how to access services if needed.
- B.** As soon as practical, the employee shall be required to meet with a representative of the City's Human Resources Department to review work requirements and the current state of the employee's benefits.

Chapter 3: The Personnel Structure
Section 22: Personnel Management System
Subsection 2: Conditions of Work



Policy/Procedure #: 1

Title: Physical Condition

CALEA Reference#: 22.2.1, 22.2.2

I. Policy: Physical Condition

In order to effectively meet the needs of the community, police officers must be capable of performing a wide variety of strenuous physical tasks. It has been documented law enforcement personnel (as an occupational class) have serious health risks in terms of cardiovascular disease, lower back disorders, and obesity. Law enforcement agencies have the responsibility of minimizing known risk. Physical fitness and overall wellness are areas that can minimize the health risk for law enforcement officers. Consequently, it shall be the policy of Urbandale Police Department to promote physical fitness and wellness among all employees and specifically sworn officers.

II. Procedure: Physical Examinations

- A.** All applicants for full time sworn positions shall be required to pass a post offer of employment physical examination and drug screen. The physical examination and drug screen shall be provided at no cost to the applicant.
- B.** The post offer of employment physical examination shall be conducted by a provider selected by the Department. Requirements needed to pass the physical examination shall be determined by the Municipal Fire and Police Retirement System and the City of Urbandale.
- C.** Employees suffering from an injury or severe illness may be required to have a physical examination prior to returning to duty. This fit-for-duty examination shall be conducted by a provider selected by the Department. The need for a fit-for-duty examination shall be based on the severity of the injury or illness as determined by the Chief of Police.
- D.** All physical examinations required by the Department as a condition of continued employment shall be provided at no cost to the employee.

III. Procedure: Physical Fitness

- A.** All sworn officers are expected to maintain a satisfactory level of general health and physical fitness so their work can be performed effectively and efficiently. Any sworn officer unable to perform job related functions due to physical fitness or health shall be reported via the chain of command to

the Chief of Police. The Chief of Police shall review each case and decide on a course of action.

- B.** To aid in the physical fitness of employees, the City of Urbandale maintains a fitness facility with various types of exercise equipment. This facility is available to all employees as a benefit of their health insurance.

Chapter 3: The Personnel Structure
Section 22: Personnel Management System
Subsection 2: Conditions of Work



Policy/Procedure #: 4

Title: Off Duty and Contracted Duty Employment

CALEA Reference#: 22.2.4, 22.2.5

I. Policy: Off Duty and Contracted Duty Employment

A policy is established to clarify procedures to be used by employees when they engage in off duty and contracted duty employment.

II. Procedure: Off Duty Employment

- A.** Off duty employment is employment in which the utilization of law enforcement powers is not anticipated. The Urbandale Police Department does allow employees to work at jobs where it is not anticipated they will use their law enforcement powers. Employees who engage in off duty employment or who are seeking such employment must submit an interdepartmental memorandum to the Chief of Police requesting such employment. The memorandum requesting off duty employment shall be submitted prior to beginning any off duty employment. The Chief of Police shall ensure there is no conflict of interest between the off duty employment and the employee's work at the Urbandale Police Department. The Chief of Police shall have final determination over all off duty work.
- B.** When an employee is no longer performing approved off duty employment, the employee shall notify the Chief of Police in writing.
- C.** Employees shall not engage in any off duty employment which may constitute a conflict of interest or discredit the Department as determined by the Chief of Police. Off duty employment is prohibited as follows:
 - 1.** In bars or businesses where the primary source of revenue is the sale of alcoholic beverages.
 - 2.** For an attorney practicing criminal law or acting as an investigator for a law firm in criminal cases.
 - 3.** Any employment interfering with the efficiency or effectiveness of the employee while working for the Urbandale Police Department.
- D.** Probationary employees are encouraged not to engage in off duty employment as it may have a detrimental effect on their efficiency or effectiveness of learning a new position with the Department. If allowed, the employee shall be closely monitored for any indication of difficulties.

- E. Employees engaged in off duty employment do so with the understanding any injuries or illness attributed to the off duty employment will not be covered by the City of Urbandale's workers compensation insurance and may not be covered by the employee's pension disability coverage.

III. Procedure: Contracted Duty Employment

- A. Contracted duty employment is employment of sworn officers of the Department by private vendors where the actual or potential use of law enforcement power is anticipated. Duties performed shall include the following:
 - 1. Security of a business or property
 - 2. Protection of an individual or group
 - 3. Crowd control
 - 4. Traffic direction
 - 5. Maintaining the peace
 - 6. Other law enforcement functions as necessary
- B. The Support Services Commander or designee shall be the point of coordination and administration of all contracted duty employment policies, processes, and other matters related to contracted duty employment as deem appropriate by the Chief of Police. Contracted duty employment shall be approved by the Support Services Commander or designee.
- C. All contracted duty employment shall be handled through the Department. Sworn officers working a contracted duty assignment will be recognized by the Department and the City of Urbandale as "on duty" with full rights and protections offered to any other "on duty" employee in their job classification. Vendors wishing to utilize officers for a specific law enforcement task such as directing traffic, crowd control, or personalized security situations shall contact the Support Services Division Commander or designee. The Support Services Commander or designee may approve or deny the use of sworn officers to assist the vendor based on a review of the nature of the work of the vendor and the duties of the officer being requested. Care shall be taken not to expose the officers to undue risk of injury. If questions arise as to the approval or denial of a vendor, the Chief of Police shall make the final determination. Vendor approval shall be conducted as follows:
 - 1. Support Services shall interview the vendor to ensure the contract will be for a specific law enforcement task and the vendor meets all of the Department requirements for contracting police services.
 - 2. The vendor shall be informed the officer(s) cannot be utilized to perform non law enforcement functions and any other restriction necessary based on the assignment.
 - 3. Based on an interview with the vendor, Support Services shall determine how many officers will be needed to perform the service safely. The vendor will be required to comply with the number of officers required or the service will not be provided.

4. Support Services shall provide a contract for services which the vendor will be required to sign prior to an officer(s) being assigned.
 5. Support Services shall maintain the signed contract and provide needed information to the Office of the Chief of Police for billing.
 6. Vendors violating the restriction placed on employment by the Support Services Commander or designee may have their ability to contract an officer revoked and approval for future contracted employment denied.
- D.** Officers assigned to contracted duty employment shall have the ability to act within the full authority of their powers as prescribed in departmental written directives or state law. Officers assigned to contracted duty employment shall only perform law enforcement functions for the vendor.
- E.** Contracted duty employment shall occur within the city limits of Urbandale. Any requests for contracted duty employment outside the City of Urbandale shall be reviewed and approved by the Chief of Police.
- F.** Contracted duty employment shall not occur at the following businesses:
1. In bars or businesses where the primary source of revenue is the sale of alcoholic beverages.
 2. For an attorney practicing criminal law or acting as an investigator for a law firm in criminal cases.
 3. Any employment interfering with the efficiency or effectiveness of the employee while working for the Urbandale Police Department.
- G.** Probationary officers that have not completed step four (4) of the field training officer (FTO) program for the Department shall not be allowed to work any contracted duty employment. Officers who have completed step four (4) of the FTO program but are still on probation shall receive approval from their division commander prior to being assigned any contracted duty employment. This approval shall be based on the level of performance of the probationary officer in their primary duties. The Support Services Division Commander shall be notified of the approval or denial to work contracted duty employment by the division commander responsible for the decision.
- H.** Vendors shall be required to pay a two (2) hour minimum based on one and one half (1½) times the hourly pay rate of the officer assigned to the contracted duty employment. Vendors requesting officers for holidays recognized in the union contract (July 4th, Thanksgiving, Christmas eve, Christmas day) requiring two (2) times the hourly pay rate shall be required to pay two (2) times the hourly pay rate of the officer assigned to the contracted duty.
- I.** Officers assigned to contracted duty assignments during holidays will not receive compensation to their bank of holiday hours for working contracted duty assignments.
- J.** Vendors requesting contracted duty employment from the Department shall be allowed to cancel the employment without penalty if at least a two (2) hour notice is given. If notice to cancel is given to the Department with less than a two (2) hour notice, the vendor shall be required to pay a two (2) hour

minimum based on one and one half (1½) times the hourly pay rate of the officer assigned to the contracted duty employment.

- K.** Vendors requesting employees for contractual duty with less than a twenty four (24) hour notice shall be required to pay a two hour minimum based on two (2) times the hourly pay rate of the officer assigned to the contracted duty employment.
- L.** Payment shall be made through an invoice system managed by the Office of the Chief of Police.
- M.** As part of the invoice system, officers shall utilize the City of Urbandale time clock system to document time spent working contracted duty employment. The time clock system shall document the date, time and place of employment. The Support Services Commander or designee shall approve all contracted duty employment in the City of Urbandale time clock system.
- N.** Patrol supervisors shall check daily to determine if a contracted duty assignment will occur during their shift. When there is a contracted duty assignment during their shift, patrol supervisors shall ensure the assigned officer has reported for duty, notifies Westcom of their assignment, and properly signs in and out of the time clock system. When an officer fails to report for an assigned contracted duty employment, the patrol supervisor shall attempt to contact the officer assigned. If the supervisor is unable to contact the assigned officer or the officer is contacted but unable to respond, the patrol supervisor shall make attempts to fill the assignment with other off duty officers. If the patrol supervisor is unable to fill the assignment, the vendor shall be notified as soon as possible.
- O.** Failure to report or reporting late for contracted duty employment shall be documented by the patrol supervisor and forwarded to the Support Services Commander with a copy to the division commander of the affected officer. Failure to report or reporting late for a contracted duty assignment shall be considered by the Department as failure to report for assigned duty and may result in prohibition from working contracted duty assignments and/or additional disciplinary action.
- P.** If an officer is unable to work contracted duty employment after being approved for said employment, it shall be the officer's responsibility to secure a replacement. Finding replacements for contracted duty employment shall be garnered out of actual need not as a means to circumvent the selection process. The officer approved but unable to work the assignment must contact other officers that have signed up for the assignment by seniority until the duty is filled. Only after all officers on the original posting for a particular duty have been contacted may an officer contact any other officer to fill the assignment.
- Q.** Except where stated in this policy, officers working contracted duty employment shall receive the same benefits and liability protections from the City of Urbandale and the Department as they shall be considered "on duty" for the Department in a law enforcement capacity when working for the vendor.

- R. If an officer is injured while working a contracted duty assignment, they shall be subject to the same reporting requirements as required when working their regular assignment.
- S. Equipment needed to provide the service, including a vehicle to transport the assigned officer to the job location, shall be provided by the Department. Any unusual requests for equipment shall be approved by the Chief of Police.
- T. Officers working contracted duty employment are subject to inspection by supervisory officers. All departmental written directives shall be applicable to any officer engaged in contracted duty employment. Violations of written directives may result in prohibition from working contracted duty assignments and/or disciplinary action.
- U. Officers working contracted duty assignments are required to wear the full uniform of the day. If traffic control is involved, officers shall wear a traffic vest or high visibility jacket. Based on the assignment, exceptions to the uniform requirement may be granted by the Support Services Commander or the Chief of Police.
- V. If an officer engages in any type of enforcement activity while working contracted duty employment, they shall be responsible for completing reports initiated as a result of their action (except motor vehicle accidents). Regular duty officers shall assist by processing any arrests made by the contracted duty officer. In the event of an unusual circumstance, the officer will submit an inter-office memorandum through the chain of command to his/her division commander describing the incident and the actions taken by the officer. Copies of any reports generated from a contracted duty assignment shall be provided to the Support Services Commander for review as they may affect the decision to provide officers for future duties with the vendor.
- W. Any criminal court appearances required as a result of working contracted duty employment shall be compensated in the same manner as court appearances for any other incident performed while on duty.

IV. Procedure: Allocation of Contracted Duty Assignments

- A. When approving contracted duty postings, those with rank with seniority determined by time in grade will have preference. If no supervisor is requesting the assignment, the duty will be assigned based on seniority with the Department. An exception to rank or employment start date with the Department will be made for contracted duty assignments having more than one occurrence during any given month. If a vendor has contracted more than one assignment for a calendar month, an officer being selected for one assignment for a vendor will not be considered for another assignment for that vendor unless no other officer has signed up for the duty. Each month the contracted duty assignments will reset in regards to approval based on rank or employment start date with the Department.
- B. When no officers volunteer to work a contracted duty assignment, the Support Services Commander or designee shall contact the vendor as soon as possible and notify them the Department is unable to provide the service.

The vendor may be referred to other law enforcement agencies or nonspecific private security companies.

V. Procedure: General

- A.** Any employee taking sick leave shall not engage in off duty or contracted duty employment until eight (8) hours after the end of the shift the officer was unable to work.
- B.** If an employee is assigned to light duty, the employee shall not engage in any off duty or contracted duty employment during their light duty status without authorization from the Chief of Police.
- C.** Complaints or alleged violations relating to employees working off duty employment will be directed to the Chief of Police or Internal Affairs.
- D.** Complaints or alleged violations relating to employees working contracted duty employment will be directed to the Support Services Commander. Based on the allegation, the complaint may be assigned to Internal Affairs for investigation.
- E.** Officers shall not jeopardize their physical or mental health by taking on too much off duty or contracted duty employment. Any adverse effects on job performance or physical/mental well-being shall be reported through the chain of command to the Chief of Police for action.
- F.** Department employees shall not be allowed to work as a full or part time sworn officer for another law enforcement agency. This does not restrict the Department's ability to assign officers for mutual aid assistance or participation in a joint task force operation.
- G.** Employees shall not work more than 16 hours of their regular duty assignment, contracted duty assignment, or any combination of regular and contracted duty assignments without a minimum of 8 hours of consecutive off duty time. Exceptions may be granted by the Chief of Police to respond to crisis situations.
- H.** Employees on leave for FMLA shall be suspended from working contracted duty assignments for the duration of their leave.

Chapter 3: The Personnel Structure
Section 22: Personnel Management System
Subsection 4: Grievance Procedures



Policy/Procedure #: 1

Title: Grievance Procedures

CALEA Reference#: 22.4.1, 22.4.2, 22.4.3

I. Policy: Grievance Procedures

An important element of a capable personnel system is a method that allows employees to resolve their grievances with management in a fair and expeditious manner. The Urbandale Police Department shall establish a policy to define the grievance procedure to be used by employees to resolve conflicts related to their employment.

II. Procedure: General

- A.** It is the intent of the Department to settle all grievances as promptly and simply as possible. An attempt shall be made by the employee and the immediate supervisor to resolve any potential problem before it develops into a grievance. If not quickly resolved, it shall be the employee's responsibility to abide by the timelines established in Iowa Code Chapter 400, City of Urbandale Civil Service Policy, City of Urbandale personnel policies and rules, and/or the current labor agreement between the City of Urbandale and the Urbandale Professional Peace Officers Association.
- B.** When a grievance is filed based on compensation, benefits, and/or conditions of employment, the following shall apply:
- 1.** Sworn full time employees covered by the current labor agreement between the City of Urbandale and the Urbandale Professional Peace Officers Association shall abide by article Seven (7) (Settlement of disputes).
 - 2.** All other employees shall abide by the City of Urbandale personnel policies and rules.
 - 3.** Where applicable, grievance procedure outlined in the City of Urbandale Civil Service Policy and Iowa Code Chapter 400 may also be utilized by all civil service protected employees.

- C.** When a grievance involves suspension, demotion or dismissal, the grievance procedure outlined in Iowa Code Chapter 400 and City of Urbandale Civil Service Policy may be utilized by all civil service protected employees.
- D.** When a grievance involves disciplinary action other than suspension, demotion, or dismissal and does not involve compensation, benefits, or condition of employment, an employee shall abide by the City of Urbandale personnel policies and rules.
- E.** Procedural steps and time limitations for filing or appealing a grievance shall be established in Iowa Code Chapter 400, City of Urbandale Civil Service policy, City of Urbandale personnel policies and rules, and/or the current labor agreement between the City of Urbandale and Urbandale Professional Peace Officers Association.
- F.** Procedural steps and time limitations for responding to a grievance or appeal shall be established in Iowa Code Chapter 400, City of Urbandale Civil Service Policy, City of Urbandale personnel policies and rules, and/or the current labor agreement between the City of Urbandale and Urbandale Professional Peace Officers Association.
- G.** All grievances and appeals shall be in writing, signed by the employee and state the following:
 - 1.** The grievance and the facts upon which it is based.
 - 2.** Allegation of the specific wrongful act and the harm done.
 - 3.** The remedy or adjustment sought.
- H.** Receipt of and response to grievances and appeals shall be documented for adherence to specified timelines.
- I.** Employees are entitled to representation as stated in Iowa Code Chapter 400, City of Urbandale Civil Service policy, and/or the current labor agreement between the City of Urbandale and Urbandale Professional Peace Officers Association.
- J.** The Chief of Police shall be responsible for the coordination of the grievance procedures as established in Iowa Code Chapter 400, City of Urbandale Civil Service Policy, City of Urbandale personnel policies and rules, and/or the current labor agreement between the City of Urbandale and Urbandale Professional Peace Officers Association for grievances filed by an employee of the Department. Coordination by the Chief of Police does not alleviate the employee filing the grievance from meeting all requirements and timelines established in Iowa Code Chapter 400, City of Urbandale Civil Service Policy, City of Urbandale personnel policies and rules, and/or the current labor agreement between the City of Urbandale and Urbandale Professional Peace Officers Association.
- K.** Formal grievances and associated correspondence, facts, solutions and outcomes shall be maintained in a formal grievance file. Formal grievance files will be maintained by the Chief of Police.

- L. The Chief of Police shall perform a documented annual analysis of any grievances filed to include examining any supporting policies, procedures and practices that were associated with the grievances. Based on the analysis, appropriate steps may be taken to reduce grievances filed in the future.

Chapter 3: The Personnel Structure
Section 22: Personnel Management System
Subsection 3: Collective Bargaining and Contract Management



Policy/Procedure #: 1

Title: Collective Bargaining

CALEA Reference#: 22.3.1, 22.3.2

I. POLICY: Collective Bargaining

A policy is established by the Urbandale Police Department to outline the activities of collective bargaining and ensure adherence to the current collective bargaining agreement.

II. Procedure: Collective Bargaining

- A.** Collective bargaining provides for compensation, benefits, and conditions of employment through negotiations between the city of Urbandale officials and the collective bargaining unit.
- B.** Employees shall have the right to join labor organizations, but nothing shall compel the city of Urbandale or the department to recognize or to engage in collective bargaining with any such labor organization except as provided by law.
- C.** The city of Urbandale and the Urbandale Police Department recognize the Urbandale Professional Peace Officers Association represented by the International Brotherhood of Teamsters Local 238 (Teamsters Local 238) as representing sworn officers in the department below the rank of sergeant.
- D.** When needed, the city of Urbandale shall engage in collective bargaining with the Urbandale Professional Peace Officers Association represented by Teamsters Local 238 to establish a labor agreement.
- E.** During times of collective bargaining, the chief of police, with the approval of the city manager, shall designate the representatives of the city's bargaining team. The city manager shall designate the principal negotiator for the city.
- F.** The department is committed to "good faith" bargaining with the Urbandale Professional Peace Officers Association represented by Teamsters Local 238 and shall abide by the ground rules for collective bargaining that arise out of the collective bargaining process or labor arbitration.

- G.** The department shall abide, in both letter and spirit, by the negotiated labor agreement signed by city officials, labor representatives and ratified by the Urbandale Professional Peace Officers Association represented by Teamster Local 238.

III. Procedure: Ratification

- A.** Upon ratification of a contract between the Urbandale Professional Peace Officers Association represented by Teamsters Local 238 and the city of Urbandale, the chief of police or his designee shall obtain a signed copy of the labor agreement.
- B.** The chief of police or designee shall disseminate information relative to the new labor agreement, including modifications to existing agreements, to all supervisors to ensure compliance with the agreement.
- C.** The office of the chief of police shall review and when necessary, amend all written directives and procedures to coincide with any new labor agreement.

Chapter 3: The Personnel Structure

Section 26: Disciplinary Procedures & Internal Affairs

Subsection 1: Disciplinary Procedures



Policy #: 1

Title: Departmental Rules and Regulations

CALEA Reference#: 1.2.10, 26.1.1, 26.1.3

I. Departmental Rules and Regulations:

The rules and regulations stated in this policy encompass all Urbandale Police Department employees, sworn and civilian, their conduct, conditions of employment, responsibilities, and overall purpose and function within and outside the structure of the police organization and its mission. This policy statement and the rules and regulations there under are intended for department use only. The policies, procedures, rules and regulations are for internal department administrative purposes and are not intended to create any higher legal standard of care or liability in an evidentiary sense than is created by law. Violations of internal written directives, policies, procedures, general orders, rules and regulations form the basis for disciplinary action by the Department. Violations of law form the basis for civil and/or criminal sanctions to be determined in a proper judicial setting, not through the administrative procedures of the Department.

It is the policy of the Urbandale Police Department that all rules & regulations are observed by each employee of the Department. Any accusation of a violation of the rules & regulations is subject to investigation or inquiry. The purpose of these regulations is to provide a basis for the orderly and disciplined performance of duty. These rules and regulations and related policies and procedures establish standards of conduct which are demanded of police officers, reserve officers, and employees in the execution of their professional duties, as well as in their private lives. It is incumbent upon each to conform to these standards so the police profession as a whole may enjoy the prestige and respect it deserves.

It is the purpose of this policy to provide additional specificity to the standards of conduct embodied in the law enforcement officer's code of ethics and the Urbandale Police Department's statement of values so employees of the Urbandale Police Department will better understand prohibitions and limitations pertaining to their conduct and activities while on and off duty.

The rules of conduct set forth in this policy are not intended to serve as an exhaustive treatment of requirements, limitations, or prohibitions on employee

conduct and activities established by this agency. They are intended to alert employees to some of the more sensitive and often problematic matters involved in police conduct and ethics. Specify, where possible, actions and inactions that are contrary to and conflict with the duties and responsibilities of department employees. Guide employees in conducting themselves and their affairs in a manner that reflects standards of department and professionalism as required of law enforcement employees. Additional guidance on matters of conduct is provided in regard to specific policies, procedures, and directives disseminated by this agency and from employees' immediate supervisors and commanders.

Actions of employees inconsistent, incompatible or in conflict with the values established by the Urbandale Police Department negatively affect its reputation and that of its employees. Such actions and inactions thereby detract from the Department's overall ability to effectively and efficiently protect the public, maintain peace and order, and conduct other essential business. Therefore, it is the policy of the Urbandale Police Department employees conduct themselves at all times in a manner that reflects the ethical standards consistent with the rules contained in this policy and otherwise disseminated by the Urbandale Police Department.

II. Rules and Regulations: General

- A. Violation of Rules:** Employees shall not commit any acts or omit any acts which constitute a violation of any of the rules, regulations, directives, orders or policies of the Department, whether stated in this section or elsewhere. Ignorance of the rules, regulations, directives, orders or policies shall not be considered as a justification for any such violations. Employees shall be responsible for their own acts and they shall not shift to others the burden of responsibility for executing or failing to execute a lawful or police duty.
- B. Improper Conduct:** Employees shall conduct themselves at all times, both on duty and off duty, in such a manner as to reflect most favorably on the Department. Improper conduct of an employee shall include that which impairs the morale of the Department, causes the public to lose confidence or respect in the Department, or impairs its efficient and effective operation.
- C. Misuse of Duty:** Employees shall not engage in any activities or personal business which would cause them to neglect or be inattentive to duty.
- D. Unethical Conduct:** Employees shall maintain a level of ethical conduct in their personal and business affairs, which is keeping with the highest standards of the law enforcement profession. Employees shall not participate in any activity that discredits the Department's motto and mission statement, impairs the ability to perform as a law enforcement agency or causes the Department to be brought into disrepute with the community.
- E. Respect within the Department:**
 - 1. Employees shall treat those in the Department of superior or lesser rank with respect at all times.
 - 2. Employees shall conduct themselves in a manner that fosters cooperation among members of the Department, showing respect, courtesy, and professionalism in their dealings with one another.
 - 3. Employees shall not use language or engage in acts that demean, harass or intimidate another person. (Members should refer to the City of Urbandale policy on "Harassment and Discrimination in the Workplace" for additional information on this subject.)

F. Recording Conversations Prohibited: Unless engaged in an investigation authorized by the chief of police or the internal affairs administrator, employees shall make no recordings of conversations involving employees of this department without the knowledge of all parties to such conversations. Conversations captured on body or in-car camera systems while meeting the requirements of Chapter 5 Section 41.3.8 (In-Car and Body Worn Recording Systems) shall not be considered a violation of this section unless captured in a surreptitious manner.

G. Accountability, Responsibility, Discipline & Conformance to Laws:

1. Employees shall at all times obey all laws of the United States, the State of Iowa and the City of Urbandale.
2. Employees are directly accountable for their actions through the chain of command, to the Chief of Police.
3. Employees shall cooperate fully in any internal administrative investigation conducted by this or other authorized agency and shall provide complete and accurate information in regard to any issue under investigation.
4. Employees shall be accurate, complete, and truthful in all matters.
5. Employees shall accept responsibility for their actions without attempting to conceal, divert, or mitigate their true culpability nor shall they engage in efforts to thwart, influence, or interfere with an internal or criminal investigation.
6. Employees who are arrested, cited, or come under investigation for any criminal offense in this or another jurisdiction shall report this fact to a superior as soon as possible.
7. Within their scope of authority and training, employees are required to intervene and notify a supervisor if they observe a Department employee or employees from other public safety agencies engage in any unreasonable use of force or if they become aware of any violation of department policy, state or federal law, or local ordinance. The intervention must be immediate if the actions could result in injury, death, or violations of constitutional or civil rights. Intervention and notification to a supervisor must occur for violations of departmental policy, state or federal law, or local ordinance if they meet one of the following criteria:
 - (a) The action by the employee is a criminal act.
 - (b) The action by the employee is unconstitutional.
 - (c) The action by the employee is a violation of civil rights.
 - (d) The action by the employee is inappropriate and will harm the reputation of the Department or the law enforcement profession as a whole.

H. Competency: Employees shall maintain sufficient competency to properly perform their duties and assume the responsibilities of their position. Employees shall perform their duties in a manner which will tend to establish and maintain the highest standards of efficiency in carrying out the functions and objectives.

I. Care and use of Equipment: Employees shall utilize departmental equipment for its intended purpose in accordance with established procedures and practice. Employees shall be responsible for the safekeeping, good care, proper maintenance, and serviceable condition of department property assigned for their use. This shall include personally owned handguns utilized while on duty. Loss of or damage to department property, including personally owned handguns utilized while on duty, due to carelessness or negligence may result in disciplinary action. Employees shall immediately report to their supervisor any loss of, damage to, or unserviceable condition of department property, vehicles,

equipment, telecommunication devices, computers, personally owned handguns utilized while on duty, or any other department items. Failure to report loss or damage to department property, including personally owned handguns utilized while on duty, may result in disciplinary action.

J. Gratuities: Employees shall not solicit gratuities at any time. Employees receiving gratuities within the boundaries of Iowa statutes, city policy and departmental policy, shall use the utmost discretion when accepting any gratuity and/or gift.

K. Shopping in Uniform: Employees in uniform shall not shop extensively or carry large quantities of merchandise unless directly connected with their normal police activity or as required in the line of duty. No alcoholic beverage shall be purchased while in uniform.

L. Cause for Disciplinary Action: Employees shall be subject to disciplinary action for acts of misconduct. Failure of an employee, either willfully or through negligence or incompetence, to perform the duties of their rank or assignment may be considered sufficient cause for discharge, demotion, suspension or other disciplinary action.

M. Public Statements:

1. Employees shall not make any public statement, publicly criticize or ridicule the Department, its policies, or other employees by use of speech, writing or other expressions. Speech, writing or other expressions which tend to impair the operations of the Department by interfering with its efficiency, interfering with the ability of supervisors to maintain discipline and morale, or having been made with reckless disregard for truth or falsity shall be prohibited.

2. Employees shall not divulge, or willfully permit to have divulged, any information gained by reason of their position for anything other than its official, authorized purpose.

3. Unless expressly authorized, employees shall not make any statements, speeches or appearances that could reasonably be considered to represent the views of the Department.

N. Public Appearances: Employees shall not address public gatherings, appear on radio or television, prepare any articles for publication, act as correspondents to a newspaper or a periodical, release or divulge investigative information, or any other matters of the Department while holding themselves out as having an official capacity in such matters of the Department without proper authority as stated in Chapter 6 Section 54.1.1 of the Operations Manual or as assigned by the Chief of Police.

O. Abuse of Position:

1. Employees are prohibited from using their official position, official identification card or badge for personal or financial gain, to obtain or grant privileges, to garner favors not otherwise available to them or others except as a private citizen, to avoid the consequences of illegal acts for themselves or others, to barter, to solicit, or to accept any goods or services (to include, gratuities, gifts, discounts, rewards, loans, or fees) whether for the employee or for another.

2. Employees shall not lend their identification card or badge to another person or permit the identification card or badge to be photographed or reproduced without the approval of the Chief of Police.

3. Employees shall report any unsolicited gifts, gratuities or other items of value they receive and if directed, shall provide a full report of the circumstances of their receipt.

4. Employees shall not purchase, convert to their own use, have a third party purchase, or have claim to any found, impounded, abandoned or recovered property, or any property held or released as evidence. Employees shall be allowed to purchase items for sale at the city's public auction as long as they are not on duty and have not garnered any unfair advantage in the bidding process for any reason (e.g. prior knowledge gained about the item).
 5. Any employee or the immediate family member of an employee of the Urbandale Police Department shall be prohibited from purchasing either directly or indirectly any property that has been forfeited to the Department due to a criminal investigation. This shall include any property forfeited to other law enforcement agencies where the Urbandale Police Department was involved (i.e. joint investigation) or to any investigative task forces in which the Department participates (e.g. Mid Iowa Narcotics Enforcement Task Force).
 6. Employees shall not solicit or accept contributions for this agency or for any other agency, organization, event or cause without the express consent of the Chief of Police or designee.
 7. Employees are prohibited from using information gained through their position at the Department to advance financial or other private interests of themselves or others.
- P. Use of Name, Photograph or Title:** Employees shall not permit or authorize the use of their names, photographs or official titles which identifies them as department employees in connection with testimonials, advertisements of any commodity, political campaigns, or commercial enterprises without the approval of the Chief of Police.
- Q. Endorsements and Referrals:** Employees shall not recommend or suggest in any manner, except in the transaction of personal business, the employment or procurement of a particular product, professional or commercial service. In the case of ambulance or towing service, when such service is necessary and the person needing the service is unable or unwilling to procure it or requests assistance, employees shall proceed in accordance with established departmental procedures.
- R. Off Duty Police Action:**
1. Officers shall not use their police powers to resolve personal grievances (e.g., those involving the officer, family members, relatives, or friends) except under circumstances that would justify the use of self-defense, actions to prevent injury to another person, or when a serious offense has been committed that would justify an arrest. In all other cases, officers shall summon on-duty police personnel and a supervisor in cases where there is personal involvement that would reasonably require law enforcement intervention.
 2. Unless operating a marked police vehicle, off-duty officers shall not arrest or issue citations or warnings to traffic violators on sight, except when the violation is of such a dangerous nature that officers would reasonably be expected to take appropriate action.
 3. Other off-duty enforcement activities shall be directed by the procedures contained in Chapter 1 Section 1.2.1 of the Operations Manual.
- S. Courtesy:**
1. Employees shall be courteous to the public. Employees shall be tactful in the performance of their duties and exercise the utmost patience and discretion. Employees may temporarily adjust their vernacular to regain control of a subject using violence oriented escalation of language and/or behaviors being

- directed at the employee and/or third parties, which sends a clear warning that the employees and/or third parties may be endangered.
2. Employees shall conduct themselves toward the public in a civil and professional manner that connotes a service orientation and will foster public respect and cooperation.
 3. Employees shall treat violators with respect and courtesy, guard against using an officious or overbearing attitude or language that may belittle, ridicule, or intimidate the individual, or act in a manner that unnecessarily delays the performance of their duty.
 4. While recognizing the need to demonstrate authority and control over criminal suspects and prisoners, officers shall adhere to this agency's use of force policy and shall observe the civil rights and protect the well-being of those in their charge.
- T. Requests for Assistance:** When any person applies for assistance or makes complaints or reports either by telephone or in person, all pertinent information will be obtained in an official and courteous manner, and will be properly and judiciously acted upon consistent with established departmental procedures.
- U. Residence Requirement:** Any employee may reside outside the corporate boundaries of the city of Urbandale provided their residence is fifty (50) miles or less by the most direct street, road, or highway route from the Urbandale Police Department. To determine distance, the Department shall utilize mapping services such as Mapquest or other current mapping applications. No employee residing outside the City of Urbandale shall be given special consideration or privilege relating to their employment with the City because of any problems that arise from the location of their residence.
- V. Department owned vehicle restrictions:** Department owned vehicles are allowed to be driven to and from an employee's residence and their work assignment as required or as authorized by a division commander or the Chief of Police. If the employee's residence is more than 25 miles from the Urbandale Police Department by the most direct street, road, or highway route, employees will not be authorized to drive a department owned vehicle home on a daily basis. To determine distance, the Department shall utilize mapping services such as Mapquest or other current mapping applications. Only during an extreme emergency or as part of maintenance, repair, or vehicle construction shall a person other than an authorized city employee operate a department owned vehicle. Department owned vehicles may be used for minor personal business if the stop is along the direct route to and from the employee's work assignment (see restrictions in section II K of this policy). Unless necessary as part of the job assignment, civilian passengers are not allowed in department owned vehicles. Permission may be granted by a supervisor to allow civilian passengers based on special circumstances.
- W. Telephone & Address Requirements:** Employees shall have a telephone and shall report any changes of telephone number or address to their supervisor or other appropriate personnel within 48 hours. Changes shall be recorded on the appropriate departmental form.
- X. Payment of Debts:** Employees shall not undertake any financial obligations which they know or should know they will be unable to meet and shall pay all just debt when due. An isolated instance of financial irresponsibility will not be grounds for discipline, except in unusual severe cases. Repeated instances of financial difficulty may be cause for disciplinary action.

Y. Gambling: Employees shall not engage in any form of illegal gambling at any time, except in performance of duty and while acting under proper and specific orders from a superior officer. Employees will not participate in legal gambling to any extent that may affect their ability to make timely payments upon their personal debts.

Z. Visiting Prohibited Establishments: Employees shall not visit, enter, or frequent a known establishment wherein the laws of the United States, the State of Iowa or the City of Urbandale are regularly violated except in the performance of duty or while acting under proper and specific orders from a superior officer.

AA. Associations:

1. Arresting, investigating, or custodial employees shall not commence social relations with the spouse, immediate family member, or romantic companion of persons in the custody of this agency.
2. Employees shall not knowingly commence or maintain a relationship with any person who is under criminal investigation, indictment, arrest, or incarceration by this or another police or criminal justice agency, and/or who has an open and notorious criminal reputation in the community (for example, persons whom they know, should know, or have reason to believe are involved in felonious activity), except as necessary to the performance of official duties, or where unavoidable because of familial relationships.
3. Employees shall not knowingly join or participate in any organization that advocates, incites, or supports criminal acts or criminal conspiracies.

BB. Political Activity: Employees shall be guided by state law regarding their participation and involvement in political activities. Where state law is silent on the issue, employees shall be guided by the following examples of prohibited political activities during working hours, while in uniform or otherwise serving as a representative of the Department:

1. Engage in any political activity.
2. Place or affix any campaign literature on city owned property.
3. Solicit political funds from any member of this agency or another governmental agency of this jurisdiction.
4. Solicit contributions, signatures or other forms of support for political candidates, parties, or ballot measures on property owned by this jurisdiction.
5. Use official authority to interfere with any election or interfere with the political actions of other employees or the general public.
6. Favor or discriminate against any person seeking employment because of political opinions or affiliations.
7. Participate in any type of political activity while in uniform.

CC. Case Involving Family Members or Relatives: Officers shall not be assigned to investigate cases involving members of their family or relatives. If it is determined during the course of the investigation a member of the investigator's family or relative is involved, the investigator shall be removed from the case and another unrelated investigator shall be assigned. Exceptions to this policy shall be approved by the Chief of Police.

DD. Civil Actions by or Involving Employees:

1. Employees shall not institute any civil action arising out of their official duties without first notifying the Chief of Police.
2. Employees shall not use their positions with the Department as a means of forcing or intimidating persons with whom they are engaged in civil matters to settle them in favor of the employee or the Department.

3. Employees shall not accept or agree to accept anything as payment for personal injury incurred in the line of duty without first notifying the Chief of Police.
4. Employees on duty shall not serve civil documents except as directed by a supervisor.

EE. Reporting for Duty: Employees shall report at the time and place required by assignment or orders and shall be physically and mentally fit to perform their duties. They shall be properly equipped and cognizant of information required for the proper performances of duty so they may immediately assume their responsibilities. Judicial subpoenas shall constitute an order to appear under this section. Employees off-duty shall report for duty immediately upon receipt of and in compliance with the directions given to them at the time of notification. Such notification shall be by a supervisor or other authority delegated by the chief of police.

Paid on-call employees must be reachable by cellular telephone or telephone during their on-call rotation. Paid on-call employees must be able and in a condition to report for duty within one hour of notification. If a paid on-call employee is unable to report for duty when called upon, it shall be the on-call employee's responsibility to find a replacement. If a paid on-call employee is unable to respond as required by their on-call status, they shall be investigated for failure to report for duty and will be subject to disciplinary action based on the results of the investigation.

FF. Supervisory contact: Excluding the Patrol Division that is required to always have a supervisor on duty, other divisions within the department shall establish an order of contact for supervisory personnel for hours outside of the division's normal work schedule to respond to issues or inquiries concerning their assigned division. The supervisor contact list shall designate a primary supervisory contact as well as a descending contact order of supervisors assigned to the division culminating with the chief of police. The order and frequency of rotation of the supervisory contact list shall be established by the division commander. Supervisors on the contact list are not paid on call and are not required to respond to inquiries if not available. Supervisors on the contact list are not required to report for duty within one hour of notification but like all sworn positions are subject to call back. An employee needing to speak to a supervisor shall attempt contact with the designated primary supervisor. If the employee is unable to reach the primary supervisory contact, they shall work their way through the supervisor contact list until contact with a supervisor is made. Supervisors contacted will be compensated for any time that meets the work hours requirement established in the city handbook and relative to their position (exempt vs non-exempt).

GG. Leaving Area of Assignment: Except when engaging immediately needed police service, employees shall not leave their area of assignment or beat area for any reason without permission of their supervisor.

HH. Use of Controlled Substance and/or Prescription Drugs: Employees shall not have in their possession, either on or off-duty, any controlled substance and/or prescription drugs, unless so prescribed by a health care professional. When prescription drugs are prescribed for an employee and the use of such prescription drug may affect the performance of the employee's duties, the employee shall notify their division commander prior to resuming duty. The

company nurse or other health care professionals may be consulted prior to the employee being authorized to return to work under the influence of a prescribed drug.

II. Use of Alcohol:

1. Employees shall not drink intoxicating beverages while on-duty unless in the official performance of duty and while acting under proper and specific orders from a superior officer. Employees shall not appear for duty, or be on-duty while under the influence of alcohol to any degree or have an odor of intoxicants on their breath.
2. An employee shall not be under the influence of alcohol in a public place, whether on or off-duty. Under the influence is defined by Iowa Code.
3. Supervisors shall order a drug or alcohol screening test when they have reasonable suspicion an employee is using and/or under the influence of drugs or alcohol. Such screening shall conform to department policy on employee drug-screening and testing as stated in Chapter 6 Section 52.2.1 of the Operations Manual.
4. While off-duty, employees shall refrain from consuming intoxicating beverages to the extent it results in obnoxious or offensive behavior which would tend to discredit them or the Department or render the employees unfit to report for their next regular tour of duty.

JJ. Alcoholic Beverages & Drugs in Police Facility: Except for prescription drugs specifically prescribed to an employee by a health care provider, employees shall not bring into or store alcoholic beverages and/or drugs in any police facility or vehicle except those held as property or evidence in accordance with established departmental procedures for handling evidence or property.

KK. Use of Tobacco Products: While on duty, an employee shall not use tobacco products unless in a designated usage area and not while conducting police business. Additionally, employees are not permitted to use tobacco products in a vehicle owned or maintained by the Department.

LL. Duty to be Truthful: Employees shall be truthful at all times. Employees are also required to answer questions or provide materials to a competent authority when so directed by the Chief of Police or designee. Employees shall not make a false report nor knowingly enter into any department record or report any inaccurate or false information.

MM. Courtroom Appearance and Decorum: When attending court, employees shall be punctual, professional and appropriately attired at all times. When a court appearance is required for job-related purposes, the appropriate attire for sworn personnel is a complete Class A uniform or business suit with coat and tie, or for female employees, suitable business apparel. Officers working a narcotics or similar assignment may be exempt from dress requirements for court based on the type of court proceeding. Officers shall comply with requests from the prosecutor for appropriate dress requirements. Testimony shall be given accurately, impartially and respectfully. Employees shall be responsible for availing themselves of police records resources in order to adequately prepare themselves for any job related courtroom testimony. If testifying in a civil non-job related matter, employees shall not wear a uniform. Prior to testifying for the defense in a non-job related criminal case, employees shall so notify the prosecutor immediately when learning their testimony is required.

NN. Official Business and Information: Employees shall consider the official business of the Department confidential. They shall not reveal any such

information, except to those for whom it is intended, as directed by policy and procedure or as prescribed by law.

OO. Expectations of Privacy:

1. Employees shall not store personal information or belongings with an expectation of personal privacy in such places as lockers, desks, departmentally owned vehicles, file cabinets, computers, or similar areas under the control and management of the Department. While the Department recognizes the need for employees to occasionally store personal items in such areas, employees should be aware these and similar places may be inspected or otherwise entered to meet operational needs, internal investigatory requirements, or for other reasons at the direction of the Chief of Police or designee.
2. No member of this agency shall maintain files or duplicate copies of official agency files in either manual or electronic formats at their place of residence or in other locations outside the confines of the Department without express permission.
3. Except in emergency situations, employees on-duty shall not use personally owned cellphones or other personally owned devices to capture audio, video, or photographs of any calls for service or other official police operations. If a personal device is used to capture an emergency situation, the file shall become the property of the Department. The details of capturing the event shall be entered into a report and the file shall be downloaded into the appropriate format and entered into evidence. Once entered into evidence, the file shall be deleted from the personal device.

PP. Posting Notices: Any notice, memo, clipping, picture or other material posted in the police facility, shall bear the signature or initials of the person posting said material. No offensive or obscene material shall be posted.

QQ. Police Officer Bill of Rights: All employees will be cognizant of the Police Officer Bill of Rights and take no intentional actions to circumvent the protections afforded to every police officer. The Chief of Police shall assure any rule, regulation, policy, or order in apparent conflict to the Police Officer Bill of Rights be adjusted accordingly.

Chapter 3: The Personnel Structure
Section 26: Disciplinary Procedures & Internal Affairs
Subsection 1: Disciplinary Procedures



Policy/Procedure #: 2

Title: Awards and Recognition Program

CALEA Reference#: 26.1.2

I. POLICY: Awards and Recognition Program

The Urbandale Police Department understands the value of recognizing and encouraging superior performance in job duties as well as meritorious and heroic acts performed by employees, volunteers, and citizens. The Department shall establish a systematic way to recognize these acts and reward the people involved.

II. PROCEDURE: General

- A.** All nominations should be forwarded on departmental memorandums.
- B.** It is the responsibility of all employees and volunteers to nominate those who qualify to receive any of the awards or recognition noted in this policy.
- C.** When necessary, memorandums shall be accompanied by supporting documentation.
- D.** Service bars and years of service awards do not require a nomination to be recognized.
- E.** The Chief's administrative specialist shall maintain the specification for each service bar and award (type, size, color, etc.).

III. PROCEDURE: Commendations

- A.** An employee or volunteer may receive a commendation as recognition for outstanding achievement while performing the duties of their job.
- B.** A division commander or the Chief of Police may issue a commendation. The following procedures shall be utilized to recognize an employee or volunteer for a commendation.
 - 1.** The employee or volunteers shall be nominated for commendation by another employee or volunteer.
 - 2.** The nomination shall be presented through the nominating employee's or volunteer's chain of command to the division commander.
 - 3.** The division commander shall review the incident and decide if a commendation shall be awarded. If in agreement with the nomination,

the division commander shall issue a commendation to the employee or volunteer utilizing a command staff memorandum to the Chief of Police.

4. A division commander or the Chief of Police may also issue a commendation for any deserving action without receiving a nomination from another employee or volunteer.
 5. When awarded, commendations may be presented to the employee or volunteer by the Chief of Police or a division commander in a command staff meeting, staff meeting, or other venue. The Chief may also utilize the annual awards banquet to recognize commendable acts.
 6. A copy of the commendation shall be placed in the personnel file of the employee and shall remain in the file for future reference.
- C. The Chief of Police may also draft letters for commendable acts to persons who are not employees or volunteers of the Department. Information on commendable acts shall be forwarded through the chain of command to the Chief of Police for action.
- D. Copies of all commendations issued shall be forwarded to the awards committee chairperson for possible recognition at the annual awards banquet.

IV. PROCEDURE: Employee of the Year

- A. The Department shall recognize one employee or volunteer for employee of the year.
- B. Annually, the Chief of Police shall call for nominations for employee of the year. Employees and volunteers of the Department may nominate who they feel is deserving of the employee of the year award. Nominations may be kept confidential and shall be given directly to the Chief of Police for review.
- C. Based on the nominations and any other information deemed relevant, the Chief of Police shall select the employee of the year.
- D. The award for employee of the year shall be presented at the annual awards banquet. The employee or volunteer shall receive a commemorative award and have their name added to the appropriate employee of the year recognition plaque.

V. PROCEDURE: Awards Committee

- A. The Department shall establish an awards committee. The awards committee shall consist of the following members:
1. All division commanders.
 2. The Chief's administrative specialist shall serve as the committee chairperson and be responsible for scheduling meetings, setting the agenda and taking meeting minutes.
 3. Two (2) sworn officers from any division in the Department. Volunteers will be requested. If more than two (2) volunteer, the staff members on the awards committee shall select the committee members. If less than two (2) volunteer, staff members on the awards committee shall select two sworn officers to serve on the committee. Sworn officers

shall serve on the committee for two (2) years and are eligible to reapply at any time.

- B.** The awards committee shall meet semi-annually to address committee responsibilities.

VI. PROCEDURE: Awards

- A.** The awards committee shall establish a set of departmental awards that may be given per incident or on an annual basis. The Chief of Police shall give final approval to all committee awards. The Chief's administrative specialist shall maintain a list documenting past recipients of any awards.
- B.** Awards may be bestowed on employees of the Department, volunteers of the Department, any other employee for the City of Urbandale as well as citizens in the community.
- C.** All employees are encouraged to inform awards committee members of any act that may qualify an individual for an award.
- D.** When the awards committee receives information about a potential awards recipient, they shall review the incident. When the incident meets the award criteria, the awards committee shall vote to determine if the award should be presented. The results of the vote shall be forwarded to the Chief of Police for the final approval or denial of the award.
- E.** The awards committee shall organize and present an annual awards banquet. All awards from the previous calendar year shall be presented at the awards banquet. At the discretion of the Chief of Police, an award may be presented at any time to include staff meetings, shift briefings, council meetings or special ceremonies.
- F.** Awards may be in the form of a medal and a bar or a plaque and/or a certificate. For sworn officers and reserves, medals awarded may be worn on the uniform during ceremonies when the class A uniform or the dress uniform is required. The bar may be displayed during normal work assignments on the class A or class B uniform. Below is the list of departmental awards, the type of award and the criteria for receiving the award:
 - 1.** Lifesaving (type: sworn and reserve officers-medal & bar, others-plaque and/or certificate): Taking action with the direct result of saving of a human life.
 - 2.** Medal of valor (type: sworn and reserve officers-medal & bar, others-plaque and/or certificate): Recognition for exhibiting unusual courage. The situation must be one of unusual danger to the person and the person is aware of the danger. Additional criteria listed below shall also be considered when determining whether to issue the award:
 - a.** The person was faced with a deadly force event.
 - b.** The strong possibility existed at the time the person acted that they could have suffered serious injury or death.
 - c.** The person did not act foolhardily.
 - d.** The person did not use poor judgment or tactics thus creating the necessity for their actions.
 - e.** The person's actions were reasonable and necessary.

3. Meritorious commendation (type: sworn and reserve officers-medal & bar, others-plaque and/or certificate): Recognition of a person whose actions deserve to be commended for an outstanding act and/or performance of their duties. General commendations awarded throughout the year shall be considered for this award.
4. Purple Heart (type: medal & bar): Recognition for a person who receives serious bodily injury while performing necessary law enforcement functions. Serious bodily injury is defined as injury that creates a substantial risk of death, serious permanent disfigurement, or protracted loss or impairment of the function of any bodily member or organ. The award does not include injury in a motor vehicle accident unless special circumstances are determined by the awards committee.
5. Silver Star for bravery (type: sworn and reserve officers-medal & bar, others-plaque and/or certificate): Recognition for extraordinary heroism. It distinguishes a person whose act of courage goes above and beyond what would be expected in the situation.
6. Chief's unit award (type: certificate and/or plaque): Recognition to any unit of departmental personnel consisting of two or more persons. The definition of unit shall remain flexible (e.g. first watch patrol, investigations, bicycle, or a collection of individuals from different divisions that have worked jointly on a single mission).
7. Civic achievement award (type: certificate and/or plaque): Recognition for a member of the department who brings unusual recognition to the department through involvement in civic affairs. This may include activities with civic groups or other government agencies where the member's participation is primarily at their own volition and is mainly during their off duty time.

VII. PROCEDURE: Service Bars Awards

- A. The awards committee shall establish a service bar program to be awarded on an annual basis. The Chief's administrative specialist shall maintain an accurate and updated list of all service bars earned during the year as well as those awarded in past years. Below is a list of service bar awards and the criteria for earning each award:
 1. Division: A division service bar shall be awarded for service to a specific division. Division services bars shall include:
 - a. Patrol
 - b. Investigations
 - c. Support Services
 2. SERT (Suburban Emergency Response Team): A SERT service bar shall be awarded to any officer assigned to SERT as part of their collateral duties.
 3. Honor Guard: An honor guard service bar shall be awarded to any officer selected to serve on the honor guard as part of their collateral duties.

4. K-9: A K-9 service bar shall be awarded to any officer assigned as a K-9 officer as their specialized assignment.
5. Instructor: An instructor bar shall be awarded to any officer assigned as a departmental instructor in the following fields:
 - Firearms
 - Defensive Tactics
 - Less Lethal
 - First Aid/CPR
 - Driving
 - Bicycle
 - Radar/Lidar
 - RAD
 - SFST
 - Data master
 - Culture of Integrity
 - Diversity
 - Others as determined by awards committee
6. Specialist: A specialist bar shall be awarded to any officer assigned to a collateral duty or specialized assignment in the following areas:
 - School resource officer
 - Field training officer
 - Accident investigator
 - Crime scene investigator
 - Polygraphist
 - Bicycle officer
 - Narcotics detective
 - Community relations officer
 - Drug recognition expert
 - Computer forensic examiner
 - Peer Support Team member
 - Drone Operator
 - Others as determined by the awards committee
- B. The Chief of Police shall give final approval to the issuance of all service bars.
- C. Service bars shall only be available for full time sworn personnel of the Department.
- D. Under normal circumstances, the service bars earned during the previous calendar year shall be awarded at the annual awards banquet.

VIII. Recognition of Years of Service

- A. The awards committee shall track and maintain the departmental years of service awards. The chief's administrative specialist shall maintain an accurate accounting of all full time employees and volunteers years of service.
- B. When a full time employee of the Department reach established years of service plateaus, they shall be recognized by the Department. The

following is a breakdown of years of service plateaus and the type of recognition they shall receive from the department:

1. Five (5), fifteen (15), twenty five (25) and thirty five (35) years of service shall be recognized at a departmental presentation with a certificate.
 2. Ten (10), Twenty (20), Thirty (30), and Forty (40) years of service shall be recognized at a departmental presentation with a commemorative service award and addition of their name to the years of service recognition plaque.
 3. Qualified retirements from the Department shall be recognized at a department presentation with a commemorative retirement award and addition of their name to the appropriate retirement recognition plaque.
- C. Volunteers shall be recognized with a certificate for every five (5) years of service.
- D. If in good standing, volunteers will be recognized upon their resignation from the Department in the following manner:
1. 1-9 years- certificate
 2. 10+ years- plaque

IX. PROCEDURE: On the Spot Awards

- A. "On the Spot" awards are recognition awards for innovative ideas, programs or equipment that advance the operational efficiency or further the mission of the department or the city of Urbandale. The award may be accompanied by a cash incentive provided by the department.
- B. Nominations for "On the Spot" awards shall be forwarded to the Chief of Police for review. The Chief shall make a determination if an "On the Spot" award is justified and any cash incentive to attach to the award.
- C. At the discretion of the Chief of Police, an "On the Spot" award may be presented at any time to include staff meetings, shift briefings, council meetings or special ceremonies.
- D. "On the Spot" awards shall be forwarded to the awards committee for possible recognition during the annual awards banquet.

Chapter 3: The Personnel Structure
Section 26: Disciplinary Procedures & Internal Affairs
Subsection 1: Disciplinary Procedures



Policy/Procedure #: 3
Title: Sexual Misconduct
CALEA Reference#:

I. POLICY: Sexual Misconduct

Law enforcement officers are empowered with the authority to protect the public from criminal activity. When an officer abuses this authority for sexual purposes and violates another person, the officer not only commits a crime against the victim, but also damages the credibility and public trust of the entire law enforcement community. The purpose of this policy is ensure no officers violate the public trust by engaging in sexual misconduct. Violations of this policy will result in severe consequences including termination of employment and prosecution to the fullest extent possible.

II. Procedure: Definitions

- A.** Criminal Sexual Misconduct: The abuse of authority by a law enforcement officer for sexual purposes that violates the law.
- B.** Sexual Misconduct: Any sexual activity while on-duty or stemming from official duty. Sexual misconduct includes but is not limited to use of official position and official resources to obtain information for purposes of pursuing sexual conduct.
- C.** Intimate Part: Genital area, inner thigh, groin, buttocks, or breasts of a person.
- D.** Actor: The person accused of sexual assault or sexual misconduct.
- E.** Sexual Contact: Any contact for the purpose of sexual gratification of the actor with the intimate parts of a person not married to the actor.

III. Procedure: General

- A.** Sexual activity of any nature while on duty is prohibited.
- B.** Any use of official position and official resources to obtain information for purposes of pursuing sexual conduct is prohibited.
- C.** Sexual Misconduct is prohibited and shall be disciplined up to and including termination.

- D. Any contact for the purpose of sexual gratification of the actor with the intimate parts of a person while on duty is prohibited.
- E. An employee shall not engage in sexual contact with another person who is in custody.
- F. Any employee of this Department who is made aware of any violation of this policy is required to report the violation to their supervisor. If the violation involves the employee's supervisor, the employee shall report the violation to their Division Commander or the Chief of Police. The supervisor notified shall immediately contact Internal Affairs Administrator who will initiate an investigation in accordance with established policy. The accused officer's supervisor will not attempt to resolve a complaint of this nature with the complainant. Upon receipt of the complaint, supervisors are required to make immediate contact with Internal Affairs Administrator or the Chief of Police.

IV. Procedure: Discipline

- A. Any employee found to be in violation of the provisions of this policy shall be disciplined up to and including termination and criminal charges where established.
- B. Any employee having knowledge of a violation of this policy and who fails to report said violation shall also be disciplined up to and including termination and criminal charges if appropriate. If the violation involves supervisory personnel, the reporting officer will notify the appropriate command level supervisor and will not be strictly held to their chain of command.

Chapter 3: The Personnel Structure
Section 26: Disciplinary Procedures & Internal Affairs
Subsection 1: Disciplinary Procedures



Policy/Procedure #: 4

Title: Disciplinary System

CALEA Reference#: 26.1.4, 26.1.5, 26.1.6, 26.1.7, 26.1.8

I. Policy: Disciplinary System

The Urbandale Police Department recognizes the value of an established disciplinary system that is known and easily understood by all employees. The elements of the disciplinary system shall be based on fairness to the employee and the department and shall encourage employee morale and motivation. The tenure of every employee shall be based on reasonable standards of personal conduct and job performance. Failure to meet such standards shall be grounds for appropriate disciplinary action, which shall be commensurate with the seriousness of the offense and with due consideration of the employee's prior performance and disciplinary record. If this policy conflicts with the discipline policy found in the City's employee handbook, the handbook policy shall take precedent.

II. Procedure: Disciplinary Action

- A.** Disciplinary action may be taken whenever an employee violates a policy, procedure, rule, regulation or any other established written directive.
- B.** The following procedure shall be utilized when an employee has violated a written directive of the department that warrants disciplinary action.
 - 1.** The immediate supervisor of the employee involved shall report the violation to their division commander. This shall be documented on departmental memorandum. If the violation involves the division commander, the report shall be directed to the chief of police.
 - 2.** The division commander or the chief of police shall determine if further investigation into the violation is needed.
 - 3.** If further investigation is needed and the violation is likely to result in suspension, demotion or termination, the violation shall be forwarded to the division commander or Internal Affairs Unit (IAU) for investigation. The division commander or IAU shall follow the

investigative procedures outlined in Chapter 6 Section 52.2.1(Complaint Procedure) of the Operations Manual.

4. If further investigation is needed and the violation is not likely to result in a suspension, demotion, or termination, the violation may be investigated by the division commander, another designated supervisor within the division, or the Chief of Police.
5. At the conclusion of an investigation not handled by the IAU, a report of the violation and the subsequent investigation shall be drafted and forwarded to the division commander on departmental memorandum. If a divisional commander conducted the investigation, a copy shall be provided to the chief of police. If the chief of police conducted the investigation, he shall retain all related documentation.
6. The supervisor conducting the investigation may be required to meet with the division commander and/or the chief of police and discuss the investigation as well as their recommendation for disciplinary action.
7. After reviewing the reports on the violation, the division commander or the chief of police shall make one of the following determinations as to the final disposition of the violation based on a preponderance of the evidence:
 - a. Exonerated (proper conduct): The allegation is true. The action of the agency or employee was consistent with agency policy, procedure or rules and regulations.
 - b. Substantiated (improper conduct): The allegation is true. The action of the agency or the employee was inconsistent with agency policy.
 - c. Substantiated on policy: The allegation is true but the agency does not have policy to cover the situation. A written directive shall be introduced to cover future situations.
 - d. Unfounded (false or not credible): The allegation is either demonstrably false or there is no credible evidence to support it.
 - e. Unsubstantiated (insufficient evidence): There is insufficient evidence to confirm or refute the allegation.
8. The disposition of the violation and the final disciplinary action taken by the department shall be recorded on the post incident summary report.
9. If the results of the investigation are exonerated, unfounded, substantiated on policy, or unsubstantiated and no action will be taken, the employee shall receive written notification.
10. If the results are substantiated on policy, the chief of police shall determine if a written directive is needed to address the issue. If needed, the chief shall assign the appropriate personnel to draft and present a written directive per policy.
11. When a violation is substantiated, the division commander or the chief of police, with due consideration for the employee's prior performance

and disciplinary record, shall determine the appropriate discipline for the violation.

12. If the investigation is concluded and the division commander recommends the violation should result in disciplinary action of suspension, demotion, or termination, the entire investigation, including the division commander's recommendation, shall be forwarded to the chief of police for a final determination.
13. Final disciplinary action shall be one of the following categories:
 - a. **Remedial Training:** Remedial training is when a violation was caused primarily by the employee being incompetent or inadequately prepared for his/her responsibilities and it is in the best interest of the employee and the department the employee undergoes additional training. The specific nature and procedure for a given retraining shall be determined by the employee's division commander and/or the chief of police. Notice to the employee of required remedial training shall be documented. All remedial training conducted shall be documented and copies forwarded to the division commander, and/or the chief of police.
 - b. **Counseling:** Counseling is when an employee is verbally made aware of his or her violation by a supervisor, but there are circumstances that impair the employee's ability to comply with the written directive violated. Action is taken by the supervisor to work with the employee in an attempt to correct the problem rather than take other disciplinary measures against the employee. Counseling may be given by the supervisor or by an outside source such as EAP or a psychologist. Notice to the employee of required counseling shall be documented. Counseling received shall be documented to the division commander and/or the chief of police.
 - c. **Verbal Warning:** A verbal warning is when an employee is made aware of his or her violation verbally by a supervisor and is informed he or she is in violation of a specific written directive and is instructed to comply in the future. The supervisor may make reference or comments on how similar action(s), behavior or policy violations may result in future discipline. Departmental memorandum or other documentation to the division commander or the chief of police shall be utilized to verify the employee received the verbal warning.
 - d. **Written Warning:** A written warning is a warning by a division commander, the chief of police or designee, finding an employee in violation of a specific written directive. Notice to the employee of a written warning shall be documented on notice of disciplinary action form.

- e. **Transfer:** Transfer is when an employee is moved from a current assignment or shift. A transfer may occur to remove an employee from a work environment that is a contributing factor to the violation. Notice to the employee of a transfer, due to violating a written directive, shall be documented on notice of disciplinary action form. A transfer due to disciplinary action may only be imposed by the chief of police or designee.
 - f. **Suspension Without Pay:** Suspension without pay is the temporary removal of an employee from the city payroll. Unless extended by approval of the city manager, the maximum period of suspension shall be 30 working days. All suspension days shall run consecutively and shall not include any scheduled days off. Notice to the employee of a suspension without pay shall be documented on notice of disciplinary action form. A suspension without pay may only be imposed by the chief of police or designee and with the approval of the human resources director.
 - g. **Demotion:** Demotion is the reduction of an employee from a position in one class to a position in another class having a lower maximum salary rate. Notice to the employee of a demotion shall be documented on notice of disciplinary action form. A demotion may only be imposed by the chief of police or designee and with the approval of the human resources director.
 - h. **Resignation in lieu of disciplinary action (option selected by employee):** An employee may be offered the opportunity to resign in lieu of disciplinary action. When offered, the employee shall decide whether to exercise this option. The resignation should be obtained in writing from the employee and shall be accepted by the chief of police or designee.
 - i. **Termination or dismissal:** Termination or dismissal is the involuntary separation of an employee from the department. Notice to the employee of termination or dismissal shall be documented on notice of disciplinary action form which shall include the reason for the termination or dismissal and the effective date of the termination. The employee shall also receive a written statement of the status of accrued employee benefits after termination or dismissal. A termination or dismissal may be imposed by the chief of police or designee, the human resources director, or the city manager. All terminations or dismissals must be approved by the city manager.
14. Copies of all disciplinary action handled at the divisional level shall be forwarded to the chief of police for review. The chief of police reserves the right to modify any disciplinary action taken at the divisional level.

- C. Upon request, the employee affected shall be allowed to view all reports related to a disciplinary action unless a pending criminal investigation would be jeopardized or state/federal law or city policy prohibit disclosure.
- D. All disciplinary investigations shall be concluded within thirty (30) days of notice to the division commander. If an extension is needed to complete an investigation, the affected employee and the chief of police shall be notified.
- E. Employees shall be required to sign the notice of disciplinary action form documenting the receipt of said form.
- F. When meeting the criteria established in Chapter 2 section 11.4.5 (Notifications to the Chief of Police) of the Operations Manual, the chief of police shall be immediately notified reference a violation of department written directives.

III. Procedure: Temporary suspensions

A. Unfit for duty

1. The highest ranking supervisor in command of an employee has the ability to impose a temporary suspension for a period not to exceed one work day on the grounds an employee is unfit for duty. Unfit for duty may include any physical or mental condition that may, in the judgment of the supervisor, render the employee incapable of adequately performing duties and/or may jeopardize the safety of the employee or others.
2. If an employee is deemed unfit for duty they shall not automatically suffer a loss of pay but may lose pay for the temporary suspension period at a later time due to disciplinary action arising from the casual factors related to the unfit for duty suspension.
3. When practical, division commanders and the chief of police shall be consulted prior to an unfit for duty suspension.
4. When deemed unfit for duty by a supervisor, an employee shall not be allowed to work any contracted duty assignments or serve in any other function for the department.

B. Relief from duty

1. The chief of police may relieve an employee from duty for a period of up to 30 days while a complaint is being investigated. If the complaint is not resolved, the relief from duty may be extended. The employee shall be kept apprised of the status of the relief from duty suspension.
2. During a relief from duty, an employee shall not automatically suffer a loss of pay but may lose pay for the relief from duty period at a later time due to disciplinary action arising from the casual factors related to the relief from duty suspension.
3. When relieved from duty, an employee shall not be allowed to work any contracted duty assignments or serve in any other function for the department.

IV. Procedure: Appeals

A. Upon notification of the recommended disciplinary action the accused may:

1. Accept the disciplinary action as recommended.
2. Appeal the action as detailed in the City of Urbandale personnel policies and rules.
3. If applicable, appeal the action through the grievance procedure as allowed in the bargaining unit labor contract.
4. If applicable, appeal to the Civil Service Commission.
 - a. If the employee should choose to appeal a suspension, demotion or termination or dismissal to the Civil Service Commission, notification shall be filed with clerk of the commission within fourteen (14) calendar days after the first day that the adverse action took effect as specified in Chapter 400.20 in the Code of Iowa.
 - b. The appeals process set forth in Chapter 400 of the Code of Iowa (400.18-400.27) shall be the basis from which all procedures will originate.

B. All requested appeals, responses, and procedures associated shall be documented by the chief of police or designee.

V. Procedure: Records

A. All records related to any disciplinary investigation, related counseling, and/or remedial training shall be filed and maintain in the IAU files by the IAU Administrator. The only exceptions are:

1. Copies of investigative records which support a criminal charge against an employee must be processed and retained using normal records procedures.
2. The original notice of disciplinary action form shall be placed in the employee's personnel file whenever disciplinary action is taken which results in a written warning, suspension, demotion, termination, or dismissal and a copy placed in the IAU files.

B. Notice of disciplinary action forms placed in the employee's personnel file on record with the human resources department and shall remain in the file permanently.

C. When determining the final disciplinary action, prior discipline shall be considered. If dissimilar or unrelated, it shall be the chief's discretion whether to consider disciplinary action occurring more than 24 months prior to the current incident.

Chapter 3: The Personnel Structure
Section 26: Disciplinary Procedures & Internal Affairs
Subsection 2: Internal Affairs Organizational Integrity



Policy/Procedure #: 1

Title: Internal Affairs

CALEA Reference#: 26.2.1, 26.2.2, 26.2.3, 26.2.4, 26.2.5

I. Policy: Internal Affairs

The Urbandale Police Department shall establish an Internal Affairs Unit (IAU) to investigate complaints (including anonymous complaints) and allegations of misconduct by the Urbandale Police Department employees.

II. Procedure: Internal Affairs

A. All complaints, including anonymous complaints, shall be investigated. For the purposes of this procedure, both complaints and allegations of misconduct will be referred to as complaints. Complaints can be received in person, by telephone, letter, or electronically.

B. IAU shall be responsible for ensuring a complete investigation of all complaints received on the Urbandale Police Department or its employees.

C. The IAU Administrator, unless otherwise designated by the Chief of Police, will have the authority and responsibility to gain facts through investigative procedures and review to ensure the Department and its employees' integrity is maintained.

D. The Division Commander of the Investigation Division shall be the IUA Administrator unless otherwise designated by the Chief of Police. Other supervisors within the Investigation Division shall be utilized as IAU investigators as needed; however, any supervisors may be utilized to perform IAU functions at the direction of the IAU Administrator or the Chief of Police.

E. The IAU Administrator shall report directly to the Chief of Police.

III. Procedure: Internal Affairs Records

A. It is the responsibility of the IAU to establish a system of receiving, recording, and filing of all complaints, use of force reports, discharge of firearms reports, etc. whether investigated by IAU or by the chain of

command. Once the investigation is complete, all records will be maintained in a secure area under the custody and control of the IAU Administrator. At no time shall the records be distributed unless ordered by the Chief of Police or a court of competent jurisdiction. During the investigation and processing of complaints, the confidentiality and security of the records will be strictly maintained.

- B.** When a final disposition of any complaint investigation has been rendered by the Chief of Police, the investigation may become a public record. Upon request, the investigation shall be released in accordance with public records laws and if needed, approval by the City of Urbandale's legal counsel.
- C.** Public record review of internal affairs files will be completed with the IAU Administrator or designee present unless otherwise directed by the Chief of Police or a court of competent jurisdiction. A record will be made of each review. Copies of files will be issued only with the approval of the Chief of Police or his/her designee. A record will be made showing who received the copies.

IV. Procedure: Registering a Complaint

- A.** The process to register a complaint or commend an employee of the Department shall be posted on the Urbandale Police Department website.
- B.** Public presentations, as part of the Department's community relations activities, may include the process for registering a complaint or commending the Department or its employees.
- C.** Each employee shall be informed of the process for registering a complaint or commending the Department or its employees.

V. Procedure: Internal Affairs Statistics

- A.** The IAU Administer shall produce an annual statistical summary of all complaints and internal affairs investigations filed against the Department or its employees.
- B.** The statistical summary shall be made available to all department employees and the public.

Chapter 3: The Personnel Structure
Section 26: Disciplinary Procedures & Internal Affairs
Subsection 3: Complaint Procedure



Policy/Procedure #: 1

Title: Complaint Procedure

CALEA Reference#: 26.3.1, 26.3.2, 26.3.3, 26.3.4, 26.3.5, 26.3.6, 26.3.7, 26.3.8

I. Policy: Complaint Procedure

It is the responsibility of the department to provide a systematic, objective and impartial method of investigating complaints of inappropriate behavior or allegations of misconduct by Urbandale Police Department employees and police reserve officers. The department has identified the types of incidents that require review by a supervisor or higher-ranking personnel and the method used for completing the report. Certain incidents, because of their complexity and/or severity, will be investigated by the Internal Affairs Unit (IAU). The following defines the procedures for the investigation, disposition, and recording of criminal and administrative investigations.

II. Procedure: General

- A.** For the purpose of this policy only, employee will include police reserve officers.
- B.** No employee shall interfere with a criminal or administrative investigation conducted by the department or any other law enforcement agency.
- C.** In all investigations, department employees, whether the subject of an investigation or a witness shall answer all questions honestly, completely and to the best of their ability.
 - 1.** During an administrative investigation, an employee's refusal to answer questions specifically, directly, and narrowly related to the performance of his or her official duties or fitness for duty shall result in additional charges of insubordination. Should such charges be substantiated, the employee will be terminated.
 - 2.** Untruthfulness by any employee to an investigator assigned to conduct an administrative investigation shall result in additional charges of untruthfulness during an investigation. Should such charges be substantiated, the employee will be terminated.

- D. During an administrative investigation, all information obtained shall be kept confidential to the extent allowed by law.
- E. The procedures for conducting an administrative investigation will be in accordance with those rights and privileges enumerated in Iowa statutes, including IA Code 80F (Peace Officer, Public Safety, and Emergency Personnel Bill of Rights), applicable collective bargaining agreement, city of Urbandale policies, city of Urbandale Civil Service rules and regulations, and any other applicable rules, regulations, ordinances, and/or laws.
- F. The United States Supreme Court in the *Garrity vs. New Jersey* and *Gardner vs. Broderick* decisions extended to police officers and other government employees the protection of the privilege against self-incrimination. Statements they are compelled to make by threatened loss of their employment or other disciplinary actions may not form the basis of a criminal prosecution against them, nor can they be compelled to waive this privilege. Recognizing legitimate needs for effective and efficient operations of a police department, the court has clearly indicated the privilege against self-incrimination is not a bar to dismissal if a police officer refuses to answer questions specifically, directly, and narrowly relating to the performance of his or her official duties or their fitness for duty, without being required to waive his or her immunity with respect to the use of his or her answers or fruits thereof in a criminal prosecution of himself or herself. In other words, refusal to answer questions intended merely to secure information concerning his or her official activities or continued fitness for office would justify dismissal or other disciplinary action.
- G. Based on the nature of the criminal allegations against a department employee, the IAU shall maintain a liaison with the county attorney's office of competent jurisdiction, the Iowa Attorney General's Office, and the United States Attorney's Office.
- H. During a criminal or administrative investigation, an employee may be relieved from duty due to physical and/or psychological unfitness for duty, an action pending the outcome of an internal affairs investigation, or whenever it would be in the public interest not to have the employee on active duty. Any supervisor has the authority and the responsibility to immediately relieve a subordinate employee from duty due to physical and/or psychological unfitness for duty when it is obvious the employee is not fit for duty. If an employee is relieved from duty, the chain of command for the employee shall be immediately notified including the chief of police. Any other relief from duty shall be at the direction of the chief of police or designee.
- I. All files, reports, evidence, and records associated with criminal or administrative investigation shall be retained in accordance with department policy, city of Urbandale policy, state and federal law.

- J. Upon investigating a complaint, supervisory personnel may uncover additional criminal or administrative violations that were not part of the original complaint. Nothing shall limit or prevent the investigation of the additional violations uncovered during a complaint investigation.
- K. Upon the completion of the investigation, if the complaint has been classified as substantiated and the employee is subjected to disciplinary action, the employee or the employee's designated legal counsel may request a complete copy of a complaint investigation to include any written or taped-recorded statements. Other complaint investigations will be provided to the employee at the discretion of the chief of police.
- L. Supervisors conducting complaint investigations or supervising complaint investigations shall complete the minimum training standards as provided by the Iowa Law Enforcement Academy (ILEA) or sanctioned by ILEA for conducting such investigations as required by Iowa Code 80F.

III. Procedure: Filing a Complaint

- A. A complaint may be any of the following:
 - 1. Any alleged act by an employee which is contrary to written rules, regulations, policies, procedures, directives or orders of the Urbandale Police Department or the city of Urbandale.
 - 2. Any alleged act or omission which, if substantiated, would constitute a violation of federal law, state law, or local ordinances.
 - 3. Any allegation which indicates an actual or potential violation of department rules, regulations, policies procedures, directives, orders, or the delivery of services.
- B. A complaint may be filed by any person to include internal complaints by other employees or supervisors of the department.
- C. Complaints received by phone or in person shall be directed to a supervisor on duty. The supervisor receiving the complaint shall complete the initial complaint and inquiry form. Complaints received by letter or electronically shall be directed to the division commander of the employee involved for completion of the initial complaint and inquiry form. If the complaint is on a division commander, the complaint shall be directed to the chief of police. When able, the supervisor shall gain as much information as possible from the complainant. Based on the information garnered, the supervisor shall make the following determination:
 - 1. The complaint is a court issue and should be handled through normal court proceedings.
 - 2. The complaint was a minor issue that was resolved with the complainant and no further action is required.
 - 3. The complaint is demonstrably false.
 - 4. The complaint requires further investigation. Due to their seriousness, complaints regarding the following shall require further investigation:
 - (a) Use of force.

- (b) Corruption.
 - (c) Civil rights violations.
 - (d) Conduct involving moral turpitude.
 - (e) Criminal misconduct.
 - (f) In-custody death.
 - (g) Officer involved shootings.
 - (h) Any complaint that may result in a suspension, demotion, or dismissal of an employee if substantiated.
 - (i) Complaints determined by the chief of police as needing further investigation.
- D. If the complaint is determined to be a court issue, the supervisor shall complete the form by entering a brief synopsis of the complaint. The supervisor shall be required to notify the complaining party their complaint is a court issue and how they may seek relief via court proceedings.
 - E. If the complaint was a minor issue that the supervisor was able to resolve with the complainant and no further action is required, the supervisor shall complete the form by entering a brief synopsis of the complaint and the resolution that was reached.
 - F. If the complaint is demonstrably false, the supervisor shall complete the form by entering a brief synopsis of the complaint and the facts that led the supervisor to classify the complaint as false.
 - G. If the complaint cannot be classified as a court issue, a minor issue that has been resolved, or demonstrably false, the supervisor shall accept the complaint by completing the initial complaint and inquiry form, entering a brief synopsis of the complaint. The complainant may be given a statement of complaint form in which the complainant may record their complaint in their own words. The statement of complaint form may be filled out by the complainant at that time or submitted later to a supervisor or the IAU administrator.
 - H. The statement of complaint form need not be completed for the investigation of the complaint to move forward. Other correspondence can be substituted for the statement of complaint form to include letters, emails, voicemails, phone conversations, or in person meetings. If the statement of complaint form is not utilized, the supervisor receiving the complaint shall indicate the statement of complaint form is not being utilized, summarize the complaint on the initial complaint and inquiry form, and sign the form.
 - I. When needed to determine the classification of a complaint, a supervisor may conduct an informal inquiry with the employee. The informal inquiry should be at minimum audio recorded. The informal inquiry shall be limited in scope to the basic facts surrounding the complaint.
 - 1. An informal inquiry may be used for very minor issues or to gain basic information about the complaint and assist the supervisor in

determining if the complaint can be resolved with the complainant, is a court issue, is demonstrably false, or requires further investigation.

2. For some complaints, it may be obvious to the supervisor the complaint will need further investigation. In these cases, the supervisor need not conduct an informal inquiry with the employee but instead refer the complaint for further investigation.
- J. Once completed, the initial complaint and inquiry form shall be forwarded directly to the IAU administrator or a division commander. Upon receipt, the IAU administrator or a division commander shall complete a secondary review of the complaint to confirm it has been classified appropriately. This includes reviewing complaints that may have been deemed a court issue, demonstrably false, or a minor issue that was resolved with the complainant. If the IAU administrator or a division commander received the complaint and are the ones completing the initial complaint and inquiry form, the chief of police shall complete the secondary review for proper classification.
- K. If further investigation is not warranted, the initial complaint and inquiry form shall be filed in IAU records. If the complainant was not informed by the supervisor taking the complaint that an investigation is not warranted, the IAU administrator or division commander shall inform the complainant of the disposition of the complaint. The IAU administrator or the division commander shall also inform the employee and their chain of command supervisors of the complaint and the disposition.
- L. If the IAU administrator or a division commander receives the initial complaint and inquiry form and determines further investigation is warranted, he/she shall determine if the complaint shall be conducted as a criminal investigation, administrative investigation or both.
- M. Once it has been determined an investigation is warranted, the IAU administrator or other supervisory personnel shall inform the complainant the complaint has been received and an investigation will be conducted.
- N. Complaints a supervisor deems serious in nature, may have a serious adverse impact on the department, or are classified as criminal shall be reported without delay through the chain of command to the chief of police. If the complaint is in reference to a minor allegation, notification to the chief of police will be made by the IAU administrator or other supervisory personnel at their earliest convenience.
- O. A complaint may consist of one or more allegations. Each allegation must be addressed when the complaint is investigated.
- P. Investigations shall be completed as soon as practical. Any delays in completing the investigation within thirty (30) days shall be approved by the chief of police. If the investigation extends beyond thirty (30) days after receiving a complaint, the supervisor investigating the complaint, the IAU administrator, or the chief of police shall inform the complainant and

the employee(s) that are the subject of the complaint the status of the investigation. This shall occur every 30 days until the completion of the complaint investigation unless prior notification has indicated a different timeline.

IV. Procedure: Criminal Investigation

- A.** If the complaint is classified as a criminal investigation, the chief of police shall determine who shall investigate. If the alleged criminal act occurred within the jurisdiction of the department, the chief may request an outside agency such as the Department of Public Safety Division of Criminal Investigations conduct the investigation. If the criminal act occurred outside the jurisdiction of the department, the appropriate agency with jurisdiction shall conduct the investigation or make the determination as to the investigating agency.
- B.** Criminal investigations involving employees investigated by the department shall be handled procedurally in the same manner as all other criminal investigations. Employees that are the suspect in a criminal investigation shall be afforded no more and no less rights or protection than any other suspect.
- C.** If a complaint is classified as a criminal investigation, an administrative investigation shall also be conducted to determine if any policy, procedures, rules and regulations, orders, or directives have been violated. Normally, the administrative investigation will be conducted at the conclusion of the criminal investigation; however, the chief of police may order the administrative investigation to proceed prior to the conclusion of the criminal investigation.

V. Procedure: Complaint Investigation

- A.** Any complaint requiring further investigation shall be assigned for investigation by the chief of police or designee to internal affairs personnel, the division commander of the employee involved, another appropriate supervisor, or the chief of police.
- B.** Complaints of a less serious nature shall be assigned to the direct supervisor or the division commander of the employee involved. If there is involvement in the incident by the direct supervisor that may hamper their ability to conduct a thorough and unbiased inquiry, the chief of police shall assign a different investigator.
- C.** If at any time during investigation into a complaint of a less serious nature facts are uncovered that indicate a more serious violation of policy or a criminal act has occurred, the supervisor shall stop the investigation and consult with the IAU administrator or the chief of police for direction on how to proceed.
- D.** If the complaint involves an in-custody death, an officer involved shooting or any other serious allegation, the chief of police may request an outside

agency to conduct the investigation. IAU shall assign an investigator to monitor the investigation being conducted by the outside agency.

- E. The assigned investigator shall conduct a thorough investigation. This shall include an interview with the employee and as many witnesses as deemed necessary. The investigator shall also determine if other evidence is available such as in-car video, reports, emails, etc.
- F. The following procedures shall be followed for each complaint requiring further investigation:
 - 1. The employee shall be notified they are the subject of an investigation and their rights during the investigation (notification of investigation form & peace officer, public safety & emergency personnel bill of rights form). The notification shall include a written summary of the complaint.
 - 2. An interview shall be scheduled allowing a reasonable amount of time for the employee to obtain representation if they wish.
 - 3. An interview with the accused employee shall be conducted and at a minimum shall be audio recorded. The employee shall be informed of their Garrity rights (notification of rights: Garrity warning form).
 - 4. The employee has a right to have a labor representative or designee, and an attorney present for any interview. Labor representatives, designees, and attorneys are not allowed to interfere with the investigation.
- G. Interviews with employees that are merely witnesses and not the subject of the investigation shall also at a minimum be audio recorded. Witness employees shall also be notified of their Garrity rights (notification of rights: Garrity warning form).
- H. Once the investigation is complete, the investigator shall submit a report to the chief of police. If the investigation was completed by internal affairs, the internal affairs administrator shall review the investigation prior to it being submitted to the chief of police to ensure completeness. The report shall document any evidence collected such as copies of related reports, video, audio or written documentation. The report shall be produced on departmental memorandum.
- I. If the complaint may result in a loss of pay, benefits, transfer of assignment, or termination, the chief of police shall meet with the employee to allow them an opportunity to respond to the complaint by presenting any additional evidence or testimony prior to a final determination of disciplinary action.
- J. Upon receiving the investigative report, the chief of police shall initiate a post incident summary report. The post incident summary report shall be used to record the final disposition of the investigation and the final disciplinary action taken by the department. Any supervisory personnel, the IAU administrator and the investigating officer may offer a recommendation on disciplinary action, if any, to be taken.

VI. Procedure: Disposition and Disciplinary Action

- A.** After reviewing a complaint investigation, the chief of police shall make a conclusion of fact as to the final disposition of the investigation based on a preponderance of the evidence. The final disposition shall be documented on the post incident summary report. A division commander may also complete and sign the post incident summary form for a complaint investigation after presentation of the investigation and consensus with the chief of police on the disposition and final disciplinary action. The determination of the disposition of an internal affairs investigation shall only be completed by the chief of police. The final disposition of the investigation shall be classified as follows for each allegation:
1. Exonerated (Proper Conduct): The allegation is true. The action of the agency or employee was consistent with agency policy, procedure or rules and regulations.
 2. Substantiated (Improper Conduct): The allegation is true. The action of the employee was inconsistent with agency policy, procedure, rules and regulations, department directives, and/or federal, state, or local laws.
 3. Substantiated on Policy: The allegation is true, but the agency does not have policy to cover the situation. A written directive may be introduced to cover future situations.
 4. Unfounded (False or Not Credible): The allegation is either false or there is no credible evidence to support it.
 5. Unsubstantiated (Insufficient Evidence): There is insufficient evidence to confirm or refute the allegation.
- B.** Based on the disposition and considering any recommendations from the IAU administrator, division commander, and the investigating officer, the chief of police shall determine the final disciplinary action taken by the department. A division commander may also determine the final disciplinary action after consultation with the chief of police. Final disciplinary action shall be recorded on the post incident summary report. Final disciplinary action shall be one of the following:
1. No action.
 2. Remedial training.
 3. Counseling.
 4. Verbal warning.
 5. Written warning.
 6. Transfer.
 7. Suspension.
 8. Demotion.
 9. Resignation in lieu of disciplinary action (option selected by employee).
 10. Termination.

- C. All records related to any complaint investigation, verbal warning, related counseling, and/or remedial training shall be filed and maintained in the IAU files by the IAU administrator. The only exceptions are:
 - 1. Copies of investigative records which support a criminal charge against an employee must be processed and retained using normal records procedures.
 - 2. The original notice of disciplinary action form shall be placed in the employee's personnel file on record with the Human Resources Department whenever disciplinary action is taken which results in a written warning, suspension, demotion, transfer, dismissal, or termination and a copy placed in the IAU files.
- D. Notice of disciplinary action forms placed in the employee's personnel file on record with the Human Resources Department will remain in the file permanently.
- E. When determining the final disciplinary action, prior discipline shall be considered. If dissimilar or unrelated, it shall be the chief's discretion whether to consider disciplinary action occurring more than 24 months prior to the current incident.

VII. Procedure: Notification and Recording

- A. Upon completing a complaint investigation, the employee that is the subject of the complaint shall be notified in writing immediately.
- B. If the chief of police or division commander determine that no action should be taken against the employee, the division commander of the affected employee or the chief of police shall notify the employee of the disposition of the complaint and provide a copy of the post incident summary report to the employee(s). Documentation of the notification to the employee(s) and a copy of the post incident summary shall be provided to the IAU administrator for inclusion in the complaint file.
- C. If disciplinary action is taken, all notices of disciplinary action shall state the effective date of the discipline. If the employee alleges in writing a violation of Iowa code 80F, any disciplinary action will be held in abeyance for a minimum of 10 calendar days.
- D. If final disciplinary action by the chief of police is remedial training, counseling, or a verbal warning, the division commander of the affected employee or the chief of police shall issue the discipline to the employee and provide them a copy of the post incident summary. The post incident summary shall serve as documentation of the notification to the employee. A copy of the post incident summary shall be provided to the IAU administrator for inclusion in the complaint file but will not be included in the employee's personnel file on record with the Human Resources Department.
- E. If final disciplinary action by the chief of police is a written warning, transfer, suspension, demotion, or termination, the notice of disciplinary

action form will be prepared, signed and served on the affected employee by the division commander or the chief of police. A copy of the disciplinary action form and a copy of the post incident summary shall be provided to the employee and the IAU administrator for inclusion in the complaint file.

- F. The notice of disciplinary action form shall state the basis of the complaint and the disciplinary action recommended and approved by the chief of police.
- G. The employee shall sign the notice of disciplinary action form as evidence of receipt.
- H. After service to the employee, the original notice of disciplinary action form shall be placed in the employee's personnel file on record with the Human Resources Department.
- I. The IAU administrator shall ensure any known complainant is notified of the disposition of the complaint.

VIII. Procedure: Appeals

- A. Upon notification of disciplinary action, the employee may:
 - 1. Accept the disciplinary action as stated.
 - 2. Appeal the action as detailed in the city of Urbandale personnel policies and rules.
 - 3. If applicable, appeal the action through the grievance procedure as allowed in the bargaining unit labor contract.
 - 4. If applicable, appeal to the Civil Service Commission.
 - a. If the employee should choose to appeal a suspension, demotion, dismissal or termination to the Civil Service Commission, notification shall be filed with Clerk of the Commission within fourteen (14) calendar days after the first day the adverse action took effect as specified in Chapter 400.20 in the Code of Iowa.
 - b. The appeals process set forth in Chapter 400 of the Code of Iowa (400.18-400.27) shall be the basis from which all procedures will originate.
 - 5. All requested appeals, responses, and procedures associated shall be documented by the chief of police or designee.

IX. Procedure: Employee Interview

- A. All complaints that are classified as needing further investigation shall include an interview with the employee accused of wrongdoing.
- B. Prior to being interviewed regarding a complaint, the accused employee shall receive written notification they are the subject of a complaint investigation or are a potential witness in a complaint investigation and a written summary of the complaint.
- C. No employee shall be required to submit to a truth verification test such as a polygraph. Such tests may be offered by the department in any administrative, civil, or criminal matter. If a truth verification test is used,

the results of such tests shall be used in accordance with federal and state laws. Refusal by the employee to submit to such a test will not form a basis for disciplinary action.

- D. When the examination is specifically directed and narrowly related to a particular internal administrative investigation, an employee may be required to submit to a medical or laboratory examination at the department's expense. Reasonable suspicion must exist to make the investigator believe the employee is under the influence of alcohol and/or drugs before requesting an employee to submit to drug or alcohol testing. Refusal by the employee to submit to such a test may form a basis for disciplinary action. Any employee has the right to request such tests if not offered by the department.
- E. Unless required by law, no employee will be required to submit to testing for AIDS or HIV.
- F. An employee may be required to be photographed and the photograph used in a lineup when reasonable suspicion exists he or she was involved in an incident and the complainant is confident that an identification of the suspect employee can be made.
 - 1. If the suspect employee refuses to be photographed, he or she may be compelled to be photographed.
 - 2. Refusal to comply could result in disciplinary action up to and including termination.
- G. An employee may be required to submit a financial disclosure statement when the actions are essential to a particular internal administrative investigation.
 - 1. If the suspect employee refuses to disclose financial records, he or she may be compelled to supply the records.
 - 2. Refusal to comply could result in the department obtaining a subpoena to acquire the records and disciplinary action up to and including termination.
- H. During administrative investigations, the employee is required to answer questions specifically, directly and narrowly related to the performance of his or her official duties or fitness for duty. Refusal to answer questions during an administrative investigation will likely result in additional charges of insubordination. Should such charges be substantiated, the employee shall be terminated. The employee shall not be required to waive his or her constitutional rights with respect to criminal prosecution.
- I. During a criminal investigation, if an employee is under arrest or is a suspect or target of a criminal investigation, the employee will be informed of his or her rights in accordance with prevailing legal requirements prior to being interviewed. If an employee chooses to invoke any or all of his or her legally protected rights, that employee will not be subjected to charges of insubordination or failure to cooperate for that reason alone.

- J.** Except as authorized or required, employees will not contact persons involved in an administrative or criminal investigation to disclose any information regarding the investigation.

Chapter 4: Personnel Process
Section 31: Recruitment & Selection
Subsection 1: Administrative Practices and Procedures



Policy/Procedure #: 1

Title: Recruitment of Personnel

CALEA Reference#: 31.1.1, 31.1.2, 31.2.1, 31.2.2, 31.2.3, 31.3.1, 31.3.2, 31.3.3, 31.3.4

I. Policy: Recruitment

The Urbandale Police Department and the City of Urbandale recognize the importance of employing mature, even-tempered, intelligent, and honest personnel for all positions. In working towards that goal, the Department shall maintain a comprehensive recruitment program designed to attract the most qualified individuals for employment at the Urbandale Police Department.

II. Procedure: Recruitment Program

- A.** The Department shall implement and maintain an active recruitment program. The Support Services Division shall actively participate with the City of Urbandale Human Resource Department and the Urbandale Civil Service Commission in seeking the best possible candidates for employment.
- B.** Under the authority of Iowa Code chapter 400 and City of Urbandale ordinance chapter 26, the Support Services Division, the Human Resources Department, and the Civil Service Commission shall conduct testing and certify a list of qualified applicants as provided by law.
- C.** The Chief of Police and the Support Services Division shall cooperate closely with the Human Resource Department and the Civil Service Commission in the recruitment and testing process and shall manage the Department's efforts to attract and recruit applicants for vacancies.
- D.** Department personnel may occasionally be assigned to participate in recruitment for the Department. Prior to this assignment, personnel shall receive training in the following areas:
 - 1.** Equal employment opportunities as established by City of Urbandale personnel policies and rules, Chapter 216 of the State of Iowa and Title VII of the Civil Rights act of 1964.
 - 2.** Recruitment needs and commitments.
 - 3.** Career opportunities, salaries, benefits and training.
 - 4.** Federal and state compliance guidelines.

5. Demographics of the community, its needs, its organizations and its educational opportunities.
 6. Cultural awareness of the community and any ethnic groups present in the community.
 7. Techniques of record keeping systems for candidate tracking.
 8. Selection process.
 9. Issues that disqualify candidates.
- E. All department personnel are encouraged to actively engage in recruiting at an individual level. Personnel will be made aware of the Department's equal employment opportunity policies along with information that would assist in recruiting.
 - F. During the course of an active recruiting campaign, the Support Services Division, assisted by the community relations officer may contact various community organizations and leaders seeking their assistance, referrals, and/or advice with reference to the Department's recruitment program. The Department shall also request permission to post job announcements with agencies in contact with individuals who are likely candidates for police recruitment.
 - G. The Department may send personnel to area schools for the purpose of discussing law enforcement career opportunities and recruiting interested candidates. The Department may arrange visits to educational institutions during an active recruitment program or at the request of school officials. Area schools should not be limited by the geographic borders of Urbandale.
 - H. The Department will sponsor student intern programs when requested by an approved college or university. The Support Services Division shall be responsible for the administration and control of the agency sponsored intern program and shall further serve as the liaison between the Department and the college or university requesting intern sponsorship.
 - I. All job announcements authorized and distributed by the Department shall include, at a minimum, the following:
 1. Description of the duties and responsibilities attendant to the advertised position.
 2. Listing of the requisite skills, education and physical requirement.
 3. A statement indicating the Department is an equal opportunity employer.
 4. A statement that a post offer physical, including a test for illegal drugs is required.
 - J. Job announcements shall be advertised through various forms of mass media. The type and extent of media advertisement shall be in cooperation with efforts of the Human Resource Department.
 - K. All job announcements and recruitment advertising authorized and distributed by the Department shall clearly indicate the official application filing deadline.
 - L. Throughout the entire application and testing process, the Human Resource Department shall maintain contact with job candidates in order to keep them

abreast of their current application status. The Support Services Division may assist with this task as needed.

- M. The Department shall not reject applications because of unintentional omissions, errors, or other deficiencies which can be corrected prior to the testing and interview process.

III. **Procedure: Recruitment Plan**

- A. The Support Services Division shall be responsible for producing and implementing the Department's recruitment plan.
- B. The Department shall produce a recruitment plan for full time sworn personnel openings. The recruitment plan shall act as a guide to the Department in working towards establishing a full time sworn personnel work force representative of the Urbandale community in racial, gender, and ethnic composition. The recruitment plan shall include the following elements:
 - 1. The recruitment objectives.
 - 2. A plan to achieve the objectives.
- C. The Support Services Division shall prepare an analysis report concerning the Department's recruitment activities for the past year for full time sworn personnel. This report shall contain the following elements:
 - 1. Measurement of recruitment activities against established quantitative objectives as established in the Department's recruitment plan.
 - 2. Demographic data of current sworn personnel.
 - 3. Analysis of the effectiveness of recruitment to achieve the stated objectives.
 - 4. Recommendations for improvement of the recruitment plan.
- D. Based on the recommendations offered in the yearly analysis, the recruitment plan shall be updated as needed.
- E. The completed recruitment analysis shall be presented to the Chief of Police for review.

IV. **Procedure: Equal Employment Opportunity Plan**

- A. The purpose of the equal employment opportunity plan is to ensure the Department's employment practices are in compliance with federal statutes and standards governing discrimination in employment.
- B. The City of Urbandale's employee handbook contains the City's equal employment opportunity policy statement, conditions of employment, wages and benefits, grievance procedures, and report procedures related to employment practices.
- C. The Urbandale Police Department is committed to the City of Urbandale's equal employment opportunity policy contained in the employee handbook.
- D. The Urbandale Police Department shall create and maintain policies and procedures consistent with the City's equal employment opportunity policy.

Chapter 4: The Personnel Process
Section 31: Recruitment & Selection
Subsection 4: Professional and Legal Requirements



Policy/Procedure #: 1

Title: Personnel Selection

CALEA Reference#: 31.4.1, 31.4.2, 31.4.3, 31.4.4, 31.4.5, 31.4.6, 31.4.7, 31.4.8, 31.5.1, 31.5.2, 31.5.3, 31.5.4, 31.5.5, 31.5.6, 31.5.7

I. Policy: Personnel Selection

The Urbandale Police Department, in cooperation with the Urbandale Civil Service Commission and the City of Urbandale Human Resources Department shall conduct an efficient, effective and unbiased selection process that results in the appointment of individuals who possess the knowledge, skills, and abilities necessary to be successful while employed by the Urbandale Police Department. All selection processes shall conform to state and federal law.

II. Procedure: Selection of Full Time Personnel

A. A detailed description of the selection process for all full and part-time sworn officer positions shall be produced by the Human Resources Department and approved by the Civil Service Commission prior to the announcement of a hiring process. The general selection process for full time and part-time sworn officer positions may consist of the following elements:

1. Submission of the City of Urbandale application.
2. Physical agility testing.
3. Police Officer Selection Test (POST).
4. Panel interview.
5. Civil Service certification.
6. Selection by Chief of Police.
7. Conditional job offer.
8. In-depth background investigation.
9. Polygraph examination.
10. Psychological testing (MMPI).
11. Medical physical and drug screen.

12. Employment as a probationary sworn officer.

- B.** A detailed description of the selection process for full and part-time administrative technicians, administrative specialists, evidence technicians, and community service officers shall be produced by the Human Resources Department and approved by the Civil Service Commission prior to the announcement of a hiring process. The general selection process for administrative technician, administrative specialist, evidence technicians, and community service officer may consist of the following elements:
 - 1. Submission of the City of Urbandale application.
 - 2. Written questionnaire.
 - 3. Panel interview.
 - 4. Civil Service certification.
 - 5. Selection by the Chief of police.
 - 6. Background investigation.
 - 7. Polygraph (evidence technician).
 - 8. Pre-employment drug screen.
 - 9. Employment as a probationary employee.
- C.** A detailed description of the selection process for Chief of Police shall be produced by the Human Resources Department and approved by the Civil Service Commission prior to the announcement of a testing process. The general selection process for Chief of Police may consist of the following elements:
 - 1. Submission of the City of Urbandale application.
 - 2. Civil service interview.
 - 3. Civil service certification.
 - 4. Background investigation.
 - 5. Interview by the City Manager.
 - 6. Selection by the City Manager.
 - 7. Pre-employment medical and drug screen (not required for existing employee).
 - 8. Acceptance/signing of contract by the City Council.
 - 9. Employment as the Chief of Police.

III. Procedure: Professional and Legal Requirements

- A.** The selection process for full and part-time personnel shall be administered by the Human Resources Department with the assistance of the Support Services Division.
- B.** All elements of the selection process for all personnel shall use rating criteria or minimum qualifications that are job related. All rating criteria and minimum qualifications shall be validated as job related by the Human Resources Department or other validation methods.
- C.** The selection process for all personnel shall be administered, scored, evaluated and interpreted in a uniform manner within the classification.

Time limits, oral instructions, practice problems, scoring, etc., shall be clearly established and applied identically for all candidates.

- D. At the time of application, candidates for all positions shall be informed in writing of the following:
 - 1. All elements of the selection process.
 - 2. The expected duration of the selection process.
 - 3. The department's policy on reapplication.
- E. If a candidate is not selected for a position, they shall be informed in writing.
- F. Whether selected or rejected for a position with the department, all applications, records, tests, background information, medical examinations, emotional stability and psychological fitness examinations, or any other selection material collected during an application process shall be stored in a secure location by the Human Resources Department. Only those with legitimate need shall be granted access to the records by the Human Resources Department and only after approval by the Human Resources Director or designee. The records shall be maintained for sixty (60) years.
- G. Material used in the selection process, such as test questions, answer sheets, etc., shall be stored in a secured area by the Human Resources Department. Only those with legitimate need will be allowed to view these items and only while under the supervision of the Human Resources Director or designee.
- H. Any selection material of a sensitive or secure nature shall be disposed of in such a manner rendering it unable to disclose any information.
- I. Selection criteria for all full, part-time, and volunteer sworn positions shall be identical as it pertains to skill, knowledge and ability.
- J. All full, part-time and volunteer sworn positions must meet all State of Iowa requirements for a police officer or reserve officer at the time of their appointment.

IV. Procedure: Administrative Practices and Procedures

- A. A background investigation of each candidate for all positions is conducted prior to appointment to probationary status. The background investigation shall include at a minimum:
 - 1. Verification of qualifying credentials.
 - 2. A review of any criminal history record.
 - 3. Verification of personal and professional references.
 - 4. Education verification.
 - 5. Employment history verification.
 - 6. Review of relevant national or state decertification resources.
- B. Personnel utilized to conduct background investigations shall receive training in how to collect required information.

- C.** When utilizing a polygraph examination as part of the selection process, candidates shall be provided advance notice as to the areas from which the polygraph questions will be drawn.
- D.** When utilizing a polygraph examination as part of the selection process, administration of the examination and evaluation of the results shall only be conducted by trained and certified personnel.
- E.** It shall be prohibited to eliminate a candidate based solely on the results of a polygraph examination; however, the results combined with other information (e.g. pre-test, test or post-test interviews) may be sufficient to eliminate a candidate from consideration.
- F.** A job related medical examination shall be required prior to appointment to probationary status to certify the general health of each candidate for a sworn position.
- G.** An emotional stability and psychological fitness examination by a qualified professional shall be required prior to appointment to probationary status to certify the mental health of each candidate for a sworn position.
- H.** If an employee hired for a sworn position has successfully completed training at the Iowa Law Enforcement Academy or another training facility certified by the Director of the Iowa Law Enforcement Academy before the initial appointment, the probationary period shall be for a period no less than six (6) months and no more than nine (9) months and shall commence with the date of initial appointment as a sworn officer. If the employee has not successfully completed training at the Iowa Law Enforcement Academy or another training facility certified by the Director of the Iowa Law Enforcement Academy before initial appointment as a sworn officer, the probationary period shall commence with the date of initial employment as a police patrol officer and shall continue for a period no less than six (6) months and no more than nine (9) months following the date of successful completion of training at the Iowa Law Enforcement Academy or another training facility certified by the Director of the Iowa Law Enforcement Academy. A sworn officer transferring employment from one jurisdiction to another shall be employed subject to a probationary period no less than six (6) months and no more than nine (9) months. Successful completion of the probationary period shall be determined by the Chief of Police.

Chapter 4: The Personnel Process
Section 33: Training and Career Development
Subsection 1: Administration



Policy/Procedure #:1

Title: Training and Career Development

CALEA Reference#: 33.1.1, 33.1.2, 33.1.3, 33.1.4, 33.1.5, 33.1.6, 33.1.7, 33.2.3, 33.2.4, 33.4.1, 33.4.2, 33.4.3, 33.4.4, 33.5.1, 33.5.2, 33.5.3, 33.5.4, 33.6.1, 33.6.2, 33.7.1, 33.7.2, 33.8.1, 33.8.2, 33.8.3

I. POLICY: Training and Career Development

The Urbandale Police Department shall offer a functional and well documented law enforcement training program to keep employees abreast of the latest techniques in law enforcement, increase productivity and effectiveness, and augment job satisfaction. The training program shall be a continuous and ongoing process offered to employees throughout their career.

II. PROCEDURE: Training Advisory Committee

A. The department shall establish a training advisory committee (TAC). The TAC shall have the following responsibilities:

1. Assist the training coordinator in evaluating the department's overall training needs.
2. Determine the positions or functions that require additional or specialized training and the type of training needed.
3. Ensure State of Iowa and CALEA training requirements are met.
4. Funnel recommendations for additional training from personnel to staff.
5. Recognize and implement training needs that are outside the required training.

B. The sergeant assigned to the Support Services Division shall be tasked as the training coordinator shall manage the TAC and shall be responsible for coordinating semi-annual meetings with members of the TAC. Following each meeting the training coordinator shall produce a report that will include the following:

1. Training processes reviewed.
2. Training recommendations.

3. Implementation issues, if any.
- C. The training report shall be forwarded to the support services division commander and the chief of police for review. If recommendations are approved by the chief of police, the support services division's training function will take action to implement the recommendations.
- D. At a minimum, the composition of the TAC will include the following representatives:
 1. Training Coordinator (assigned support services sergeant)
 2. Accreditation Manager
 3. Handgun/Rifle firearms instructor
 4. Driving instructor
 5. Defensive tactics/LL instructor
 6. One (1) member of the patrol division (By appointment)
 7. One (1) member of the investigation division (By appointment)
 8. One (1) civilian employee (By appointment)
- E. To be an instructor appointed to the TAC, personnel shall be an active, certified instructor in good standing with the department. Selection of instructor positions to serve on the TAC shall be made by the division commanders and the chief of police. Other members of the TAC shall be appointed by the appropriate division commander to represent their respective division. The support services division commander shall appoint a civilian to represent non-sworn personnel.
- F. Personnel assigned to the TAC shall participate for a period of no less than two (2) years, except for the training coordinator and the accreditation manager who shall remain on the committee as long as assigned to those roles within the department. In the event a member is no longer available or qualified due to reassignment within the department or other circumstances, the selection process noted above will be implemented to provide a new member to the TAC.
- G. Appointed members shall serve as the point of contact for personnel within their division; however, this does not prevent suggestions from department personnel not received through their point of contact from being considered by the TAC.

III. Procedure: Administration

- A. Any training provided by the department shall be designated as mandatory or optional. The chief of police, division commanders or the training coordinator may designate any training as mandatory based on the needs of the department. The training shall also indicate if the training is for sworn personnel, civilian personnel or both. Any training designated as mandatory shall be completed by the required employees. Division commanders shall ensure mandatory training is attended by the required personnel in their chain of command.

- B.** All training, mandatory and optional, shall be documented and forwarded to the support services division to be filed in an employee's training file.
- C.** Training announcements shall be made as early as possible to allow for scheduling. An employee may request to be excused from mandatory training by notifying their supervisor. Requests to be excused should only be granted if an alternate time to attend the mandatory training can be scheduled. If an employee is scheduled for optional training and is unable to attend, notice must be given to their immediate supervisor. Unexcused absences from training programs shall be treated in the same manner as if the employee had an unexcused absence from work.
- D.** Time spent attending training shall be considered work hours in compliance with the applicable labor contract or City of Urbandale policy and shall be compensated accordingly. When the training is occurring outside the City of Urbandale city complex (e.g. not occurring at the police department, city hall, or the library), compensation for travel, meals and housing shall be compliant with the applicable labor contract and/or City of Urbandale travel reimbursement policy.
- E.** Only official U.P.D. vehicles shall be authorized for travel to and from any training event where reimbursement for travel costs can be requested under the City of Urbandale's travel reimbursement policy. Employees seeking to utilize the convenience of their personally owned vehicles for travel to and from a training assignment will do so at their expense unless receiving prior approval from their division commander and the chief of police. Arrangements for utilizing official vehicles for training assignments will be coordinated through the support services division.
- F.** All training shall require a lesson plan. Each lesson plan shall be approved by the training coordinator, division commander or the chief of police. Each lesson plan shall include the following:
 - 1. A statement of performance and job related objectives
 - 2. The content of the training.
 - 3. Specific instruction techniques used.
 - 4. List of resources used in the development of the curriculum.
 - 5. List of resources required in the delivery of the training.
 - 6. Identification of any tests used in the training process.
- G.** The training coordinator or designee shall maintain a record of training classes conducted to include the lesson plan, names of attendees, and if test(s) are administered, performance of individual attendees on said tests. The training records for each employee shall be updated to document the employee's participation in any type of training. Records of training to include lesson plans shall be permanently maintained per the Iowa League of Cities Record Retention Manual that was adopted by the City of Urbandale.

H. Remedial training is personalized training to correct a specific deficiency identified by testing and other evaluation processes during training or routine job performance. Remedial training shall occur in the following manner:

1. Remedial training shall be made available by the training coordinator, as the need arises and shall be documented through the use of a lesson plan and attendance log. Although timetables are difficult to impose upon remedial efforts due to physical problems, injury, skill development, available seats, course type and instructor availability, etc., a period of 30 days from the point of observed and documented need for remedial training shall be considered reasonable. Extensions to remedial training beyond the 30 days period may be granted by a division commander or the chief of police. Any extension of remedial training beyond 30 days shall be documented by a command staff memorandum detailing the circumstances that warrant the extension.
2. Exception to the 30 day time period may occur in critical skill areas such as use of force, firearms proficiency and less lethal weapons. In critical skill areas, remedial training shall occur as soon as practical and will normally be administered within days. These exceptions will be addressed on a case-by-case basis with input from instructor(s), immediate supervisor, and the training coordinator.
3. At the end of 30 days, or earlier in case of a critical skill area, if failure (or specific deficiency) still exists, then a determination shall be made in conjunction with the instructor(s), immediate supervisor, and training coordinator, as to the issue of incompetency.
4. A written recommendation shall be drafted to the chief of police. Disciplinary action may result.
5. Members assigned to remedial training shall display an effort to participate. Failure to do so may result in disciplinary action.
6. Specific remedial training is required for less lethal weapons and firearms as stated in the Operations Manual in Chapter 1 Section 1.3.1(Use of Force) and Section 1.3.9 (Firearms).

IV. Procedure: Law Enforcement Academy

A. The department shall utilize the services of the Iowa Law Enforcement Academy for basic law enforcement training. In exigent circumstances, other police academies may be utilized. The department shall only utilize basic law enforcement training programs in academies offering the State of Iowa mandated training and certification as stated in Iowa Code Section 80B. The curriculum of these programs shall be based upon state law and a job task analysis of the most frequent assignments in required skills, knowledge and abilities.

- B. The training coordinator shall maintain a close liaison with the staff of the Iowa Law Enforcement Academy in order to stay abreast of current training curriculum and provide input to the academy training program.
- C. When requested through the director of the academy, the department may make instructors and resources available to assist in completing the training curriculum.
- D. Under normal circumstances, liability for any training-related injury or impairment to a newly hired sworn officer while attending academy training shall be borne by the department. The newly hired sworn officer shall be considered "on duty" while attending academy training and shall enjoy the same protections and be compensated the same as other probationary employees with the department. This does not release the academy from exercising due diligence in the health and welfare of the employee while attending the academy. Any employee who feels their health or welfare is not being properly managed while at the academy shall alert the training coordinator as soon as possible.
- E. The academy shall be responsible for the administration of the prescribed training programs and provide for the fair and non-discriminatory testing of each student. Liability for said administration shall be borne by the academy.
- F. Specific instruction on departmental policies, procedures, rules and regulation shall be the responsibility of the department and shall be taught to the newly hired sworn officer during the department's field training program.

V. Procedure: Newly Hired Sworn Officer Training

- A. All full-time and part-time employees as well as volunteers responsible for performing sworn law enforcement duties must complete a basic law enforcement training program equivalent to that required of full-time sworn officers.
- B. All newly hired sworn officers must comply with the State of Iowa mandatory basic law enforcement training requirements, regardless of prior experience or training. In accordance with the Iowa Code Section 80B, no person shall receive a permanent appointment as a law enforcement officer unless that person has been awarded a certificate attesting to successful completion of the minimum standards basic law enforcement training course or received a waiver of the basic training requirements as a result of the officer having already successfully completed a basic training program prescribed by the State of Iowa. Basic law enforcement academy training of newly hired sworn officers shall include:
 - 1. A curriculum based on the tasks of the most frequent duties of a fully functioning sworn officer of the department.

2. Use of evaluation techniques designed to measure the newly hired sworn officer's competency in the required knowledge skills and abilities.
 3. The academy utilized by this department shall provide a documented orientation session for all new newly hired sworn officers at the time academy training begins. The information contained in the session shall include:
 - (a) The organization of the academy.
 - (b) The academy's rating, testing and evaluation system.
 - (c) Physical fitness and proficiency requirements.
 - (d) Daily training schedules.
 - (e) The academy's rules and regulations.
- C. Employees attending newly hired sworn officer training shall be expected to observe all rules and regulations set forth by the course director and must maintain passing grades on newly hired sworn officer training examinations.
1. Newly hired sworn officers shall maintain a liaison with the training coordinator during their academy training, keeping the coordinator apprised of their progress and any problems encountered. The training coordinator shall maintain liaison with departmental and academy staff in order to assure an orderly transition from the academy to the field training program.
 2. Serious violations of training academy rules or failure to maintain passing grades shall result in dismissal from the department.
- D. All newly hired sworn officers shall be required to successfully complete the field training officer (FTO) program administered by the department. The FTO program shall train newly hired sworn officers in the basic tasks of a fully functioning sworn officer of the department. The Training Coordinator from the support services division shall be assigned to administer the FTO program and manage the field training officers. As part of administering the FTO program, the supervisor assigned shall ensure the following:
1. Newly hired sworn officers are assigned to the FTO program for a minimum of 160 hours not including classroom hours from academy training or certification.
 2. Unless part of the prescribed training of the FTO program, no police personnel are authorized to carry a weapon or make a full-custody arrest until the completion of the FTO program and completion of a basic law enforcement training program. In addition, no police personnel are allowed to carry a weapon until satisfactorily completing training pertaining to the department's use of force policy and passing proficiency testing as stated in Chapter 1 Section 4.1.1 (Use of Force) and Chapter 1 Section 4.3.1 (Firearms) in the Operations Manual.

3. When necessary, liaison with academy staff reference newly hired sworn officer's progress and to stay abreast of any training deficiencies.
 4. Rotations of newly hired sworn officer's field assignments.
 5. Guidelines are established for the evaluation of newly hired sworn officers by field training officers.
 6. Required reports from field training officers and supervisors are completed.
 7. The curriculum for the FTO program is based on the tasks most frequently encountered by a fully functioning sworn officer for the department.
 8. The evaluation techniques used by FTOs and supervisors for newly hired sworn officers are consistent and measure competency in the required skills, knowledge, and abilities.
- E.** Field training officers shall be selected for the position as a collateral duty assignment as prescribed in Chapter 2 Section 11.5.1 (Temporary, Specialized and Collateral Duty Assignments) of the Operations Manual. All field training officers shall receive initial instruction on administering the FTO program prior to being assigned a newly hired sworn officers for training. Field training officers shall meet regularly with the supervisor in charge of the FTO program for in-service training to stay abreast of the latest training techniques as well as department policy, procedures, rules and regulations.
- F.** The training coordinator shall supervise the officers and other supervisors assigned to administering of Field Training Officer program for the department and shall include completing an annual collateral duty evaluation of the officers assigned as field training officers.
- G.** The training coordinator shall conduct an annual administrative review of the field training program providing recommendations for policy or training modifications and provide the review to the chief of police.

VI. Procedure: Prior Basic Law Enforcement Training

- A.** When hiring a new officer with prior law enforcement experience or certification the following will be completed:
1. A documented review of the new officer's completed basis law enforcement training curriculum.
 2. A documented review of the new officer's completed supplemental in-service and specialty training.
 3. A documented comparison of the completed training to the State of Iowa basis law enforcement training program to identify training gaps.
 4. A documented completion of any additional training to address any identified training gaps.

VII. Procedure: In-Service, Shift briefing, and Accreditation Training

- A. All sworn personnel shall complete annual in-service training consistent with the position held and the functions performed. In-service training shall encompass a legal update as well as any other relevant topics as determined by the chief of police, division commanders, and the training coordinator.
- B. Shift briefing training shall utilize the time at the beginning or end of a sworn officer's shift. Sergeants shall utilize shift briefing training to cover a variety of topics that typically require less than one hour to instruct. The training coordinator may also utilize shift briefing training to cover required training topics.
- C. If the topic during shift briefing training is mandatory training for other employees, all supervisors shall be notified in advance of the training to allow additional personnel to attend.
- D. Shift briefing training shall be subject to the same requirements as other training as stated in this policy.
- E. All agency personnel shall receive accreditation training within 30 days of employment or within 30 days of completion of newly hired sworn officer academy training.
- F. An employee assigned to the position of accreditation manager for the department shall receive specialized accreditation training within one year of being appointed. The specialized training may include training from the previous accreditation manager, CALEA conference training sessions, participation in mock assessments, attending periodic meetings with the Midwest CALEA PAC, etc. The accreditation manager shall also be responsible for appropriate training of any personnel assigned to assist with the accreditation process on a full or part-time basis.

VIII. Procedure: Specialized Training and Non-Sworn Employee Training

- A. The department shall list all assignments in which training and specialized training is required of personnel on a master training list. The list will contain the following categories:
 - 1. Description of initial required training.
 - 2. Ongoing in-service requirements, if applicable.
 - 3. Supervised on the job training, if applicable.
- B. Personnel assigned to the Suburban Emergency Response Team (SERT) shall be required to participate in training and readiness exercises. The training requirements of SERT members are detailed in the SERT SOP manual.
- C. Initial training shall occur for all non-sworn positions within the department as listed below:
 - 1. Civilian records supervisor/CALEA manager: CALEA Accreditation Manager certification (online training course), Power DMS, Tracs, Laserfiche, RMS, Open Records law, UCR auditing and reporting, rater training for the Performance Evaluation, NCIC TAC & certification,

Shieldware, phone system, time clock management, Adobe Pro, cash register

2. Administrative specialist assigned to the Office of the Chief of Police: Initial training: Phone system, New World, invoicing, timeclock manager, Power DMS, Adobe Pro, Laserfiche.
 3. Administrative specialist assigned to the Support Services Division: Initial training: Power DMS, NCIC certification, Laserfiche, cash register, TRACS, phone system, Shieldware, victim witness coordination, crime analysis, computerized background searching, Central Square RMS, UCR auditing and reporting, Adobe Pro, Iowa Courts online.
 4. Administrative technicians assigned to the Support Services Division: Laserfiche, cash register, NCIC certification, phone system, Adobe Pro, Iowa Courts online, Shieldware, TRACS, UCR auditing and reporting, Central Square RMS, Power DMS, Fingerprinting, PetPoint (as assigned), department identification card software (as assigned).
 5. Community service officer: Laserfiche, cash register, NCIC certification, phone system, Adobe Pro, File on Q, Iowa courts on-line, Shieldware, TRACS, MS Office, Adobe video editor, department identification software, Central Square RMS, PetPoint, department inventory software, fingerprinting.
- D. In addition to the training listed above, all non-sworn employees shall complete the following:
1. Orientation: Introduction to the department's role, purpose, goals, policies and procedure.
 2. Orientation: Departmental working conditions and regulations.
 3. Orientation: Responsibilities and rights of employees including a statement clearly indicating the position does not possess the authority of a sworn officer to make a full-custody arrest.
 4. Initial training: Bias issues including legal aspects.
 5. Initial training: CALEA accreditation training within 30 days of employment.
 6. Initial training: Mental illness entry level training.
 7. Ongoing In-service: Ethics, mental illness, biased issues including legal aspects, All Hazards Plan, NCIC re-certification, Records software programs as needed (Power DMS, RMS, Tracs, Laserfiche, Shieldware, MS Office), open records law as needed.

IX. Procedure: Career Development

- A. The department shall provide job related supervisory training to all newly promoted personnel.
- B. Supervisory personnel shall receive training on conducting career development for personnel under their direction from the City of Urbandale

Human Resources Department. Additional training may be obtained from outside sources. Training provided by human resources shall include:

1. The purpose of career development for employees.
 2. The process for supporting an employee's career development.
- C. Career development for the department shall consist of the following:
1. Employees are encouraged to apply for training and other educational opportunities as they arise. Assistance in locating training opportunities in specific areas of interest may be garnered from the training coordinator. Command staff shall consider career development needs when approving requests for training.
 2. Employees are encouraged to apply for collateral duty assignments and rotating assignments to reach their career goals. When applying for the assignment, employees shall make their career aspirations clearly known. Command staff should consider the career development needs of employees when assignments to collateral duty and rotating assignments are made.
 3. During annual evaluations, employees and supervisory personnel may discuss the employee's career goals. When requested, supervisors shall assist the employee in developing career goals and a plan to achieve the goals.

Chapter 4: The Personnel Process
Section 34: Promotion
Subsection 1: Professional and Legal Requirements



Policy/Procedure #: 1

Title: Promotion

CALEA Reference#: 34.1.1, 34.1.2, 34.1.3, 34.1.4, 34.1.5, 34.1.6

I. Policy: Promotion

A policy is established to inform employees of the promotional process utilized to fill vacant supervisory positions in the Police Department.

II. Procedure: Promotional Process

- A.** The Chief of Police or designee, in conjunction with the City of Urbandale Civil Service Commission and the Human Resources Department shall have the authority to administer and be responsible for the promotional process for personnel within the Police Department. The Chief of Police or designee shall work in concert with the Human Resources Department and the Civil Service Commission to establish a testing mechanism that accurately measures the knowledge, skills, and abilities of personnel to be successful in the supervisory role they are seeking.
- B.** Minimum eligibility requirements to apply for a promotion to sergeant shall be as follows:
 - 1.** A minimum of four (4) years of experience as a sworn officer with the Urbandale Police Department. Time in grade will be determined from hire date to the close of the application period as stated in the promotional posting.
 - 2.** A minimum of an associate degree with at least 60 semester hours or equivalent from an accredited college or university. Preference will be given to those with a degree in criminal justice, public administration, or a related field.
- C.** Minimum eligibility requirements to apply for promotion to captain shall be as follows:
 - 1.** A minimum of two (2) years of experience at the rank of police sergeant for the Urbandale Police Department. Time in grade will be

determined from date of promotion to the close of the application period as stated in the promotional posting.

2. Possession of a bachelor's degree with a minimum of 120 semester hours or equivalent from an accredited college or university. Preference will be given to those with a degree in criminal justice, public administration, or a related field.
- D. Minimum eligibility requirements to apply for the civilian records supervisor position shall be as follows:
1. An associate degree with at least 60 semester hours or equivalent from an accredited college or university.
 2. Five years' experience in office management with supervisory responsibilities.
- E. The testing and evaluation process for the for promotion shall be conducted as follows:
1. The promotional process shall be administered by the City of Urbandale Human Resources Department. The Human Resources Department may enlist the assistance of a qualified testing agency to assist.
 2. The promotional process shall be based on study material provided to the candidates no later than when the positions are posted as open for application. The promotional process (e.g. written test, assessment center, interview, etc.) shall be established by the Department in conjunction with the City of Urbandale Human Resources Department and approved by the Civil Service Commission for the City of Urbandale.
 3. All details of the promotional process, to include minimum passing scores, shall be established by the Civil Service Commission and shall be included in the posting.
- F. Promotional lists shall be established in accordance with Iowa Code Chapter 400 and the Urbandale Civil Service Rules and Regulations. The promotional lists shall be established as follows:
1. Promotional list(s) shall be established from passing scores received during the promotional process.
 2. Each candidate shall be ranked on the applicable promotional list from highest to lowest score obtained during the promotional process. The scoring method for all phase of the process will be listed in the promotional posting to include how the final score for eligibility list will be obtained. The promotional list shall contain no more candidates than allowed under Iowa Code Chapter 400. Ties shall be addressed according to Iowa Code Chapter 400.
 3. Promotional lists shall be valid for a period of two (2) years from the date of certification by the Civil Service Commission.

- G.** Once a certified promotional list has been established by the Civil Service Commission, the Chief of Police may appoint any employee on the certified list to fill vacant positions. The Chief shall evaluate the promotional potential of each candidate on the certified list and select the most qualified employee for promotion. The Chief may query current staff members to receive input as to the promotional potential of each candidate but the promotional decision shall be made by the Chief of Police. The Chief shall consider the following areas when determining the promotional potential of each candidate:
1. Work history
 2. Educational background
 3. Experience
 4. Communication skills
 5. Integrity
 6. Knowledge, skills, and abilities to perform the essential functions of the position.
- H.** The hiring of external candidates is permitted as established by Iowa Code Chapter 400.
- I.** All testing elements used to evaluate candidates for promotion shall be job related and nondiscriminatory.
- J.** Candidates failing to be selected for promotion shall be eligible to reapply during the next promotional process.
- K.** Material used in the promotional process, such as test questions and answer sheets, shall be stored in a secured area by the Human Resources Department or if applicable, by the agency utilized to perform the testing. Only those with legitimate need will be allowed to view these items and only while under the supervision of the Human Resources Director or designee or representatives of the testing agency.
- L.** Candidates shall have the right to review and appeal the results of a promotional process as stated in the Urbandale Civil Service Commission rules and regulations and Chapter 400 of the Iowa Code.
- M.** The Police Department shall provide a minimum of thirty (30) days advance written notice of a promotional process. Notice time will begin with the official posting of the position by the Department or the City of Urbandale Human Resources Department.
- N.** Current employees of the Department that are promoted are not subject to a probationary period. New employees to the Department are subject to a probationary period as established by Iowa Code Chapter 400.

III. Procedure: Mentoring

- A.** A mentoring program is established to create a formalized process for sworn officers interested in advancing to a supervisor position to receive guidance and coaching from current sworn staff members.

- B.** Officers wishing to participate in the mentoring program must meet the minimum requirements established by this policy to apply for a sergeant position.
- C.** Officers shall submit a memorandum to their respective division commander stating their interest in participating in the mentoring program. The memorandum shall outline the officers desire to participate in the program, outline how they have met the minimum requirements to apply, and summarize any other qualifications they possess.
- D.** Once received, the division commander will present the information to the chief for discussion and approval to participate.
- E.** If multiple officers within a division/specific patrol squad are approved to participate, seniority will determine the order of participation; however, officers on the civil service promotional list will be given priority.
- F.** Division commanders shall determine which supervisors within their division will serve as mentors.
- G.** Participation in the mentoring program is not a requirement to apply for supervisory position within the department.
- H.** Those participating in the program will not receive any additional pay or benefits.
- I.** The period of mentoring shall be for no more than 2 months barring special circumstances and officers may only participate in the program once every 2 years.
- J.** Upon completion of the mentoring program, the supervisor assigned as the mentor shall complete a memorandum to the division commander and the chief of police accompanied by the mentorship checklist summarizing the tasks completed noting any strengths or areas of needed improvement. The memo shall also include a debrief of the officer participating in the program.
- K.** Updated mentoring checklists shall be maintained by each division.

Chapter 4: The Personnel Process
Section 35: Performance Evaluation
Subsection 1: Administration



Policy/Procedure #: 1

Title: Performance Evaluation

CALEA Reference#: 35.1.1, 35.1.2, 35.1.4, 35.1.5, 35.1.6, 35.1.7, 35.1.8

I. Policy: Performance Evaluation

The Urbandale Police Department recognizes the value of an unbiased and fair performance evaluation. Department staff members shall administer a performance evaluation system designed to assist employees with their on-the-job performance of assigned duties. Properly conducted performance evaluations ensure personnel problems are identified and addressed promptly and fairly allowing the employee to enjoy optimum job satisfaction.

II. Procedure: Performance Evaluations

- A.** The performance evaluation system utilized by the Department shall be developed and administered by the City of Urbandale Human Resources Department.
- B.** All supervisory personnel shall receive training on the evaluation system prior to conducting any evaluations.
- C.** The performance evaluation system shall measure the following areas:
 - 1. Attendance/punctuality.
 - 2. Job knowledge.
 - 3. Productivity/Initiative.
 - 4. Quality of work.
 - 5. Customer service.
 - 6. Professionalism.
 - 7. Teamwork/relationships.
 - 8. Problem solving.
 - 9. Safety.
 - 10. Decision-making (supervisors only)
 - 11. Leadership (supervisors only)
 - 12. Safety leadership (supervisors only)
- D.** The performance evaluation system shall adhere to the following guidelines:
 - 1. The evaluation shall cover a specific time period.

2. Explanatory comments must accompany each rating of needs improvement or exceeds expectations.
 3. Each performance evaluation shall be reviewed and signed by the rater's supervisor and the Chief of Police.
 4. Employees shall sign the evaluation as acknowledgement of receipt.
 5. Employees shall be allowed to make written comments to supplement the completed performance evaluation. The comments shall be restricted to the contents of the evaluation.
 6. A copy of the completed performance evaluation shall be provided to the employee.
- E.** Contested performance evaluation for all employees shall follow the appeal process established in the City of Urbandale Employee Handbook.
- F.** All original copies of performance evaluations shall be retained by the City of Urbandale Human Resources Department. Copies of the evaluation may be retained by department staff members who are directly involved in the supervision of an employee to reference performance improvement and goals noted in the previous evaluation. Access to performance evaluations shall be restricted to those with a right and a need to know.
- G.** The Department shall require an annual performance evaluation on all full-time employees, and all sworn personnel to include reserve officers. For full time employees, all evaluations shall be conducted by the supervisor to whom the employee directly reports. For reserve officers, all evaluations shall be completed by the coordinator of the reserve program or designee.
- H.** All entry level probationary employees shall have monthly performance evaluations. Probationary reserve officers shall have quarterly performance evaluations.
- I.** Criteria used to evaluate the performance of an employee and the measurement definitions shall be specific to the assignment of the employee during the evaluation period.
- J.** If an employee's performance is deemed unsatisfactory, they shall be advised in writing in a timely manner. The notice of unsatisfactory performance shall be accompanied by stated actions that must be taken by the employee to correct the unsatisfactory performance.
- K.** During the annual performance evaluations, supervisors shall meet in person with the employee and discuss the following:
1. Results of the performance evaluation.
 2. Level of performance expected for the next rating period.
 3. Any change in rating criteria as well as any goals for the upcoming rating period.
 4. Career counseling on topics appropriate to the employee's position.
- L.** Performance reviews of supervisory personnel shall include a review of the quality of the ratings the rater is giving to their subordinates. The Chief of Police may also review the quality of the ratings given to subordinates by any supervisor in the Department. If any problems, inconsistencies, or rating errors are discovered, the supervisor of the rater responsible for the

evaluation or the Chief of Police shall counsel the rater on the issues discovered and document the counseling. Raters may also be required to attend further training on rating performance evaluations.

- M.** Except where responsibilities are stated, the Chief of Police shall be exempt from this policy and shall have their annual performance evaluated by the City Manager for the City of Urbandale.

Chapter 4: The Personnel Process
Section 35: Performance Evaluation
Subsection 1: Administration



Policy/Procedure #: 9
Title: Personnel Early Intervention System
CALEA Reference#: 35.1.9

I. Policy: Personnel Early Intervention System

The personnel early intervention system is designed to help identify and assist employees who display behavior inconsistent with the department's mission and may need additional training, supervision, or counseling. The intent of the early intervention system is not disciplinary in nature. The process shall allow the employee the best chance to succeed by identifying problems and/or deficiencies as early as possible and change the unwanted behavior prior to entering a disciplinary tract. Actions by the department as part of the early intervention system are intended to be a positive effort towards this goal.

II. Procedure: Early Intervention System

- A.** The early intervention system captures critical incidents over a period of time in order to identify those employees who may benefit from assistance or further training.
- B.** Numerous categories shall be tracked to quantify the events and situations that form the early intervention system. All categories shall be reported according to departmental policy with copies being forwarded to the chief of police. The categories to be tracked shall include but not be limited to the following:
 - 1. Pursuits
 - 2. At fault accidents
 - 3. Complaint and internal affairs investigations (excludes unfounded, exonerated, court issue, and demonstrably false complaints)
 - 4. Use of force
 - 5. Use of sick leave
 - 6. Habitual or documented tardiness
 - 7. Ongoing or sudden poor performance

8. Inability to effectively work with co-workers
 9. Incidents of workplace violence
 10. Garnishment of wages
 11. Being the subject of a restraining order
 12. Any disciplinary action taken by the department
- C.** Support services supervisory personnel shall conduct semi-annual review of the department's early intervention system to identify patterns of behavior that may be indicative of a need for intervention. Five or more incidents occurring during a six-month review period shall require an intervention review; however, any supervisor can request an intervention review at any time for any number of incidents to include a single incident if the behavior by an employee indicates there may be a need for intervention. An incident that is captured in several different categories shall be considered a single incident for the purposes of this review (e.g. pursuit that results in disciplinary action).
- D.** The support services supervisor conducting the semi-annual review, or a requested intervention review shall notify the division commander of the employee when the early intervention system is activated.
- E.** The division commander of the effected employee shall coordinate with the direct supervisor to conduct a review of the incidents that prompted the early intervention system to be activated. A report detailing the findings of the review shall be produced and presented to the chief of police. The report shall include an interview with the effected employee. The review may include recommendations.
- F.** The chief of police shall determine final course of action on all early intervention system activations. The course of action may include but not be limited to the following:
1. No further action- The employee's performance is within policy.
 2. Mandatory remedial or additional training designed to improve employee's skills and performance.
 3. Informal counseling.
 4. Supervisory job performance interview.
 5. Informal monitoring by FTOs or supervisors.
 6. Formal monitoring by FTOs or supervisors with prescribed reviews and reports.
 7. Referral to professional counseling.
 8. Mandatory or voluntary referral to the city's employee assistance program (EAP).
 9. Referral to the department's peer support team.
 10. Substance abuse counseling or treatment.
 11. Permanent or temporary reassignment.
- G.** A finding other than "no further action" will require the division commander to develop and implement a performance improvement plan for the

employee. The plan shall state timelines for activity to be completed. All performance improvement plans shall be approved by the chief of police.

- H. The performance improvement plan will be communicated to the employee by their direct supervisor or the division commander. The division commander will be responsible for reviewing the performance improvement plan with the direct supervisor for compliance and completion. Completion of the improvement plan and the results therein shall be reported to the chief of police.
- I. The chief of police shall conduct a documented annual evaluation of the early intervention system for effectiveness.

Chapter 5: Law Enforcement Operations
Section 40: Crime Analysis
Subsection 1: Crime Analysis



Policy/Procedure #: 1
Title: Crime Analysis
CALEA Reference#: 40.1.1

I. Policy: Crime Analysis

Information generated through crime analysis is integral to the successful prevention and/or suppression of criminal activity by law enforcement. It is the policy of the Urbandale Police Department to utilize crime analysis to provide systematically concise and timely statistical information to both line and staff personnel. Crime analysis shall be a coordinated effort by all the divisions.

II. Procedure: Crime Analysis

- A.** The Department shall establish a systematic method for the collection and analysis of crime data and its distribution. Objectives of crime analysis include the recognition of crime patterns or trends, the effective deployment of manpower, the successful development of crime prevention programs, and the integration of crime analysis to maximize efforts of all units within the Department.
- B.** The primary components of an effective crime analysis system include the collection, analysis, and distribution of crime data in useable form and the subsequent evaluation of the applicability and timeliness of the data. The Support Services Division shall have the primary responsibility for crime analysis by providing needed reports and statistical data from records. Support services shall also support the crime analysis function through community relations, press information, and technical support.
- C.** Data shall be collected and distributed in a crime analysis report to all supervisory staff and the Chief of Police at the quarterly staff meeting.
- D.** During the quarterly staff meeting, the crime analysis report shall be reviewed and the following shall be discussed:
 - 1.** Identify patterns and trends.
 - 2.** Formulate conclusions and recommendations.

- E. The Support Services Civilian Records Supervisor shall be responsible for evaluation of the crime analysis data for accuracy prior to distribution.
- F. The crime analysis report may be forwarded to other appropriate personnel (patrol, K-9, CID, community relations, etc.) based on the conclusions and/or recommendations.

III. **Procedure: Action plans**

- A. Based on monthly statistical reports and the quarterly crime analysis, the Chief of Police, division commanders or assigned line supervisors may develop an action plan. The action plan shall include but not be limited to:
 - 1. Force Distribution - Special assignments and personnel needed.
 - 2. Measurement criteria (short-term goal & performance measurement).
- B. If developed by a line supervisor, action plans will be reviewed with the appropriate division commander prior to implementation.
- C. At predetermined intervals, the division commanders or line supervisors shall produce a summary report of their action plan including report of actions (goals) and the results (performance measurements). Copies of the action plan summary report shall be distributed to the Chief of Police and the division commanders.
- D. Subsequent crime analysis shall include the effect of any previous or current action plans.

IV. **Procedure: Collection and Analysis of Data**

- A. The Support Services Division shall have the primary responsibility for gathering data needed to perform the crime analysis function. The collection of data shall be aided by other divisions as needed.
- B. Data or information used in the crime analysis function shall include but not be limited to the following:
 - 1. Incident reports
 - 2. Arrest reports
 - 3. Supplemental investigative reports
 - 4. Field interview reports
 - 5. Other departmental reports/correspondence
 - 6. Other law enforcement agency information
 - 7. Data within the records management system
 - 8. National Crime Information Center
 - 9. Mid States Organized Crime Information Center
 - 10. Law Enforcement Intelligence Network
 - 11. Iowa Fusion Center
 - 12. Iowa sex offender registry
 - 13. Social networking sites
 - 14. Other miscellaneous resources
- C. Crime analysis information is intended to benefit personnel in their efforts to achieve near-term crime control and prevention objectives. Crime analysis can maximize this benefit via:

1. The identification and analysis of the modus operandi of individual criminals.
 2. The recognition of offense trends in terms of time, location and their inter-relationships.
 3. The identification of actual or potential hazards to police personnel.
- D. Crime analysis information also plays an integral role in the success of the Department's long-term plans, priorities, manpower requirements, and budgetary concerns. This is accomplished by the following:
1. The collection and collation of related data.
 2. An accurate assessment of crime trends by offense code, offender characteristics and crime trends by location.
 3. Distribution of statistics and analysis to appropriate command personnel.
 4. Recommendations provided to the Chief of Police by the command staff based on crime analysis.
 5. Evaluation and feedback by users of the data regarding the quality of the information.
- E. The variables to be researched in the analysis of crime activities may include but are not limited to the following:
1. Frequency by type of offense:
 - a. Selected crimes
 - b. All reported incidents
 2. Location factors:
 - a. Calls for service/criminal activity by territory
 - b. Calls for service/criminal activity by locale, i.e., parking lots, residences, street, etc.
 3. Time variables:
 - a. Time of day
 - b. Day of week
 - c. Month of year
 - d. Seasonality
 4. Victim demographics
 5. Target descriptors
 6. Suspect descriptors
 7. Suspect vehicle descriptors
 8. Modus operandi components
 9. Physical evidence information
 - a. Similarities/distinctions
 - b. Fingerprints

V. Procedure: Distribution of Crime Analysis Information

- A. All division commanders have the responsibility to notify the Chief of Police of current and potential crime trends or patterns as they are documented.

- B.** Internal distribution of pertinent information shall be made to affected units on a timely basis.
- C.** Data relevant to the operations of specific components will be directed to the appropriate personnel.
- D.** Data relevant to the development and maintenance of the Department's goals and objective and multi-year plan shall be provided to the Chief of Police and division commanders.
- E.** Distribution of crime analysis information to outside law enforcement agencies shall be made at the discretion of the Chief of Police except where noted below.
- F.** Dissemination for public knowledge shall be approved by the Chief of Police.
- G.** Dissemination by subordinate personnel will be governed by the respective division commander.
- H.** Dissemination by investigative members, such as that which regularly occurs at area detectives' meetings, shall be at the discretion of the Criminal Investigation Division Commander with the understanding that barring special circumstances the information shall be shared with other jurisdictions.
- I.** The dissemination of crime analysis information intended to enhance both public awareness and community support, will be made at the discretion of the Support Services Division Commander and the Chief of Police. Such information is generally provided to:
 - 1. The media.
 - 2. Community groups.
 - 3. Individual citizens, upon request.
- J.** Confidential information developed via intelligence operations shall be rigidly controlled. Dissemination will be at the discretion of the Chief of Police or designee and shall be solely restricted to law enforcement agencies. Such information may include:
 - 1. Known offenders
 - 2. Suspected offenders
 - 3. Investigative leads
 - 4. Modus operandi
- K.** Assessment of the crime analysis may occur as an agenda item at command staff meetings. Topics of discussion may include:
 - 1. Timeliness of the data.
 - 2. Clarity of format of the data.
 - 3. Usefulness of the data.
 - 4. Applicability of the data.
 - 5. Scope of the data.

Chapter 5: Law Enforcement Operations
Section 40: Crime Analysis and Intelligence
Subsection 2: Criminal Intelligence Analysis



Policy/Procedure #: 1

Title: Intelligence Information

CALEA Reference#: 40.2.1, 40.2.2, 40.2.3

I. Policy: Intelligence Information

The collection and dissemination of intelligence information necessary to support the control of serious criminal activity also represents a potential threat to the constitutional rights and the privacy of individuals to whom such data relates. It is the policy of the Urbandale Police Department to fulfill its dual obligations of preventing and solving crime and maintaining homeland security, while protecting the privacy and constitutional rights of individuals.

The Department shall gather, analyze, and produce intelligence information directed toward the identification of specific individuals or organizations suspected of criminal activity and/or present a potential threat to the public, performing these activities with due respect for the rights of those involved, and disseminating the information only to authorized individuals as prescribed by Chapter 692 of the Iowa Code, 661 Iowa Administrative Code Chapter 81, and other applicable laws of the State of Iowa and of the United States.

It is the goal of the Department to carry out the intelligence function in order to advance the principles of intelligence-led policing, and contribute toward the crime prevention, security, investigative, enforcement, and other public safety priorities identified by the Department, provide tactical, operational, and strategic intelligence information and services to the department and its partners, and ensure the intelligence function is carried out in a manner consistent with applicable local, state, and federal laws, regulations, and administrative rules, and professional and ethical criminal intelligence practices.

II. Procedure: Definitions

A. Criminal Investigative Data - Information collected in the course of an investigation where there are reasonable grounds to suspect that specific criminal acts have been committed by a person.

- B.** Criminal Intelligence Information - Intelligence information which has been evaluated to determine if it is relevant to the identification of and the criminal activity engaged in by an individual who or organization which is reasonably suspected of involvement in criminal activity and meets submission criteria for a criminal intelligence system that complies with Title 28 Code of Federal Regulations, Part 23.
- C.** Intelligence Assessment - An analysis of information based in whole or in part upon intelligence data.
- D.** Intelligence Data - Information on identifiable individuals compiled in an effort to anticipate, prevent, or monitor possible criminal activity.
- E.** Intelligence Information - A general term used in this policy to refer to criminal intelligence information, intelligence data, or intelligence assessment.
- F.** Intelligence-led Policing - The dynamic use of intelligence to guide operational law enforcement activities to targets, commodities, or threats for both tactical responses and strategic decision making for resource allocation and/or strategic responses. A model in which intelligence serves as a guide to operations, with the intelligence function at the heart of the decision making process.
- G.** Non-Criminal Predicate Surveillance Data - Information on individuals, pertaining to participation in organizations, groups, meetings or assemblies, where there are no reasonable grounds to suspect involvement or participation in criminal activity by any person.
- H.** Suspicious Activity - A reported or observed incident, activity, or behavior that may be indicative of intelligence gathering or pre-operational planning related to criminal activity (including terrorism) or other illicit intention. A report of suspicious activity that is received by the Criminal Investigation Division (CID) is considered intelligence data.

III. Procedure: Responsibility of Agency Personnel

- A.** Each member of the Department is responsible for gathering and reporting information in support of and acting on information produced by the intelligence functions within the Department.
- B.** In addition to the responsibilities delegated to each member of the Department, the Chief of Police has established CID as having the primary responsibility for coordinating activities that include planning and managing intelligence priorities/information requirements, and collecting, evaluating, collating, analyzing, and disseminating information in support of the intelligence function, under the direction of the CID commander.

IV. Procedure: Training

- A.** All employees with access to intelligence information shall be trained on the proper use and control of intelligence information. Officers shall receive this training as part of their field training program.
- B.** CID shall be responsible for providing a training program to address the proper use and control of intelligence information.

- C. The training coordinator shall ensure all new employees receive the training during their probationary period and the training is documented in their respective training file.

V. Procedure: Criminal Intelligence File

- A. All information in the Department's intelligence files shall be consistent with criminal intelligence file criteria as described below.
 - 1. Information that may be collected and stored includes:
 - a. Information about individuals who:
 - (1) Are suspected of being involved in the actual or attempted planning, organizing, financing, or commission of criminal acts;
 - (2) Are suspected of being involved in criminal activities with known or suspected crime figures.
 - b. Organizations, businesses, and groups that:
 - (1) Are suspected of being involved in the actual or attempted planning, organizing, financing, or commission of criminal acts.
 - (2) Are suspected of being operated, controlled, financed, or infiltrated by known or suspected crime figures for use in an illegal manner.
- B. Only information with a criminal predicate and which meets the Department's file criteria will be collected and stored in the intelligence files. Intelligence data on individuals and organizations shall refer to possible criminal activities that may have an impact on or pose a threat to Urbandale or other Iowa communities. Examples of criminal activity categories include, but are not limited to:
 - 1. Narcotics manufacturing and/or trafficking
 - 2. Terrorism and criminal extremism
 - 3. Unlawful gambling
 - 4. Money laundering
 - 5. Ongoing criminal conduct and organized crime
 - 6. Loan sharking
 - 7. Extortion
 - 8. Smuggling of contraband
 - 9. Vice and pornography
 - 10. Infiltration of legitimate businesses for illegitimate purposes
 - 11. Stolen securities
 - 12. Major crime including homicide, burglary, auto theft, kidnapping, destruction of property, robbery, fraud, forgery, fencing stolen property, and arson
 - 13. Manufacture, use, or possession of explosive devices for fraud, intimidation, or political reasons
 - 14. Bribery
 - 15. Corruption of public officials
 - 16. Threats to public officials and private citizens

17. Traveling criminals

18. Other criminal activities designated by the CID commander.

- C. Gathering, storing, analyzing, and sharing of intelligence information shall be based on intelligence priorities and information requirements of the Department that are communicated to all personnel.
- D. Non-criminal predicate surveillance data (as defined in this policy) shall not be placed in files, manuals, or automated data storage systems by any member of the Department. Intelligence files shall not contain information about the political, religious, or social views, associations, or activities of any individual or any group, association, corporation, business, partnership, or other organization unless such information directly relates to criminal conduct or activity, or to the investigation of criminal conduct or activity, and the subject of the information is, or may be involved in criminal conduct or activity. Specifically, intelligence files shall not include information on an individual or group merely on the basis of:
 - 1. Support for causes some may consider to be unpopular
 - 2. Race, ethnicity, religion, or political affiliation.
 - 3. Non-criminal personal habits
 - 4. Associations with individuals that are clearly not of a criminal nature.
- E. Employees shall comply with all legal and privacy requirements in the handling of intelligence information, including Chapter 692 of the Iowa Code, 661 Iowa Administrative Code Chapter 81, and Title 28 Code of Federal Regulations, Part 23, as applicable.

VI. Procedure: Gathering and Submitting Intelligence

- A. Information which supports established intelligence priorities and information requirements and complies with criminal intelligence file criteria shall be submitted by members of the Department to CID in an Information/Lead notification form. The form shall be submitted to CID by utilizing the specific email account established for submission.
- B. The collection, storage, and dissemination of intelligence data by Department personnel shall be predicated on suspicion a crime has been committed or is being planned. Members of the Department shall ensure information submitted to CID is relevant to criminal activity.
- C. Information gathering and investigative techniques shall be carried out in a lawful manner. Members of the Department shall not knowingly use unlawful means to acquire information from sources (including confidential informants, physical, electronic, photographic, and other technical surveillance devices).
- D. Evaluation of source reliability and information validity. Information submitted to CID shall be evaluated by the contributor with respect to source reliability and information validity. Evaluating the information's source and content indicates to future users the information's worth and usefulness. Whenever possible, information submitted to CID should be

the product of dependable and trustworthy sources of information. Some of the information contained in intelligence files, however, may consist of unverified allegations or information, including reports of suspicious activity. Written procedures for evaluating source reliability and information validity will be established by CID.

VII. Procedure: Receipt, Evaluation, and Storage of Information

- A.** The Department's intelligence files shall be maintained by CID and shall be filed separately from all other records. The Department's intelligence files may contain intelligence data, intelligence assessments, and criminal intelligence information. Intelligence information in the Department's intelligence system may contain information from the news media, public records, criminal investigative data, and other sources.
- B.** Upon receipt of information that is to be processed and stored as intelligence information, CID personnel shall review the information for accuracy and quality control, giving particular attention to the following criteria:
 - 1.** Determination of a criminal nexus. Intelligence information that is retained for processing and storage must have a nexus to a criminal activity or threat.
 - 2.** Lawfully-acquired data. Any information known to have been obtained by a member of the Department in violation of any applicable federal, state, or local law or ordinance shall not be included in the intelligence files. CID employees shall reject any information that has not been lawfully acquired by a member of the Department and shall immediately forward such information to the CID commander.
 - 3.** Source reliability, information validity, and information security level as articulated in this policy.

VIII. Procedure: Information Security and Release Authority

- A.** All intelligence files shall be physically and electronically secured, as applicable. Access to all intelligence information shall be controlled and recorded. Computer systems that store intelligence data shall be secure and protected against unauthorized attempts to access modify, remove, or destroy stored information.
- B.** Contributors of data to CID shall provide information to assist with categorizing the data in order to protect sources, methods used, current investigations, and the right to privacy for all individuals, as well as to reflect the contributor's preferences for how accessible the information shall be to other authorized persons. These categories will provide a structure that will enable the Department to control subsequent access to and dissemination of intelligence data. Written procedures for designating information security levels and release authority classifications will be established by CID.

IX. Procedure: Dissemination of Intelligence Information

- A. Intelligence information shall be shared insofar as information sharing is consistent with Iowa law and procedures established by this Department.
- B. Criminal intelligence information may be disseminated or re-disseminated by CID consistent with Chapter 692 of the Iowa Code.
- C. Intelligence data shall only be disseminated when recipients possess the right-to-know the information, when they have the need to know the information, and when their intended use of the information is considered reasonable. In accordance with Chapter 692 of the Iowa Code, and 661 Iowa Administrative Code Chapter 81, intelligence data may be released only to the following:
 - 1. Peace officers, on a need-to-know basis.
 - 2. Criminal or juvenile justice agencies, on a need-to-know basis.
 - 3. State or federal regulatory agencies, on a need-to-know basis.
 - 4. An agency, organization, or person when disseminated for an official purpose and in order to protect a person or property from a threat of imminent serious harm.
- D. Intelligence assessments may be disseminated to any agency or organization if necessary or carrying out the official duties of the agency or organization, or to a person if disseminated for an official purpose, and to a person if necessary to protect a person or property from a threat of imminent serious harm.
- E. A list of the agencies, organizations, or persons receiving the intelligence information and the date and purpose of the dissemination must be maintained by CID.

X. Procedure: Auditing and Purging Files

- A. Intelligence information shall be maintained in accordance with the goals and objectives of the Department, and should only include information that is both timely and relevant. Intelligence information in the Department's intelligence system must be periodically reviewed, audited, and purged to ensure that the information is accurate, relevant, and current to the needs and objectives of law enforcement.
- B. Criminal intelligence information shall be reviewed, audited, and when appropriate, purged at least every five (5) years. Criminal intelligence information shall also be reviewed, audited, and when appropriate, purged whenever an employee reviews the information for dissemination or other purposes.
- C. The decision to purge or to retain criminal intelligence information shall be based upon the following criteria:
 - 1. Age of the intelligence data.
 - 2. Frequency of use
 - 3. Quality and reliability
 - 4. Completeness and accuracy.
 - 5. Usefulness.

6. Availability of the information from other sources
 7. Other relevant criteria.
 8. Misleading or inaccurate information. If any information in the Department's intelligence system is found at any time to be misleading, untrue, or otherwise inaccurate or unreliable.
 9. When information is ordered expunged by competent judicial authority, the information shall be immediately purged from the system.
- D.** At the completion of the audit/review process, a record of the intelligence file audit shall be created.
- E.** Policies and procedures relating to the intelligence function will be reviewed at least annually to ensure they are current and sufficient. This review will be initiated and/or conducted by the CID Commander.

Chapter 5: Law Enforcement Operation
Section 41: Patrol
Subsection 1: Administration



Policy/Procedure #: 1

Title: Patrol

CALEA Reference#: 41.1.1, 41.1.2, 41.3.1, 41.3.2, 41.3.3, 41.3.5, 41.3.6

I. Policy: Patrol

The Urbandale Police Department shall maintain a proactive and innovative patrol division to address the daily demands for police service in the community.

II. Procedure: Patrol Shift Assignments

- A.** The Department shall maintain continuous patrol coverage twenty four (24) hours a day seven (7) days a week through the use of patrol shifts as determined by the Chief of Police.
- B.** The Patrol Commander shall ensure sworn officers assigned to the Patrol Division are assigned to a specific shift based on seniority with the Department. Supervisors in the Patrol Division shall be assigned to a patrol shift at the discretion of the Chief of Police.
- C.** Shift selection will take place on a semi-annual basis or prior to the institution of any change in work schedule or shifts. Prior to the selection of shifts, the Department will designate the dates on which each position on each shift will be scheduled to work for the ensuing six month period. The semi-annual selection of shifts and the final posting of officer's shift schedules shall occur in March and September barring any special circumstances that would delay the process.
- D.** Officers assigned to the Patrol Division after the semi-annual shift selection has been completed shall be allowed to select a shift based on their seniority. Any other officers are affected by the selection will be allowed to re-select a shift based on their seniority. This will continue until all officers affected have selected a shift based on seniority.
- E.** The Chief of Police reserves the right to assign an officer to any shift in lieu of seniority with valid justification.

- F. The jurisdictional boundaries of the City of Urbandale shall be divided into specific patrol areas. Patrol shift supervisors shall assign officers to specific patrol areas each shift based on available manpower and need. Each patrol shift supervisor shall determine the frequency of the rotation of officers to different patrol areas. Patrol areas shall be determined by the Chief of Police.
- G. Each patrol shift shall be scheduled for a set number of hours each day as determined by the Chief of Police and implemented by the Patrol Commander. Each shift shall work a scheduled number of days on and off as determined by the Chief of Police and implemented by the Patrol Commander.

III. Procedure: Shift Briefing

- A. Prior to the beginning of each patrol shift, the patrol shift supervisor shall conduct a shift briefing. During the briefing the following tasks shall be performed:
 - 1. Assignment of officers for the upcoming shift.
 - 2. Assignment of specific vehicles and equipment.
 - 3. Briefing on calls for service from the previous shifts.
 - 4. Relaying of any pertinent information for the upcoming shift.
- B. Prior to deploying for duty, the patrol shift supervisor shall inform WestCom of personnel assignments for the upcoming shift.
- C. Shift briefings may also be utilized by patrol to liaison with the Investigation Division to share information on intelligence, crime trends, wanted persons, etc.

IV. Procedure: Patrol Vehicles

- A. All vehicles assigned to patrol shall be equipped with operational emergency lights and siren.
- B. When an officer prior to their shift or a supervisor during the inspection process, observes missing, depleted, nonfunctional, or damaged equipment, a repair/service request form shall be completed and forwarded to the Support Services Division. The following equipment shall be contained in each patrol vehicle:
 - 1. Police radio
 - 2. Radar unit
 - 3. Lights and siren control panel
 - 4. Gun Rack
 - 5. First aid kit & AED
 - 6. Fire extinguisher
 - 7. Digital camera
 - 8. P.B.T.
 - 9. Flashlight
 - 10. Flares
 - 11. Stop sticks

- 12. Video camera
 - 13. Traffic safety vest
 - 14. Bar code reader
 - 15. Printer
 - 16. Computer
 - 17. Door unlocking device
 - 18. Tire chalk
 - 19. Windshield marker
 - 20. Window punch
 - 21. Latent fingerprint kit
- C. All occupants of a department owned vehicles are required to use their safety belts regardless of their position in the vehicle. Exceptions to the safety belt requirement are as following:
- 1. Officers are allowed discretion in the use of a safety belt when arriving on a call for service in which a quick exit of the vehicle may be necessary; however, these instances shall be extremely limited and the officer must be able to articulate the need to remove the safety belt prior to stopping the vehicle.
 - 2. Occupants riding in the rear of the rapid deployment vehicle are not required to wear a safety belt.
 - 3. In cases where the detainee is combative, it is not necessary to utilize safety belts if doing so would expose the transporting officer to substantial risk of attack.

V. Procedure: Protective Vests

- A. Protective vests shall be provided to all sworn members of the Department as well as all reserve officers.
- B. A protective vest shall be worn by all officers working patrol duty or any other duty requiring a uniform. When conditions warrant, such as a specialized assignment that does not involve enforcement activity, supervisors may temporarily suspend the requirement to wear a protective vest.
- C. When engaged in enforcement activity, investigators shall be required to wear a protective vest. Exceptions may be granted by a supervisor for undercover type operations.
- D. Command staff and other administrative assignments normally not engaged in enforcement activity are exempt from the requirement wear a protective vest.
- E. If an officer is exempt from the protective vest requirement as stated above, their vest shall be readily available in their office, work locker, or department vehicle for donning in case of an emergency situation.
- F. Urbandale officers assigned as operators to the Suburban Emergency Response Team (SERT) shall be issued a tactical ballistic protective vest that offers an even greater level of protection than the standard protective

vest. Urbandale SERT officers shall be required to wear their tactical vests during high risk tactical situations as stated in the SERT SOP.

- G.** All officers participating in a planned warrant execution shall be required to wear a protective vest unless the location or person has already been secured.

Chapter 5: Law Enforcement Operations
Section 41: Patrol
Subsection 1: Administration



Policy/Procedure #: 3

Title: Patrol Bicycle and Other Special Purpose Vehicles

CALEA Reference#: 41.1.3

I. Policy: Special Purpose Vehicles

The demands for police service require the use of different styles and types of special purpose vehicles for efficient and effective policing. The appropriate use of these vehicles will ensure the safety of officers and the public.

II. Procedure: Patrol Bicycle

A. The Department has established a patrol bicycle unit to educate, interact, and enhance officer presence in the City of Urbandale. The unit shall have the following objectives:

- 1.** Conduct concentrated patrols in Urbandale parks, recreation areas, bike trails, and schools.
- 2.** Improve contact with the general public, schools, and businesses as part of the Department's community oriented policing efforts.
- 3.** Establish a positive, progressive image between the community and the Department.
- 4.** Assist in crime prevention, criminal apprehension, and special operations.
- 5.** Provide bicycle safety education to schools, businesses, and the public.

B. Bicycles used by officers shall be of a mountain bike style able to accommodate proper safety equipment as well as storage for first aid supplies.

C. The patrol bicycle is authorized for use to patrol all areas of Urbandale. The bicycle's primary use is for patrolling parks and the bike trail system. The bicycle may also be utilized for special events with traffic or pedestrian congestion for increased mobility. There will be no bicycle patrol during inclement weather unless directed by a supervisor.

D. Patrol bicycle officers may respond to emergency calls within a reasonable radius of their deployment and as directed by the on-duty watch commander.

- E. Under no circumstances shall the patrol bicycle be utilized for any type of pursuit situation involving a motorized vehicle.
- F. The patrol bicycle unit shall be assigned a supervisor to manage the unit by the Patrol Division Commander.
- G. When deployed, patrol bicycle officers shall be under the direct supervision of the on-duty watch commander unless functioning as part of a special assignment with a designated supervisor. Any supervisor may approve or deny qualified personnel to operate the patrol bicycle based on manpower needs, weather, or other relevant factors.
- H. Bicycle officer for the Department shall be considered a collateral duty assignment and selection shall follow the procedures outlined in Chapter 2 Section 16.2.1 of the Operations Manual. Once selected for the collateral duty, officers must complete an instructional course to become certified to operate the patrol bicycle. Additionally, each certified bicycle officer shall be required to complete refresher training annually.
- I. The Patrol Division Commander or designee, shall be responsible for scheduling of all operations involving patrol bicycle, ordering of equipment, repairing equipment, facilitation of meetings and the ordering of new and/or replacement equipment and uniforms. Assistance in ordering or repairing of equipment and uniforms may be obtained from the Support Services Division.
- J. The unit shall utilize a certified bicycle maintenance officer or a reputable bicycle shop to maintain the bicycles in a safe and operable condition. Records of maintenance shall be kept by the supervisor in charge of the unit.
- K. An inspection the bicycles shall be performed prior to utilization to ensure all equipment is operational and the bicycle is safe to deploy.
- L. When deployed, all traffic laws and bicycle safety rules applicable to operation of a bicycle shall apply to the officer. Officers are except from conforming to traffic laws when needed to take enforcement action. Patrol bicycle officers are prohibited from conducting traffic stops.
- M. Patrol bicycle officers shall advise the communication center when conducting any enforcement activity. During deployment the following shall apply:
 - 1. Unless absolutely necessary, the bicycle shall not leave the officers sight unsecured.
 - 2. When out of sight of the officer, the bicycle shall be locked to a stationary object. All equipment shall also be secured.
- N. Each bicycle shall have an equipment bag, headlight, rear reflector or light and a small medical kit to respond to basic emergencies.
- O. Officers authorized to ride the patrol bicycle shall be required to wear proper riding equipment to include:
 - 1. Helmet
 - 2. Bicycle uniform approved by the Patrol Division Commander.

III. Procedure: Rapid Deployment Vehicle (RDV)

- A. The rapid deployment vehicle (RDV) is primarily used for transportation of the Suburban Emergency Response Team (SERT) to operational assignments and training.
- B. Under rare circumstances, the RDV may be utilized to transport prisoners when a large number of subjects have been detained and there is a need to remove them from the scene quickly. Only compliant detainees shall be transported in the RDV. When utilized as a detainee transport, a minimum of one officer shall be assigned to the rear compartment with the detainees for control purposes.
- C. The RDV may be operated by any SERT member or officer. No special licensing is required. When the RDV is being utilized for non SERT activity, supervisor approval must be obtained.
- D. Proper maintenance of the RDV shall be the responsibility of the Support Services Division. Any employee that observes damage or deficiencies of the RDV or associated equipment shall complete a repair request form and forward to Support Services.
- E. The RDV holds equipment specific to the operational and training needs of SERT. A UPD SERT officer shall be tasked with maintaining an equipment checklist for the RDV as well as completing semi-annual inspections of said equipment for operational readiness. The equipment in the RDV shall include but not be limited to:
 - 1. Rams
 - 2. Sledge hammer
 - 3. Breacher pack
 - 4. Halligan tool
 - 5. Ballistic shield
 - 6. Fire extinguisher
 - 7. Gas pack
 - 8. Mirrors
 - 9. Fireman's hook
 - 10. Ballistic blanket
 - 11. Power inverter
 - 12. WatchGuard charging docks
 - 13. Glass house kit
 - 14. Traffic cones
 - 15. Road flares
 - 16. Ladder
 - 17. Break and rake tools
 - 18. Bang poles
 - 19. Wallbanger

IV. Procedure: Special Event Vehicles

- A. During special events the Department occasionally uses motorized vehicles donated for temporary use from area businesses such as all-terrain vehicles, golf carts, etc. Any employee wishing to utilize a special event vehicle shall obtain permission from a supervisor. Prior to use, the

officer shall demonstrate proficiency and knowledge of the use of said vehicle for the approving supervisor.

- B.** Under no circumstances shall any special event vehicle be utilized in any type of pursuit.
- C.** Any deficiencies noted by an officer operating a special event vehicle shall be relayed to the supervisor in charge who shall in turn notify the owner of the vehicle. If the deficiencies affect the safe operation of the vehicle, it shall no longer be utilized until repaired.

V. Procedure: Canine Vehicle

- A.** The Department shall have a specially equipped vehicle intended for the purpose of transporting the canine. The canine officer shall use the vehicle to transport the canine to and from work or to other canine related duties. Personal use of the vehicle is not allowed. The canine vehicle shall be a "take home" vehicle allowing the canine officer to safely transport the canine to and from work and respond to calls for service directly from his/her home. Except for vehicle maintenance requirements, only the canine officer is authorized to operate the vehicle. The canine vehicle shall be a marked unit with lights and siren. The canine vehicle shall be utilized by the canine officer to perform canine duties as well as patrol officer duties. The canine vehicle shall not be used to transport detainees.
- B.** The canine officer shall meet all the requirements to operate a marked patrol unit. This shall include driving training as required by the Department in Chapter 5 Section 41.2.2 (Vehicle Pursuits) of the Operations Manual. The canine officer shall also have operational knowledge of the specialized equipment installed in the canine vehicle to include:
 - 1. Door releases
 - 2. Automatic temperature controls
- C.** The canine officer shall be responsible for the condition and maintenance of the canine vehicle. Any needed repair or replacement of the vehicle or the equipment assigned to the vehicle shall be submitted on a repair/service order to the Support Services Division. As the canine vehicle is utilized for daily patrol use, the vehicle shall be inspected quarterly as stated in Chapter 6 Section 53.1.1 of the Operations Manual.
- D.** The canine vehicle shall have a cage designed specifically for the transport of canines. The cage shall be of a design that gives the canine adequate room for extended periods of stay and constructed in a manner that safeguards the canine from injury. The cage shall protect the driver and other occupants of the vehicle from the canine and shall shield the canine from outside contact.
- E.** Canine vehicle(s) shall have a temperature monitoring device that will alert the canine officer by an audible alert when the vehicle temperature exceeds safe levels. This system shall also incorporate a remote controlled door opening system to allow rapid exit of the canine for

emergency situations. The canine vehicle shall also contain all the equipment of a regular patrol unit to include:

1. Police radio
2. Radar unit
3. Lights, siren and controls
4. Gun rack (shotgun and AR-15)
5. First aid kit & AED
6. Fire extinguisher
7. Digital camera
8. P.B.T.
9. Flashlight
10. Flares
11. Stop Sticks
12. Video camera
13. Traffic safety vest
14. Bar code reader
15. Printer
16. Computer
17. Door unlocking device
18. Tire chalk
19. Windshield marker
20. Window punch
21. Latent fingerprint kit

VI. Procedure: Department All-Terrain Vehicle:

- A.** The Department all-terrain vehicle is utilized for patrolling city bike trails and parks, transportation during community policing or special events, transportation to remote or underdeveloped areas, or any other law enforcement purpose as needed. The all-terrain vehicle may be utilized for limited use on city streets based on the needs of the Department. The all-terrain vehicle shall not be utilized for motor vehicle traffic stops or motor vehicle pursuits.
- B.** The all-terrain vehicle may be operated by any employee of the Department upon supervisory approval. Prior to initial operation, employees are required to complete an introductory training course.
- C.** The all-terrain vehicle shall be assigned to the Patrol Division and shall be inspected annually for proper functioning and a condition by the Support Services Division.
- D.** Proper maintenance of the all-terrain vehicle shall be the responsibility of the Support Services Division. Any employee that observes the need for regularly scheduled service, damage, or deficiencies to the all-terrain vehicle or associated equipment shall notify their supervisor and complete a repair/service request form and forward to the Support Services Division.
- E.** When operating the all-terrain vehicle on the city trails, officers shall utilize caution and operate the vehicle at a safe and reasonable speed with the knowledge that pedestrians and bicyclists will likely be utilizing the trails.

- F. The all-terrain vehicle shall be equipped with a first aid kit to respond to medical emergencies.

VII. Procedure: SERT Sniper Van

- A. The SERT sniper van is used for transportation of the Suburban Emergency Response Team (SERT) snipers to operational assignments and training.
- B. The SERT sniper van may be operated by any employee. No special licensing is required. When the SERT sniper van is being utilized for non SERT activity, supervisor approval must be obtained.
- C. Proper maintenance of the SERT sniper van shall be the responsibility of the Support Services Division. Any employee that observes damage or deficiencies of the SERT sniper van or associated equipment shall complete a repair request form and forward to Support Services.
- D. The SERT sniper van does not hold any equipment. The van is simply utilized to transport SERT snipers to and from operational assignments and training. A UPD SERT officer shall be tasked with completing semi-annual inspections of the SERT sniper van for operational readiness.

VIII. Procedure: Crime Scene Investigation (CSI) Vehicle

- A. The CSI vehicle is utilized to transport CSI personnel and equipment to a crime scene. The vehicle shall also be utilized to transport evidence collected at a scene back to the Department or to the appropriate lab for analysis. The vehicle shall not be used for any other purpose without the approval of a supervisor.
- B. The CSI van may be operated by any employee. No special licensing or training is required.
- C. Proper maintenance of the CSI vehicle shall be the responsibility of the Support Services Division. Any employee that observes damage to deficiencies to the CSI van or associated equipment shall complete a repair/service request form and forward to Support Services. CSI personnel shall be responsible for the annual inspection on the CSI vehicle.
- D. The following equipment shall be kept in the CSI vehicle (note: specific items may be stored in the Department due to temperature concerns (extreme cold or heat):
- Black bag with Number Placards 1-80, Letter Placards A-Z, Orange foam pointers
 - Orange Cones
 - Small Orange Cones
 - Wire Flag Markers
 - Duct Tape
 - String
 - Instant Shooter ID Kit
 - Absorption Analysis Kit (gunshot residue)
 - Electrostatic Dust Print Lifter
 - Post Mortem Fingerprint Kit
 - Dialing Measuring Device

- 25 ft Tape Measure
- 100 ft roll tape Measure
- 100 ft Tape Measure
- Yellow Adhesive Back Tape Measure
- Clear 6" rulers
- White 6" ruler
- Roll of 2" white adhesive tape measure
- Compass
- Sheet Protectors
- REMCO Trace Tape
- Elimination Fingerprint Kit
- Metal Stakes
- Crime Scene Tape
- Bolt Cutters
- Disposable Fingerprint Brushes
- Disposable Tweezers
- Sterile Scalpels
- Blood Tubes
- Aluminum Trays
- Pill Boxes
- Misc. jars
- Bio-hazard tubes
- Foam Impression Kits
- Assorted Evidence Bags
- Gun and Knife Boxes
- Paint cans for fire residue
- Spray Bottles
- Metal Trajectory Rods
- Sirchi BlueMaxx Portable Illumination Kit
- Shoe Covers
- Gloves
- Masks
- Tyvek suits
- Blood borne pathogens kits
- Sharps container
- Batteries, Garbage bags, superglue
- Tarps, boots, vest
- Flood light
- CSI tool kit
- Bungee Cord
- Nylon Ribbon Rope
- Braided Rope
- Assorted garden tools
- Crime Scene Barrier

- Tripod
- Shovel
- Metal Detector
- Metal rod (for trajectory)
- Search Warrant Kit - Evidence Bags
- Ladder
- First Aid Kit
- Flashlights

Kits (moved from lab to van due to weather)

- Digital Camera and Accessories
- Foster-Freeman Crime Lites
- Trajectory Kit
 - Roll of 2" white adhesive tape measure
 - Gunshot Residue Presumptive Test
 - Green Trajectory String
 - Yellow mason string
 - 8" level
 - 2" line level
 - small laser light
 - adhesive clips
- Uncontaminated Latent Print Kit
 - Sterile brushes
 - Sterile Powders (black, grey, red, green)
 - Sterile Magnetic Brush
 - Sterile Magnetic Powders (black, grey, red, green)
 - Aluminum Trays
 - Card, lifts
- Presumptive and Enhancement Kit
 - White small particle Reagent
 - Black small particle Reagent
 - Hard Evidence-Cyanoacrylate pouches
 - Presumptive Blood Tests
 - Presumptive Semen Tests
 - Luminol
 - Blue Star
- Casting Kit – Plaster Casting
 - Microsil Casting Material
 - AccuTran casting gun and supplies
 - Dental Stone
- DNA KIT
 - Disposable Masks
 - Gloves
 - Sterile Cotton Swabs
 - Sterile Water
 - Disposable Tweezers
 - Sterile Tweezers

- Sharpie Marker
- Drying Chamber for Swabs
- Alcohol Prep Pads
- Knife Set
- Metal Tweezers
- Fingernail Collection Kit

IX. Procedure: Patrol Commander vehicle:

- A.** The Patrol commander vehicle is utilized by the Patrol Division Commander for the performance of his/her duties as well as other department personnel as approved by the Patrol Division Commander or the Chief of Police. The vehicle is authorized for use for any police function to include patrol assignments as needed. The main purpose of the vehicle is for use by the Patrol Division Commander to perform various divisional assignments. The vehicle may also be utilized as a mobile commander center during various incidents. The vehicle is authorized to transport the Patrol Division Commander from their residence to their work assignments. The vehicle is not authorized for personal use.
- B.** When functioning as a patrol unit, the operator shall meet all the requirements to operate a marked patrol unit. This shall include driving training as required by the Department in Chapter 5 Section 41.2.2 (Vehicle Pursuits) of the Operations Manual. When not being utilized as a patrol unit, no special licensing or training is required.
- C.** The Patrol Division Commander shall be responsible for the condition and maintenance of the patrol commander vehicle. Any needed repair or replacement of the vehicle or the equipment assigned to the vehicle shall be submitted on a repair/service order to the Support Services Division.
- D.** The patrol commander vehicle shall contain the following equipment:
 - 1. Police radio
 - 2. Lights and siren control panel
 - 3. First aid kit
 - 4. Fire extinguisher
 - 5. Flashlight
 - 6. Traffic vest
 - 7. Tire chalk
 - 8. Window punch
 - 9. Fire Hydrant Wrench
 - 10. White Board
 - 11. School Maps
 - 12. Ballistic Helmet
 - 13. Ballistic Entry Vest
 - 14. Command Box (2)

X. Procedure: Small Unmanned Aircraft Systems (sUAS)

- A.** The Department shall obtain all authorizations, permits, certifications, and licensing from the Federal Aviation Administration (FAA) as required for the specific type of sUAS being deployed.

- B.** All deployments of the sUAS must be specifically authorized by the chief of police, patrol division commander or designee.
- C.** The sUAS is a shared asset with the Urbandale Fire Department but is an asset maintained by the Urbandale Police Department. Fire personnel operating the sUAS shall be required to meet all of the requirements of this policy.
- D.** Use of the sUAS is authorized when needed to provide an aerial visual perspective for emergency situations and other exigent circumstances including but not limited to the following:
 - 1.** For situational awareness in understanding the nature, scope, and scale of an incident and planning an appropriate response.
 - 2.** To document crime scenes, accident scenes, fire scenes, and other types of scenes where an aerial perspective and documentation will be beneficial.
 - 3.** To assist in the search for missing persons and aid in rescue missions.
 - 4.** To support tactical deployment and/or perimeter security.
 - 5.** For intelligence information when conducting physical surveillance operations to identify routes of travel, neighborhoods, and member placements for acquiring or reacquiring surveillance targets in public areas.
 - 6.** To search for suspects eluding capture or that have escaped from police custody.
 - 7.** Security during large public gatherings.
 - 8.** To aid law enforcement training.
- E.** The main use of the sUAS shall be to support official law enforcement or public safety missions; however, the sUAS may be used for other official uses for the City of Urbandale or other governmental bodies such as project documentation, engineering, media production, etc.
- F.** Use of the sUAS shall meet all requirements of the United States Constitution and the Constitution of the State of Iowa. Operators of the sUAS shall be trained to identify when use of the sUAS requires a search warrant.
- G.** The sUAS shall not be equipped with any lethal or less lethal weapons of any kind.
- H.** Digital media produced by the sUAS shall be managed in the following manner:
 - 1.** If the digital media captured by the sUAS is part of a response to a public safety incident, it shall be considered evidence and stored as established in Chapter 9 Section 83.1.1 utilizing the incident or case number for identification. The media captured shall also be documented in the appropriate reporting mechanism to include date, time, location, and personnel capturing. All procedures for the management and use of evidence in department policy shall apply.

2. If the digital media captured is not public safety related (construction project, community event, etc.) the media shall not be considered evidentiary and can be stored and shared as appropriate.
 3. Digital media captured as intelligence information shall meet all the requirements of Chapter 5 Section 40.2.1 (Intelligence Information) and be managed by the Criminal Investigation Division commander or designee.
 4. Digital media may be approved for training purposes upon approval by the chief of police or the patrol division commander.
- I. Any personnel assigned to operate the sUAS must be licensed in accordance with FAA regulations and complete an agency approved training program to ensure proper use. Additional training shall occur as needed to ensure continued proficiency. Only authorized, trained, and licensed personnel shall operate the sUAS.
 - J. An operations log shall be maintained by the patrol division to document use of the sUAS. All uses, including training, shall be tracked through the use of the log. The supervisor assigned to oversee the sUAS program shall audit the log periodically to ensure flights are being properly recorded.
 - K. The supervisor assigned to oversee the sUAS program shall be responsible for the condition and maintenance of the sUAS and shall complete a documented inspection of the sUAS and related equipment annually.
 - L. Equipment associated with this vehicle shall include the following:
 1. Spotlight
 2. Speaker
 3. Controller (2)
 4. Batteries (8)
 5. Carrying case
 6. Battery charging station
 7. Shoulder harness
 8. Remote controller (2)

Chapter 5: Law Enforcement Operations
Section 41: Patrol
Subsection 1: Administration



Policy/Procedure #: 5
Title: Police Canine
CALEA Reference#: 41.1.5

I. Policy: Police Canine

A policy is established to provide guidelines for the management of the Department's canine unit and use of the unit in field operations. Due to superior senses and agility, the trained law enforcement canine is a valuable supplement to police personnel. Utilization of a police canine requires adherence to procedures that properly control the use of force potential and channel the specialized capabilities of the canine into acceptable crime prevention activities. It is the policy of the Department the police canine unit be utilized under the following guidelines for community service, crime prevention, proactive enforcement of laws, and the detection and apprehension of criminal offenders.

II. Procedure: Canine Selection and Evaluation

A. New canines will be selected from a vendor approved by the Chief of Police specializing in the provision of canines for law enforcement agencies. Personnel assigned to assist in the selection of a new canine for the Department shall complete the following steps:

1. Determine the type of canine needed by the Department and what services the canine will provide. Services may include:
 - (a) Narcotics detection
 - (b) Article detection
 - (c) Handler protection
 - (d) Suspect apprehension
 - (e) Tracking
 - (f) Other purposes as determined by Department need.
2. Conduct research on prospective breeders/trainers to include:
 - (a) Demonstrations
 - (b) Performance
 - (c) Health
 - (d) Warranty
 - (e) Availability of on-going training

(f) Prior customer reviews

3. Provide a detailed report on prospective canines and the breeders/trainers examined including cost estimates.

B. Prospective canines will be evaluated by the Chief of Police, division commander the canine coordinator, and the canine handler based on cost, the specific needs of the Department and the overall characteristics of the canine. The final selection of a canine for the Department will be made by the Chief of Police.

III. Procedure: Canine Use

A. A trained canine officer and a police canine shall be considered a canine unit. A supervisor shall be assigned by the Chief of Police as the canine coordinator to administer and oversee the canine unit(s) for the Department. Canine unit(s) shall be operated within the Patrol Division and be subject to the Patrol Division chain of command.

B. Based on a canine's certification to perform various tasks, subject to availability and within the restrictions of this policy, the canine unit shall respond on a 24-hour on-call basis to conduct building searches for offenders in hiding, assist in the arrest or prevent the escape of serious or violent offenders, protect officers or others from death or serious injury, track suspects, locate lost or missing persons, locate hidden evidence of a crime, detect the presence of concealed narcotics, and assist in community policing efforts.

C. The canine officer is responsible for determining if a situation justifies canine use and the appropriate tactical measures to be taken based on his/her knowledge, training, and experience. When an on-scene supervisor with the Department disagrees with the handler's assessment, the direction of the supervisor shall be followed as stated in Chapter 2 Section 12.1.3 (Lawful Orders) of the Operations Manual.

D. When the canine unit is assisting another agency, the canine officer shall have the discretion to determine whether a situation justifies canine use. If assistance is denied, the canine officer will give an explanation to the requesting agency, preferably a supervisor.

E. Requests for canine unit assistance shall be handled as follows:

1. When the canine unit is working a normal patrol shift, departmental and outside agency requests for canine assistance shall be approved by the patrol shift supervisor with consideration for manpower.
2. When the canine unit is off-duty, requests for assistance shall be directed to and approved by an on-duty supervisor. Availability to respond to incidents while off-duty shall be at the discretion of the canine officer.
3. On-duty supervisors receiving requests for canine assistance shall notify the canine coordinator of any requests for assistance and the disposition of the request as a means of maintaining accurate records of the canine unit's use. This will normally be accomplished by email at the supervisor's earliest convenience. The canine coordinator shall

review all requests for canine assistance to determine if the canine team is appropriately responding to requests for assistance.

- F. When requests for assistance are received, communication center personnel shall forward essential information concerning the incident to the on-duty supervisor and the canine officer. The following information shall be obtained by communications when receiving a request to utilize the canine unit:
 - 1. Type of call.
 - 2. Location of call.
 - 3. Terrain (building or field).
 - 4. Weather conditions at scene.
 - 5. Security of the scene.
- G. Each canine shall be assigned a unique identifying name for purposes of record keeping. The canine shall be referred to by name in any needed report.
- H. Recognizing the importance of identifying the canine as belonging to the Department, the canine shall be issued identification and a uniform badge. In situations where the wearing of the badge is impractical, the canine shall always wear identification stating the canine belongs to the Department.

IV. Procedure: Canine Officer

- A. The canine officer shall be considered a specialized assignment as established in Chapter 2 Section 11.5.1 of the Operations Manual. In addition to the minimum requirements established for application and selection to a specialized assignment, an officer must be able and willing to do the following:
 - 1. Be able (in conjunction with other family members) to care for and house the canine at the officer's residence with a secure outdoor area for the canine. The canine officer shall be responsible for 24 hour care and maintenance of the canine.
 - 2. Demonstrate a strong desire to work with the canine and the willingness to care for and train the animal.
 - 3. Possess the physical ability to train and deploy the canine.
 - 4. Annually, successfully complete a canine training/certification course and successfully meet all course requirements.
 - 5. Be available on a twenty four (24) hour on call status subject to canine unit availability.
 - 6. Promote the Department and the canine program through educational and public relations duties (e.g. school visits, talks to civic groups, demonstrations, etc.).

V. Procedure: Use of Force

- A. When trained for apprehension or handler protection, use of specially trained police canines for law enforcement responsibilities constitutes a real or implied use of force. Officers may only use the degree of force that reasonably appears necessary to apprehend or secure a suspect as governed by the Department's use of force policy stated in Chapter 1 Section 4.1.1 of the Operations Manual. In all instances where a canine is

deployed in a tactical situation, the incident and details shall be documented. Whenever a canine bites an individual, whether or not in the line of duty, the canine officer shall do the following:

1. Summon a supervisory officer to the scene.
 2. Examine the affected area to determine the seriousness of the bite or injury.
 3. Obtain medical treatment for the person. Medical personnel should examine the affected area regardless of the perceived seriousness of the bite or injury.
 4. If possible, take photographs of the affected area prior to and following medical treatment.
 5. Whenever it has been alleged the canine has bitten or otherwise injured an individual, a use of force report must be completed. The report must detail the circumstances surrounding the incident, the identity of the individual involved and any witnesses, the extent of the injuries, and the measures taken to respond to the incident.
- B.** When apprehending suspects or protecting the canine officer, the canine shall be commanded to disengage as soon as the subject is subdued or readily complies with officer direction to avoid or reduce the severity of an injury.
- C.** Police canines shall not be handled or given commands by anyone other than the assigned handler.

VI. Procedure: Training

- A.** A new police canine and handler shall undergo a pre-service training program as recommended by the selected breeder/trainer. Initial training shall include the canine and handler meeting the minimum certification standards in all applicable tasks as established by a reputable certifying organization. Initial training certification shall occur prior to being approved for use within the community.
- B.** Police canine unit(s) shall maintain at least annual certification of proficiency by a reputable certifying organization in areas of usage as determined by need. The Department shall fund certifying organization memberships for the canine officer and the police canine.
- C.** Police canine unit(s) shall undergo continuing training and education to maintain proficiency which shall include monthly in-service training tasks established by the canine coordinator.
- D.** Only trained police canine decoys, current or former police canine officers, and police canine trainers shall be utilized for training involving bite work. Individuals used for bite work meeting the above requirements must be currently employed by the Department, under a training contract with the Department, working with a credentialing association utilized by the Department, or working for a law enforcement agency that routinely trains with the Department.
- E.** The Department shall enhance the effectiveness of canine training and the reliability of court testimony by utilizing controlled substances in the training

process. The following procedures shall be utilized for the use of controlled substances as canine training aids:

1. All controlled substances used for canine training shall be obtained from the Drug Enforcement Administration (D.E.A.) Special Testing and Research Laboratory. The current D.E.A. procurement process will be followed. All documentation relating to the procurement shall be preserved to enable tracking at a later date.
2. All controlled substances obtained for canine training shall be stored in a dedicated safe in a secure locker when not in use for training. Only the canine officer, and the canine coordinator shall have access to the safe.
3. The canine officer will maintain a log of the controlled substances that will be stored in the dedicated safe. The log will document all chain of custody events concerning the use of the controlled substances.
4. In the event the training controlled substances become lost, stolen, damaged, spilled, or unusable, the canine handler will complete an interdepartmental memorandum explaining the incident. This report will be forwarded to the canine coordinator who will notify the Patrol Commander.
5. The canine coordinator shall conduct semiannual inspections of the training controlled substances. A report of the semiannual inspections will be submitted to the Patrol Commander and the Chief of Police on departmental memorandum. The report will include the weight and condition of each controlled substance and include reference to any occurrence of lost, stolen, damaged, spilled, or unusable substances since the last inspection.
6. Random inspections may also be undertaken by the canine coordinator, Patrol Commander, or the Chief of Police or designee.
7. Once a controlled substance is no longer usable for training, D.E.A. and departmental procedures for documenting controlled substance destruction shall be followed.
8. Any requests for the replacement controlled substances will follow the current D.E.A. procurement process.

VII. Procedure: Canine Usage

- A.** If the canine is trained to locate suspects in buildings or related structures where a search by officers would create an unnecessary risk, the search shall be governed by the following:
1. The building perimeter shall be secured.
 2. Whenever possible, the building's owner should be contacted to determine whether there may be tenants or others in the building and to ascertain the building's layout.
 3. When a canine building search is anticipated, a preliminary search by officers should not be conducted as this will interfere with the canine's ability to discriminate scents.
 4. The on-scene supervisor shall also take the following steps in preparation for the canine search:

- a. Evacuate all tenants, workers or others from the facility.
 - b. Request that all air-conditioning, heating or other air blowing systems be shut off so as not to interfere with the canine's scent capabilities.
5. Upon entrance to the building, all exits shall be secured, and communications limited to those of a tactical nature.
6. The canine may be unleashed during a building search unless there is an imminent risk of injury to innocent persons within the facility.
7. The canine shall not be used to search facilities that contain substances potentially harmful to the canine unless over-riding risks to human life is present.
8. Before commencing the search, the canine officer shall loudly announce and repeat the statement indicating there are police officers on the premises and a trained police canine will be released if the individual(s) does not surrender. A reasonable amount of time shall be allowed for the suspect to respond. This warning shall be repeated on each level of all multi-level structures.
9. When apprehending suspects in these or related circumstances, canines shall be commanded to disengage as soon as the suspect is subdued or readily complies with officer's direction.
10. Arrestees shall not be transported in the same vehicle with a police canine unless alternative transportation is not available and immediate transport is essential for safety or security reasons.
- B. If trained for handler protection or apprehension, canine teams may be used for crowd control as protection upon the approval of the watch commander during a riot or other major unauthorized gathering that cannot be controlled by other means. In these situations the canine shall:
 1. Be short leashed at all times unless no other means are available to protect an individual from serious injury.
 2. Not initiate any offense action, unless to guard against imminent loss of life or serious injury.
 3. Canine teams shall not be used for crowd control at peaceful demonstrations but may be on standby in a discrete location with the approval of the Patrol Commander or designee.
- C. Searches and exploratory sniffs using the police canine for controlled substances shall be conducted in accordance with departmental policy for searches as stated in Chapter 1 Section 1.2.4 of the Operations Manual and consistent with known case law governing the use of a canine for searches at the time the action was taken.
- D. The canine officer shall maintain records documenting the use and the proficiency of an individual canine. This documentation shall be readily available to officers and prosecutors who may utilize it when seeking warrants.
- E. Random exploratory sniffing of luggage, packages and other inanimate objects may be conducted in public facilities such as airports, train or bus

stations upon authorization from the Patrol Commander, shift supervisor, or canine coordinator.

1. When possible, exploratory sniffing in these facilities with the advance knowledge and consent of the appropriate manager.
 2. Exploratory sniffing shall be conducted without interference or annoyances to the public or interruption of facility operations.
- F.** Canine teams may be utilized to assist school districts during periodic searches of school lockers, desks and other facilities or spaces owned by the school. Such searches will be conducted after a formal request is made by the school district to the Department or in the interest of public safety. The search shall be conducted within the school district's policy and/or applicable search and seizure law related to the search.
- G.** Police canines are available to track missing persons, suspects, or to locate evidence that has been abandoned or hidden in a specific open area. Such searches require officers to do the following in preparation for a canine search:
1. When officers are pursuing suspects and contact with the suspect is lost, the officer shall immediately stop and pinpoint the location where the suspect was last seen.
 2. Officers shall shut off engines of vehicles in the area if possible.
 3. Officers shall avoid vehicle or foot movement in the area where the suspect or subjects were last seen.
- H.** Canines used for tracking persons should remain on a leash of sufficient length to provide a reasonable measure of safety to the subject of the search without compromising the canine's tracking abilities.
- I.** Canine teams trained should not be used to locate missing persons unless there is a reasonable suspicion of foul play or a belief that serious bodily harm or death will occur if the person is not located immediately. Where the use of a canine is deemed necessary, the risk of attack to the person shall be explained to the next of kin or the reporting party and their approval obtained prior to use of the canine.
- J.** If no other crime is involved, canine teams should not be used to apprehend anyone under the influence of alcohol, drugs, or the mentally disabled.
- K.** On scene supervisory personnel shall:
1. Secure the perimeter of the area to be searched.
 2. Secure the integrity of the area to be searched by keeping all personnel out of the area.
- L.** Police canines shall not be used for breeding, participation in shows, field trials or exhibitions, unless authorized by the Chief of Police or Patrol Commander.
- M.** When not at the residence of the handler and when outside of the police vehicle, police canines shall be on a leash unless actively training, performing a controlled demonstration, being deployed for an apprehension, or being deployed for handler protection.
- N.** Public demonstrations are an important part of the canine unit's function and requests will be fulfilled whenever possible. Demonstrations allow the

Department to show the effectiveness of the canine unit and how it can assist law enforcement as well as foster strong community relations. Demonstrations shall only be conducted in an environment that ensures the safety of all participants and bystanders.

VIII. Procedure: Canine Officer Incapacitation

A. The following guidelines shall be used by officers when a canine handler becomes incapacitated and the canine is not contained:

1. Officers shall follow the directions of the handler if still conscious.
2. If the handler loses consciousness, officers shall consider the following:
 - a. Avoid direct eye contact with the dog.
 - b. Don't excite the dog with loud noises or sudden movements.
 - c. Don't approach the handler, unless absolutely necessary, as the canine will be protective.
 - d. Locate the canine's reward toy, get the canine's attention with it and throw it into the caged area of the canine vehicle or other secure area. Once inside, secure the canine in this area.
 - e. If previous measures are not successful, protective clothing found in the canine vehicle coupled with loud noises and sudden movements will attract the canine's attention. When the canine engages the protective clothing, he may be dragged off to the waiting vehicle or other suitable area of confinement.

B. The canine will only be destroyed as a last resort and when human life is in jeopardy.

IX. Procedure: Equipment

A. Canine officers shall have a specially equipped vehicle intended for the purpose of transporting the canine. The canine officer shall use the vehicle to transport the canine to and from work or to other canine related duties.

B. Canine transport vehicles shall have a cage designed specifically for the transport of canines. The cage shall be of a design that gives the canine adequate room for extended periods of stay and constructed in a manner that safeguards the canine from injury. The cage shall protect the driver and other occupants of the vehicle from the canine and shall shield the canine from outside contact. The canine vehicle shall not be utilized to transport detainees

C. Canine transport vehicles shall be equipped with a temperature monitoring device that will alert the canine officer by an audible alert when the vehicle temperature exceeds safe levels. This system may also incorporate a remote controlled door opening system to allow rapid exit of the canine for emergency situations.

D. Canine officers shall be provided with the necessary equipment for work, care, and use of the canine. At a minimum this will include:

1. Water and food bowls
2. An indoor crate of proper size for the breed of canine assigned to the officer.

3. Walking and tracking leads
4. Collars and neck chains to include tracking harnesses, collars, and general duty choker chains.
5. Secure containers for narcotics used in training.
6. General purpose and hidden bite sleeves for use in bite training.
7. Reward "toys" for use in training.
8. Grooming equipment to include brushes, nail clippers, other tools, and supplies for maintaining the canine's appearance
9. When necessary, the Department shall have constructed an appropriate outdoor dog run at the canine officer's residence for containment of the canine. Any dog run utilized by the canine officer for securing the canine outside shall be approved by the canine coordinator and include a visual inspection. Any needed repairs or maintenance shall be provided by the Department. The canine officer shall be responsible for maintaining the outside dog run in a condition to prevent the escape of the police canine.
10. Other equipment may be provided as necessary.

E. All equipment provided to the canine officer shall be documented according to Chapter 2 Section 17.5.1 of the Operations Manual.

X. Procedure: Care of the Canine/Equipment:

- A. The canine officer shall be personally responsible for the daily care and feeding of their animal to include:
 1. Maintenance and cleaning of the kennel and yard area where the canine is housed.
 2. Provisions of food, water and general diet maintenance as prescribed by the veterinarian authorized by the Department.
 3. Grooming on a daily basis or more often as required by weather, working conditions, or other factors.
 4. Daily exercise (police canines are not permitted to run at-large).
 5. General medical attention and maintenance of health care records.
- B. The canine officer shall ensure the assigned patrol vehicle is properly maintained and secured when not being officially used. The patrol vehicle assigned cannot be utilized for personnel business under any conditions, unless authorized by a division commander or the Chief of Police.
- C. When the canine officer is unable to perform their duties due to illness, injury, or leave:
 1. Another officer may be assigned to temporarily care for the canine.
 2. The canine may be housed in a Department approved kennel.
- D. Teasing, agitating, or roughhousing with a police canine is strictly prohibited unless performed as part of the training exercise.
- E. Canine officers shall not permit others to have personal contact with the canine (e.g. petting, hugging, etc.). Professional grooming or veterinary care are permissible after notification the canine is a trained for handler protection and subject apprehension and if appropriate, precautions such as a muzzle are utilized.

- F. When shift minimums, call volume, etc. allow, as determined by the shift supervisor, one (1) hour of a canine officer's shift shall be allocated for accomplishment of the daily care tasks. During this hour, the canine officer will not be responsible for calls for service and will be allowed to go off-duty. If one hour of the canine officer's shift cannot be allocated to daily care tasks, the canine officer shall receive either one (1) hour compensatory time or one (1) hour of the canine officer's hourly rate of pay as compensation for the completion of the daily care tasks. The type of compensation to be received shall be determined by the Chief of Police.
- G. On days that the canine officer is not working a scheduled shift, the canine officer shall receive either one (1) hour compensatory time or one (1) hour of the canine officer's hourly rate of pay as compensation for the completion of the daily care tasks. The type of compensation to be received shall be determined by the Chief of Police.

XI. Procedure: Medical Care

- A. Non-emergency medical care shall be administered by a Department approved veterinarian(s).
- B. Department approved veterinarian(s), a designated emergency care center, or any acceptable source of care may be used to administer emergency care to the canine.

XII. Procedure: Reporting

- A. All training completed by police canine units shall be documented and readily available to the supervisors of the canine program. Copies of all training records shall be provided to the training coordinator for entry into department records.
- B. In addition to complying with the normal reporting requirements of the department, canine officers shall complete documentation of training and deployments within the designated canine software program utilized by the department. Records of activity shall be recorded in the canine software program prior to the end of the canine officer's tour of duty unless receiving permission to complete the reporting at a later specified time by the canine coordinator or the shift supervisor.
- C. The canine coordinator shall submit a quarterly report to the Patrol Division Commander and the Chief of Police. The report shall include but not be limited to the following:
 - 1. Number of canine deployments differentiating between self-deployments and requested deployments.
 - 2. Number of requests in which the canine officer was unavailable for deployment.
 - 3. Outcome of deployment activity.
 - 4. Detailed training summary.
- D. The canine coordinator shall also submit an annual review of all canine unit activity to the Patrol Commander and the Chief of Police.

XIII. Procedure: Retirement:

- A. The following criteria shall be used when determining whether a canine should be retired:

1. The canine has lost its innate interest in performing its duties.
 2. The canine is not able to meet or maintain certification in one or more areas.
 3. The canine has a medical problem that makes it incapable of performing its duties.
 4. The canine officer leaves the department and it is impractical for the canine to be reassigned.
 5. The Department is no longer able to supply the funding and support necessary to sustain the canine program.
- B.** When one or more of the above criteria are experienced by the canine, the canine officer, or the Department, the canine shall be recommended for retirement. Once retirement has been determined, a memorandum will be forwarded through the canine officer's chain of command to the Chief of Police for consideration and formal action.
- C.** Once retirement has been approved and proper paperwork has been completed, the canine officer may be granted ownership of the canine at the discretion of the Chief of Police.

Chapter 5: Law Enforcement Operations
Section 41: Patrol
Subsection 2: Operations



Policy/Procedure #: 1

Title: Use of Emergency Vehicle Equipment

CALEA Reference#: 41.2.1

I. POLICY: Use of Emergency Vehicle Equipment

A policy is established to guide officers in the use of emergency vehicle equipment to include emergency lights and siren. It is the purpose of this policy to ensure all officers adhere to statutory restrictions on the use of emergency equipment. Emergency vehicle equipment shall be utilized only in prescribed conditions and circumstances and in ways that minimize the risk of accidents and injuries to employees and the public.

II. Procedure: Authorized Use

- A.** An authorized emergency vehicle is a vehicle equipped with emergency warning devices as required by Iowa law and used for emergency response situations.
- B.** Emergency warning devices are lights, sirens, and other equipment placed in/on each Department emergency vehicle that emit audible and/or visual signals in order to warn others that law enforcement services are in the process of being delivered.
- C.** Requests for police service shall be considered non-emergency calls and responding officers shall not use emergency warning devices in the following situations:
 - 1. Calls for service the officer reasonably believes have no potential to result in death or serious bodily injury.
 - 2. Calls for service where no crime is actively occurring and a delay in response time will not hinder the investigation.
- D.** Requests for police services shall be considered emergency calls and the responding officers shall use emergency warning devices to include lights and siren in the following situations:
 - 1. Calls for service the officer reasonably believes have or may result in death or serious bodily injury.
 - 2. Calls for service where a crime is actively occurring and a delay in response time may hinder the investigation. In these instances,

officers must be reasonable in their response considering the seriousness of the crime in progress.

- E.** Authorized emergency vehicles utilizing emergency warning devices shall be authorized for the following types of emergency calls:
- 1.** Pursuit of a fleeing motorist.
 - 2.** Officer in trouble. When an officer is involved in a situation where help is needed, they must be aware that a non-specific or over-zealous request may result in an uncoordinated response by other officers. This may be a greater risk to life and property than the original incident. When able, officers shall minimize this potential hazard by giving the following information:
 - a.** Police unit number.
 - b.** Exact location.
 - c.** Reason for the request.
 - d.** Specify, "Emergency, Emergent or Help" if an emergency response is required, "Backup or Non-emergent" if routine.
 - e.** Number of units required to handle the situation.
 - f.** If possible, the officer making the request shall remain near the radio long enough to determine if the call has been received by the communication center. Additionally, the officer shall provide status reports to coordinate the efforts of arriving units, and to confirm that adequate assistance arrives.
 - g.** In all "officer in trouble" calls, the supervisor shall serve as the primary responding or backup unit unless another unit is closer. At their discretion, the supervisor may direct another or additional units to respond.
 - h.** Upon notification by the officer originating the call for assistance or by the supervisor the status of the request has changed to a non-emergency situation, all responding units shall terminate emergency vehicle response immediately.
 - 3.** Felony in progress involving an actual or threatened attack which the officer reasonably believes could or has resulted in death or serious bodily injury. When responding to burglary in progress or robbery in progress calls, officers shall use their vehicle's emergency warning equipment to expedite their response, but based on the type of call the officer may choose not to use the siren within the hearing range of the scene.
 - 4.** Assault in progress. Communication operators should make every effort to determine that such calls involve an actual physical assault in progress. The caller shall be kept on the phone line if possible to provide updates and information on the incident to assist responding police units.
 - 5.** Accidents, Fires, or EMS calls where human life may be in jeopardy.

6. Other calls for service the officer reasonably believes may result in death or serious bodily injury.
 7. The supervisor is responsible for monitoring response modes for calls for assistance and shall have the authority to upgrade or downgrade assigned response modes.
- F. In instances where an officer initiates the emergency warning devices in response to a sudden occurrence, the officer shall inform the communication center as soon as possible of the following:
1. The nature of the situation.
 2. The location and status of the officer.

III. Procedure: Use of Emergency Warning Devices While in Emergency Response Mode

- A. During an emergency response, emergency warning devices shall be activated to include lights and siren.
- B. Regardless of the call for service and the use of emergency warning devices to include lights and siren, an officer shall not operate an emergency vehicle in a reckless manner endangering themselves or the public. Reasonableness will be the standard utilized to determine if the response was appropriate based on the call for service.
- C. Emergency warning devices may be deactivated at a distance from the scene (to be determined by the officer) so as to not alert subjects to law enforcement proximity. When emergency warning devices are deactivated, the emergency vehicle operator shall comply with posted speed limits, obey all traffic control devices, signals, and proceed in a manner consistent with normal traffic flow.

IV. Procedure: Use of Emergency Warning Devices While Conducting Vehicle Stops

- A. Emergency warning devices shall be used to make adequate notice of intent to stop a motor vehicle and provide a safe environment for the stopping officer and the violator.
- B. Officers are allowed to use only emergency lights to conduct a traffic stop. If the vehicle the officer is attempting to stop does not immediately comply, the emergency siren shall be activated until compliance is gained.

V. Procedure: Discretionary Use of Emergency Equipment

- A. Officers may activate emergency warning devices when required to assist in handling any perceived emergency situation.
- B. In other than emergency situations, when expediency is required to effectively eliminate a potential hazard, officers may activate emergency warning devices to allow orderly and safe transit through heavily congested roadways. Examples of permissible use of emergency warning devices during non-emergency response situations include, but are not limited to:
 1. Using emergency lights to protect disabled motorists.

2. When necessary, using emergency lights and the police vehicle as a temporary protective barrier.
3. Intermittent use of the emergency lights and siren to transverse heavy traffic that is slowly moving or stopped in an attempt to reach an incident.

VI. Procedure: Traffic Signal Preemption

- A. Patrol vehicles equipped with traffic signal preemption devices may activate the devices at any time there is a legitimate law enforcement need to move through an intersection while responding to a call for service. Below are examples of when the preemption device may be utilized:
 1. All calls for service requiring the use of emergency lights and siren.
 2. Response to calls in which traffic congestion is prohibiting the responding unit from arriving on scene of an active incident (e.g. accident causing traffic to back up and preventing the officer from arriving at the accident and protecting the scene).
- B. Traffic signal preemption devices shall not be utilized as outlined below:
 1. To allow the officer mitigate traffic congestion to respond to calls for service that are non-emergency and not active. (e.g. responding to a theft that occurred 2 days ago and traffic is heavy due to rush hour).
 2. Use of the traffic signal preemption device does not alleviate the officer from using necessary caution when entering an intersection utilizing their emergency warning devices.

Chapter 5: Law Enforcement Operation

Section 41:

Subsection 2: Operations



Policy/Procedure #: 2
Title: Vehicle Pursuits
CALEA Reference#: 41.2.2, 41.2.3

I. Policy: Vehicle Pursuits

Vehicular pursuit of fleeing suspects can present a danger to the lives of the public, officers, and suspects involved. It is the responsibility of the Department to assist officers in the safe performance of their duties. To fulfill these obligations, it shall be the policy of the Urbandale Police Department to regulate the manner in which vehicle pursuits are undertaken and performed.

All personnel operating departmental vehicles shall exercise due regard for the safety of all persons. There are no tasks in the Department of such importance that they justify the reckless disregard of the safety of innocent persons. Officers shall always use reasonable force to apprehend a fleeing suspect.

II. Procedure: Definitions

- A.** Vehicular Pursuit: An attempt by an officer in an authorized emergency vehicle to apprehend a fleeing suspect who is actively attempting to elude the police.
- B.** Authorized Emergency Vehicle: A vehicle equipped with operable emergency equipment as designated by Iowa Code.
- C.** Primary Unit: The police unit which initiates a pursuit or any unit which assumes control of the pursuit.
- D.** Secondary Unit: Any police vehicle involved as a backup to the primary unit.

III. Procedure: Pursuit Decisions

- A.** Officers shall use the following as a guide in determining whether to initiate or continue a pursuit. The factors described below are a guide designed to assist officers and supervisors in their use of discretion. The degrees of risks are defined as follows:

1. Lower Risk
 - a. Marked vehicles
 - b. Straight roads, good surfaces, clear line of sight
 - c. Few intersections
 - d. Few or no pedestrians
 - e. Good weather
 - f. No hazardous maneuvers by violator
 - g. Speeds at or less than 20 mph over the posted speed limit
 - h. Officer is calm and in control
2. Moderate Risk:
 - a. Some intersecting streets
 - b. Light pedestrian traffic
 - c. Moderate traffic, little congestion
 - d. Speeds 20 mph greater than the posted speed limit
 - e. Officer generally calm, under control
 - f. Some hazardous, but not extreme, maneuvers by the violator(e.g., crossing center line to pass vehicles, sudden lane changes)
3. High Risk:
 - a. Frequent intersecting streets
 - b. Poor weather, slick streets, low visibility
 - c. Blind curves, intersections, narrow streets
 - d. Numerous pedestrians
 - e. Heavy, congested traffic
 - f. Speed twice the posted speed limit, or greater than 80 mph
 - g. Extremely hazardous maneuvers by the violator (e.g., driving against oncoming traffic, failing to stop for red lights)
 - h. Numerous vehicles in pursuit
 - i. Officer excited, not in full control of emotions
 - j. Special circumstances (e.g., school zones, hospitals, etc.)

IV. Procedure: Initiation of a Pursuit

- A. Any law enforcement officer in an authorized emergency vehicle may initiate a vehicle pursuit when the suspect exhibits the intention to avoid apprehension by refusing to stop when properly directed to do so. Pursuits may also be justified if the officer reasonably believes that the suspect, if allowed to flee, would present a danger to human life or cause serious injury. Reserve officers shall not be allowed to engage in a pursuit or any type of intervention technique.
- B. In deciding whether to initiate pursuit, the officer shall take into consideration the following:
 1. Road, weather, and environmental conditions.
 2. Population density and vehicular and pedestrian traffic.
 3. The relative performance capabilities of the pursuit vehicle, the vehicle being pursued, and the officer's abilities.
 4. The seriousness of the offense.
 5. Identification of the offender.
 6. The presence of other persons in the vehicle.

7. The probability of successful apprehension.
8. The type of vehicle the officer is operating.

V. Procedure: Pursuit Operations

- A. Upon engaging in a pursuit, the pursuing vehicle shall activate appropriate emergency lights and siren as required by Iowa law.
- B. Upon engaging in a vehicle pursuit, the officer shall notify communications of the location, direction, and speed of the pursuit, the description of the pursued vehicle and the initial purpose of the stop. Any officer involved in a pursuit as a primary or secondary unit shall specifically notify communications that they are in a pursuit. Verbiage such as “attempting to catch up to” shall not be acceptable.
- C. When engaged in a pursuit, officers shall not drive with reckless disregard for the safety of themselves and others.
- D. When the Department is involved in an intra-agency pursuit (within the city limits of Urbandale), there shall be no more than three (3) police vehicles actively involved in a pursuit. Pursuits shall consist of a primary unit and no more than two (2) additional (secondary) units. All other personnel shall stay clear of the pursuit unless they are instructed to participate by a supervisor. During inter-agency pursuits (pursuits that leave the city limits of Urbandale or were initiated outside of Urbandale) and units from other jurisdictions are involved, a total of four (4) police vehicles may be involved in the pursuit.
- E. The secondary unit’s responsibility is to relay information about the pursuit to other officers and dispatch. The secondary unit shall maintain a safe distance behind the primary unit to avoid a collision but close enough to render assistance when the pursued vehicle is stopped.
- F. The primary unit shall become a secondary unit when the fleeing vehicle comes under air surveillance or when another unit has been assigned primary responsibility.
- G. Only sport utility vehicles (SUV) that are pursuit rated shall be utilized in vehicle pursuits. All SUVs that are assigned to the patrol division for normal patrol duties shall be pursuit rated. If the primary officer in a pursuit is operating a non-pursuit rated sport utility vehicle (SUV), they will only pursue the suspect until another officer can take the primary position and the speeds do not exceed a safe level for operation of the SUV. When support units engage in the pursuit, the non-pursuit rated SUV shall disengage and terminate their involvement in the pursuit. If the non-pursuit rated SUV is operated by the supervisor, he/she may continue at a safe speed in the direction of the pursuit to its conclusion.
- H. No officers shall engage in a vehicle pursuit when they have a civilian passenger (reserve officers are not considered civilians). Options for the officer are to not pursue the suspect vehicle or drop the civilian passenger in a safe location prior to engaging in the pursuit. At the earliest convenience, the officer shall arrange for the civilian passenger to be picked up and transported to the police department.

VI. Procedure: Communication Responsibilities (Per WestCom Policy)

- A. Upon being advised by an officer they are in a vehicle pursuit, the dispatcher will activate one long alert tone, broadcast the officer is in a pursuit to all appropriate agencies on the main police operations channel, include any pertinent information provided by the officer, notify the officer in charge, and clear the channel for the pursuing officer.
- B. Direction of the pursuit may require use of alternate interoperable radio channels available on the console such as IA TAC radio channels.
- C. Special attention must be given to changes in direction of the pursuit and additional notifications made if necessary.
- D. The dispatcher handling the pursuit shall verbally announce the vehicle pursuit to the other dispatchers in the room.
- E. The dispatcher shall repeat all radio transmissions and record all information in the computer aided dispatch (CAD) incident.
- F. The pursuit will not be switched to an alternate radio channel but can be patched to an additional radio channel as necessary.
- G. In order to establish communications with agencies that may assist with the vehicle pursuit:
 - 1. All appropriate radio channels will be multi-selected and the dispatcher will repeat and relay all pertinent information on the selected channels.
 - 2. If it becomes necessary to connect VHF radio channels with 800 MHz channels, the dispatcher may patch the frequencies from the dispatch radio console. Delays associated with the radio patch can cause transmissions to be cut off. Officers shall be aware that they will need to wait a few seconds after keying up their radio before talking.
 - 3. The ISICS radio channels will be utilized.
- H. Should the officer in charge advise to terminate the pursuit, the dispatcher shall immediately re-broadcast that information and ensure that the pursuing officer(s) acknowledge the information.
- I. Agencies that had been notified of the incident will be re-contacted with any updated information.
- J. When the pursuit ends or is terminated, another broadcast on the police main operations channel and any additional radio channels being used will be completed stating the location where the pursuit ended and reason for termination.

VII. Procedure: Supervisor Responsibilities

- A. During a pursuit, the supervisor shall monitor incoming information, coordinate and direct activities as needed to ensure that proper procedures are followed.
- B. Supervisors shall have the discretion to terminate any pursuit.
- C. When possible, the supervisor shall give the approval for the use of force to end a pursuit.
- D. When possible, a supervisor shall respond to the location where a vehicle has been stopped following a pursuit.
- E. Supervisors actively involved in a vehicle pursuit shall relinquish to another marked unit as soon as possible.

VIII. Procedure: Pursuit Tactics

- A. Unless authorized by a supervisor, officers shall not follow or attempt to intercept the pursuit on adjacent streets. When authorized by a supervisor, the officer(s) must be able to intercept the pursuit utilizing safe emergency vehicle operations and speeds.
- B. Officers must be operating an authorized emergency vehicles to pursue a fleeing vehicle. Vehicles fully equipped for use within the Patrol Division and utilizing required emergency lights and siren per the Iowa Code shall be used to pursue fleeing vehicles. When a pursuit is initiated by an officer operating an authorized emergency vehicle other than a fully equipped patrol vehicle (e.g. an Investigation Division or Support Services Division vehicle), the officer shall disengage as the primary and/or secondary unit as soon as other fully equipped patrol units are available.
- C. All intervention tactics short of deadly force, such as spike strips and low speed channeling (with appropriate advance warning) shall be used when it is possible to do so safely and when the officers utilizing them have received appropriate training in their use.
- D. The decisions to discharge firearm(s) at or from a moving vehicle is strictly governed by the Department's use of force policy and is prohibited if it presents an unreasonable risk to others.
- E. Once the pursued vehicle is stopped, officers shall utilize appropriate officer safety tactics and shall be aware of the necessity to utilize only reasonable and necessary force to take suspects into custody.
- F. In the event a pursued vehicle travels the wrong way on a fully controlled access roadway such as an interstate, freeway, or bypass, officers shall not follow. In the event a pursued vehicle travels the wrong way on a divided roadway or one way street, officers shall use extreme caution in their decision to follow as dictated by the circumstances of the pursuit. This does not prohibit officers from continuing the pursuit on an adjacent roadway where the officer is traveling with the flow of traffic.

IX. Procedure: Termination of the Pursuit

- A. All pursuing units and the supervisor shall continually re-evaluate and assess the pursuit situation including all of the initiating factors and terminate the pursuit whenever they reasonably believe the risks associated with the continued pursuit are greater than the public safety benefit of making an immediate apprehension.
- B. Pursuing unit(s) may terminate a pursuit at any time. If a pursuit is terminated for any reason, the pursuing unit(s) shall give communications the location where the pursuit was terminated. The officer(s) involved in the pursuit shall state to communications "I am terminating the pursuit." Other verbiage is not acceptable. If other units are involved in the pursuit when terminated by the primary unit, they must seek supervisory approval to continue the pursuit or to re-engage in the pursuit.
- C. The supervisor may order the termination of a pursuit at any time and shall also state "terminate the pursuit." Other verbiage is not acceptable.

- D. A pursuit shall be terminated when the suspect's identity can be determined and immediate apprehension is not necessary to protect the public or officers.

X. Procedure: Inter-Jurisdictional Pursuits

- A. An inter-jurisdictional pursuit is a pursuit that is initiated by an Urbandale officer and crosses into another jurisdiction or a pursuit initiated by an outside jurisdiction and crosses into Urbandale. The agency initiating the pursuit shall remain the primary unit and retain command and control over the pursuit. Under normal circumstances, the role of the jurisdiction being entered shall be a support role (e.g. traffic control, stop sticks). When a pursuit is initiated by another agency, officers shall obtain supervisory approval to become actively engaged in the pursuit as the second or subsequent pursuing officer. Only under the most extreme circumstances and only by supervisory approval shall the Urbandale Police Department take command and control or become the primary unit of a pursuit initiated by another agency.
- B. Dispatch for the jurisdiction being entered will be notified immediately and a description of known charges will be given.
- C. The agency initiating the pursuit shall ensure the jurisdiction being entered is able to monitor radio communications.
- D. The jurisdiction being entered has the option to participate in the pursuit or not participate. Urbandale officers and supervisors may terminate their participation in an inter-jurisdictional pursuit at any time. Communications shall be immediately notified of termination by any unit per the requirements of this policy.
- E. The pursuit policy of each law enforcement agency will be adhered to by their employees regardless of where the pursuit takes place.
- F. No more than four (4) vehicles shall be directly involved in an inter-agency pursuit regardless of the number of agencies involved. If a supervisor becomes aware that more than four (4) police vehicles are actively involved in a pursuit, they shall immediately terminate active participation by Urbandale police units until the total number of police units is four (4). An exception to limiting the Urbandale units may be made by the supervisor if the only Urbandale police unit involved in the pursuit is currently acting as the primary unit. Officers shall also recognize the need to limit the number of pursuing vehicles to four (4). Unless they are the primary unit, officers shall terminate any active involvement if they become aware that the total number of police vehicles involved in the pursuit is more than four (4). Communications shall be immediately notified of termination by any unit per the requirements of this policy.

XI. Procedure: Reporting

- A. In addition to a detailed incident report and any other needed paperwork, an officer actively participating or assisting (traffic control, stop sticks, etc.) in a pursuit shall file a written report on the post pursuit form detailing the circumstances. This report shall be reviewed by the immediate supervisor of the officer(s) involved, the division commander, the internal affairs

administrator, and the Chief of Police. All levels of review shall determine compliance to policy. Any supervisor reviewing a post pursuit report may recommend discipline for failure to follow policy. The Chief of Police shall make the final determination on disciplinary action.

- B.** Officers shall mark for retention within the in-car and body worn recording systems all video and audio recordings related to a pursuit. The details of how the video/audio was marked in the system shall be included by the officer in the post pursuit review form for easy identification of the files by reviewing supervisors. If deemed necessary for the review, the division commander or designee of the officer(s) involved in the pursuit shall be responsible for obtaining any recordings of the incident from communications and submitting a copy with the post pursuit review.
- C.** Any time an officer is involved in a pursuit, the officer's direct supervisor at the time of the incident shall review all aspects of the incident to identify training needs, violation of policy, proper performance, etc. This shall include a review of all video and audio recordings. The review shall be documented on the post pursuit report.
- D.** The division commander shall be responsible for viewing all video and audio recordings of the pursuit to determine if policy and procedure were followed by the officer and the supervisor. If deemed necessary, the review shall include any recordings or post incident review of the incident from communications. Any deviation from policy observed in the video and audio recordings or the post incident review from communications shall be noted in the post pursuit review. The Internal Affairs Administrator and the Chief of Police may also review the video/audio recordings and communications post incident review as needed.
- E.** Once the review on the post pursuit form has been completed by all parties, the division commander or designee shall request a post pursuit review meeting. The meeting shall be scheduled by the division commander or designee and attended as determined by the division commander or designee. The purpose of the meeting will be to review the pursuit and any issues noted in the post pursuit review form. The meeting contents will be documented by the division commander or designee on the post pursuit review form. The Chief of Police may also request a post pursuit review meeting at any time.
- F.** The division commander or designee shall also notify a WestCom supervisor of any communication concerns or issues discovered during the review process.
- G.** The Patrol Division Commander shall conduct a documented annual analysis of police pursuit activity to identify any patterns or trends which may forecast or indicate pursuit policy effectiveness, training needs, equipment upgrades, and/or policy and procedure modifications.
- H.** The Patrol Division Commander shall submit an annual review of the vehicle pursuit policy, procedures, and reporting to the Chief of Police.

XII. Procedure: Training

- A. Officers shall receive initial training in the Department's pursuit policy as part of the Department's Field Training Program.
- B. Officers shall receive biennial training in Department approved intervention tactics, and safe driving tactics. This shall include instruction from qualified instructors on the use of road spikes.
- C. All sworn officers shall be required to review the Department's pursuit policy annually.

XIII. Procedure: Roadblock and Pursuit Intervention Technique (PIT)

- A. A roadblock is the forcible stopping of a pursued vehicle by establishing a barrier that allows no outlet. Allowing no outlet for a pursued vehicle is extremely dangerous for the occupant(s) of the pursued vehicle and the officers establishing the roadblock as it often results in a collision. Roadblocks as defined in this policy shall be prohibited.
- B. Pursuit Intervention Technique (PIT) is the forcible stopping of a vehicle by causing the vehicle to spin by initiating contact with the rear of the vehicle. PIT as defined in this policy shall be prohibited.

XIV. Procedure: Channeling

- A. Channeling is the positioning of a patrol car to direct a pursued vehicle to a specific location or direction of travel. An example of channeling would be to direct a pursued vehicle to an open highway from a residential street or directing a pursued vehicle to a specific lane in the roadway as part of deploying a road spike device.
- B. When channeling is utilized, the driver of the pursued vehicle must be allowed ample time to react to the channeling as opposed to striking another vehicle or object. Officers shall not attempt to channel a vehicle being operated at high speeds.
- C. Channeling shall only be attempted with marked patrol vehicles utilizing all available emergency lights. When attempting to channel a pursued vehicle, officers shall remain inside of their vehicle for protection.
- D. Unless time does not allow, officers shall receive supervisor approval before attempting to channel any pursued vehicle.

XV. Procedure: ROAD SPIKE DEVICES (STOP STICKS)

- A. Road spikes come in various shapes and sizes and are all designed to work in the same manner. They are placed across the road way when officers are attempting to end a pursuit and are designed to break the spikes off in the tires of the pursued vehicle. It is an effective tool designed to disable a vehicle by deflating the tires at a controlled rate of deflation resulting in a safe and effective immobilization of the vehicle.
- B. When possible, road spike devices shall be used in conjunction with a stationary patrol vehicle in an attempt to slow down the suspect vehicle prior to striking the road spike device. The stationary patrol vehicle shall not restrict the suspect vehicle's path as this will likely cause a collision with the patrol vehicle.
- C. Officers will broadcast to pursuing vehicles over the radio their intent to use and the location of the road spike device.
- D. Road spikes shall NOT be used for attempting to stop a motorcycle.

- E.** Road spikes shall NOT be used in locations where specific geographic configurations increase the risk of injury to any person.
- F.** When able, oncoming traffic on a two-way road shall be stopped at a reasonable distance from the deployment site to avoid having uninvolved motorists affected by the strips. Traffic on Interstate 80/35 shall not be stopped for the deployment of road spikes.
- G.** Officers shall consider the amount of traffic on the roadway and the likelihood of uninvolved vehicles being damaged. If there is a strong possibility uninvolved vehicles will be damaged, the road spikes shall not be deployed. This is especially relevant on Interstate 80/35. When high volumes of traffic are present on Interstate 80/35, road spike shall not be deployed.
- H.** Due to limitations of the road spike device, deployment across four or more lanes of traffic is not advised and alternate methods of deployment should be considered.
- I.** When deploying the road spikes, officers shall stand at a safe distance from the deployment site to avoid injury from the road spikes and the suspect vehicle after they are struck by the suspect vehicle. A stationary patrol car will not offer protection to an officer if struck by another vehicle at high speed. At no time shall an officer stand in the roadway to deploy road spikes.
- J.** Officers shall use extreme caution when deploying road spike devices as suspects are known to swerve to avoid the device. Swerving by the suspect places the officer in danger of being struck. A stationary patrol car will not offer protection to an officer if struck by another vehicle at high speed.
- K.** If damage is done to an uninvolved vehicle by a deployed road spike device, officers shall provide the motorist a business card with the case number and advise them to contact the division commander. The damage shall be documented by photographs and/or memorandum to the division commander. When appropriate, the division commander shall facilitate repair of the damage with the motorist through City administration and the City's insurance carrier.

Chapter 5: Law Enforcement Operations
Section 41: Patrol
Subsection 2: Operations



Policy/Procedure #: 4

Title: First Responder Notifications

CALEA Reference#: 41.2.4

I. Policy: Notifications

A policy is established to notify the appropriate agencies when confronted with the need to respond with services outside the department's control.

II. Procedure: Notifications

- A.** The medical examiner shall be notified of all unattended deaths within the City of Urbandale.
- B.** Public works or the Iowa Department of Transportation shall be notified of any road hazard which the officer is unable to immediately correct.
- C.** When a problem or disruption with a utility providing vital public services such as electricity, natural gas, or phone service is discovered, the appropriate agency shall be notified.
- D.** When an officer encounters a fire or medical situation, they shall immediately notify Urbandale Fire Department.
- E.** Communications personnel shall assist in making the above notifications when directed by an officer.
- F.** This policy shall not prevent officers and supervisors from making appropriate notifications according to other sections in the Operations Manual.

III. Procedure: Police Hazards

- A.** A police hazard is any situation, person, property, or place that may create or contribute to an incident requiring law enforcement intervention.
- B.** Hazards which may be encountered by police officers can be permanent or temporary and may vary hourly, daily, or seasonally.
- C.** Information on hazards identified shall be disseminated at roll call, via radio communications, or by any on-duty supervisor as the need arises.
- D.** Intelligence bulletins shall be disseminated on a regular basis to provide department members information about specific activities and potential hazardous situations concerning persons that may be encountered.

- E. Severe weather bulletins shall be received at the communications center and relayed to on-duty shift members.

IV. Procedure: Hazardous Highway Conditions

- A. During normal patrol activities, officers must remain alert for unsafe or hazardous conditions on or near roadways.
- B. When a hazard presents an immediate danger to public safety, the officer shall notify communications who will notify the responsible agency to correct the problem as soon as possible. When roadway hazards are such that there is an immediate danger to the motoring public, officers shall initiate appropriate corrective action whenever practical to remove the hazard, or take action to protect the hazard until corrective action can be taken by the appropriate agency.
- C. When the hazard requires corrective action that is not an imminent danger (e.g. median marker sign down), the officer shall have communications notify the responsible agency when convenient.

V. Procedure: Hazardous Materials

- A. A hazardous substance is any substance or mixture of substances that presents a danger to public health or safety and includes, but is not limited to, a substance that is toxic, corrosive, flammable, infectious, a strong sensitizer, or is an irritant or generates pressure through decomposition, heat, or other means. This may include hazardous waste or material as identified or listed under the United States Solid Waste Disposal Act, Water Pollution Control Act, or Hazardous Materials Transportation Act.
- B. A hazardous condition is a situation involving the actual, imminent, or probable spillage, leakage, or release of a hazardous substance onto the land, or into the water or atmosphere, which creates an immediate or potential danger to public health or safety or to the environment.
- C. Upon notification or discovery of a hazardous condition, Urbandale Fire Department and the Iowa Department of Natural Resources will be immediately notified.
- D. In the event of a motor vehicle accident involving the transportation of a hazardous material upon a public highway that results in a spill or breach of the container(s), the Urbandale Fire Department and the Iowa Department of Transportation shall be notified as soon as practical.

Chapter 5: Law Enforcement Operations
Section 41: Patrol
Subsection 2: Operations



Policy/Procedure #: 5

Title: Missing Persons

CALEA Reference#: 41.2.5, 41.2.6

I. Policy: Missing Persons

It shall be the policy of the Urbandale Police Department to thoroughly investigate all reports of missing persons. Additionally, The Department holds that every person reported as missing will be considered “at risk” until significant information to the contrary is confirmed.

Jurisdictional conflicts are to be avoided when a person is reported missing. If a missing person either resides in, or was last seen in the City of Urbandale, the Department will immediately initiate the required reporting process. If a missing person has an established residence in Urbandale and was last seen in another jurisdiction but the law-enforcement agency covering that jurisdiction chooses not to take a missing-person report, the Department will assume reporting and investigative responsibility. Reporting and investigative responsibility will occur only after the Department has confirmed with a supervisor from the law enforcement agency having jurisdiction they will not be taking a missing person report.

Questions concerning parental custody occasionally arise in relation to missing-child reports. It shall be the policy of the Urbandale Police Department to accept the report of a missing child even if custody has not been formally established. Reporting parties shall be encouraged to obtain legal custody as soon as possible; however, since the safety of the missing child is paramount, members of the Department will open a case when it can be shown the child is missing, without explanation, from his or her usual place of residence.

II. Procedure: Definitions

A. The term missing adult refers to a person who is:

1. 18 years of age or older.

2. The person's absence is contrary to his or her normal patterns of behavior and may be due to one or more of the unusual circumstances listed below.
- B.** The term missing child refers to a person who is:
1. Younger than 18 years of age.
 2. The child's whereabouts are unknown to his or her parent, guardian, or responsible party.
- C.** A missing adult or child will be considered "at-risk" when one or more of the unusual circumstances noted below are present.
- D.** The term unusual circumstances refer to:
1. A missing child 13 years of age or younger. This age was established by the federal Missing Children Assistance Act because children of this age group have not established independence from parental control and do not have the survival skills necessary to protect themselves from exploitation.
 2. A child or an adult who is missing and believed to be one or more of the items noted below:
 - a. Out of the zone of safety for his or her age and physical and mental condition. The zone of safety will vary depending on age. In the case of an infant, for example, the zone of safety will include the immediate presence of an adult custodian or the crib, stroller, or carriage in which the infant was placed. For a school-aged child the zone of safety might be the immediate neighborhood or route taken between home and school. In the case of an elderly person of diminished physical and/or mental health, the zone of safety might include the close proximity and availability of a caregiver familiar with the individual's condition and needs.
 - b. Mentally diminished. If the person is developmentally disabled or emotionally disturbed, or the victim of disease, he or she may have difficulty communicating with others about needs, identity, or address.
 - c. Drug dependent. In the case of a child, the term "drug dependent" shall refer to dependence on either prescription or illicit substances, since any drug dependency puts a child at substantially increased risk. In the case of an adult, the term "drug dependent" shall refer to a dependence on legally prescribed medicines vital to the adult's continued physical well-being. This in no way limits an officer's discretion in determining exigent circumstances regarding an adult's use of illicit drugs.
 - d. A potential victim of foul play or sexual exploitation.
 - e. In a life-threatening situation. The environment in which the person is missing may be particularly hazardous. Examples of a dangerous environment could be a busy highway for a toddler, an all-night truck stop for a teenager, or an outdoor environment in inclement weather for a child of any age or elderly missing person.

- f. Absent from home for more than 24 hours before being reported to law enforcement as missing. While some persons may incorrectly assume 24 hours must pass before law enforcement will accept a missing-person case, a delay in reporting might also indicate the existence of neglect or abuse within the family.
- g. Believed to be with persons who could endanger his or her welfare.
- h. Is absent under circumstances inconsistent with established patterns of behavior. Most children and adults to some degree have established routines that are reasonably predictable. Significant, unexplained deviations from those routines increase the probability the person may be at risk. A child or adult whose disappearance involves circumstances that would cause a reasonable person to conclude the missing person should be considered at risk.

III. Procedure: Action to be taken

- A. If it is determined unusual circumstances are involved in the report of a missing adult or child, the person will be considered at-risk, and an expanded investigation, including the use of all appropriate resources, will immediately commence. While all missing-person incidents shall be thoroughly investigated, those involving unusual circumstances indicate a heightened likelihood of risk to the person and therefore, require an intensive response.
- B. If appropriate, response protocols including the AMBER Alert system and/or other immediate community notification methods shall be activated.

IV. Procedure: Communications

- A. WestCom personnel receiving the report of a missing person shall determine if circumstances of the report meet the definition of a missing child or adult. By questioning the caller about the circumstances of the report, WestCom can make a preliminary assessment about the level of risk to the missing person.
- B. Promptly dispatch an officer to the scene of the report. The handling of missing-person reports over the telephone is discouraged since accurate assessments of risk to the person cannot be made.
 - 1. The National Child Search Assistance Act of 1990 mandates law enforcement's immediate response to reports of missing children and the prompt entry of descriptive information into the Federal Bureau of Investigation's (FBI) National Crime Information Center (NCIC) Missing Person File.
 - 2. The PROTECT Act of 2003 amended the National Child Search Assistance Act to extend the same NCIC reporting responsibility and other benefits to young adults, 18, 19, and 20 years of age.
- C. Due to the complexity of some missing-person cases, especially those that may require the immediate mobilization of investigative resources, WestCom shall verify a supervisor has been notified whenever

officers respond to a missing person report where unusual circumstances as defined above are determined to exist.

- D. Transmit the appropriate radio alerts and other notifications. A critical responsibility of WestCom is to obtain sufficient information from the reporting party to broadcast a radio message that alerts other officers about the circumstances of the person's disappearance. Information should include the person's height, weight, hair and eye color, and clothing, as well as the location where last seen. The radio alert shall contain any information known about a possible abductor with special emphasis on the description of the suspect and vehicle used as well as direction of travel.
- E. Search agency records for related information. It is essential for responding officers to know if the person or family has been the subject of previous reports that might have a bearing on this incident. If possible, records shall also be reviewed to learn if any incidents have been reported in proximate time or location to this incident that might have investigative value in this case. Complaints such as attempted abductions, prowlers, public lewdness, and suspicious persons will be of particular interest.
- F. WestCom shall be prepared to immediately activate the appropriate immediate, community-notification method if so directed by appropriate law-enforcement personnel.
- G. Upon an officer's request, immediately enter the missing person into the National Crime Information Center (NCIC).
- H. Once the missing person is located, remove the entry from NCIC.

V. Procedure: Response

- A. The initial officer assigned to the report of a missing person shall:
 - 1. Respond promptly to the scene of the report. Even if the assigned officer has been provided with initial information such as the missing person's description and other facts about the incident, it would be inappropriate to delay response to conduct a random search or stop suspicious individuals. Unless in immediate response to the missing person's safety, these activities can be handled by other patrol units.
 - 2. Interview the person(s) who made the initial report. The purpose of the interview is to gain insight into the circumstances surrounding the disappearance and other information needed to conduct an initial assessment of the case.
 - 3. Obtain a description of the missing person. The collection of information about the missing person, including race, height, weight, hair and eye color, clothing, and other noteworthy features, shall be done promptly and relayed to other officers who may be assisting in the investigation. Recent photographs and/or videotape shall be secured if available.
 - 4. Verify the person is in fact missing. In the case of children, first responders shall never assume searches conducted by distraught parents or others have been performed in a thorough manner. Another check of the house and grounds shall be made to include places where

children could be trapped, asleep, or hiding. Special attention shall be paid to enclosures like refrigerators, freezers, and the interior of parked vehicles where limited breathing air may place the child at even greater risk. In the case of older children, first responders shall ask if parents have checked with the child's friends or perhaps overlooked or forgotten something the child may have said that would explain the absence. Note: A search of the home shall be conducted even if the missing person was last seen elsewhere.

5. Confirm custody status. First responders shall ascertain whether a dispute over the child's custody might have played a role in the disappearance. Questions regarding whether the reporting party has full legal custody, if the noncustodial parent has been contesting custody, or if the missing child expressed a wish to live with the other parent, may help an officer gain important insight into the case.
6. Identify the circumstances of the disappearance. Officers need to ascertain whether the circumstances surrounding a person's disappearance are such a heightened level of response is warranted. If "unusual circumstances" exist, as defined above, then the decision to employ additional response methods is clear. In other situations where the circumstances are not clear, officers shall keep the missing person's safety in mind and act accordingly.
7. Determine when, where, and by whom the missing person was last seen. This information is needed to determine factors such as abduction time frame, window of opportunity, and verification of previously received information.
8. Interview the individual(s) who last had contact with the missing person. Effective questioning of those individuals who last saw or spoke with a missing person is crucial in the case-assessment process. While seeking information about the person's appearance, demeanor, and actions, officers shall also be alert to contradictions or evasiveness by the witness, especially if these statements cannot be readily substantiated.
9. Identify the missing person's zone of safety for his or her age and physical and mental state. Responding officers shall attempt to determine how far the missing person could travel from the location where last seen before he or she would most likely be at risk of injury or exploitation. This perimeter shall, under many circumstances, define the first search zone or the community notification zone.
10. Make an initial determination of the type of incident. If unusual circumstances exist, officers shall immediately notify their supervisor. Note: Officers must be cautious in "labeling" or classifying a missing-person case, since the classification process shall affect the way in which initial information or evidence is gathered. Even if first indications suggest a less urgent incident, officers shall consider all possibilities until the case category is clearly determined.

- 11.** Obtain a description of the suspected abductor(s) and other pertinent information. If the abduction scene involves a business or other public place, officers may be able to supplement witness information with video from security cameras that might provide crucial information about the suspect, vehicles, and circumstances. In the case of a suspected family abduction, the reporting party may have photographs of the abductor or other valuable information.
- 12.** Evaluate whether circumstances of the child's disappearance meet existing AMBER Alert and/or other immediate community notification protocols. Discuss plan activation with supervisor. The decision to activate an AMBER Alert or other community notification shall be made by a supervisor.
- 13.** Determine the correct NCIC Missing Person File category and ensure a notification is promptly transmitted. There are eight (8) categories within the Missing Person File. They are disability, endangered, involuntary, juvenile, familial abduction, lost or wandered away, catastrophe, and other missing adult. In the case of a missing child, simply because the child is younger than 18 does not require the juvenile category must be used. The circumstances of the disappearance shall govern category selection.
- 14.** Provide detailed descriptive information to WestCom for broadcast updates. As information becomes available regarding the missing person's physical appearance, circumstances of the case, or description of the potential abductor, the initial officer shall ensure other officers and agencies are provided with up-to-date facts.
- 15.** Identify and interview everyone at the scene. The name, address, home and work telephone numbers of everyone present at the scene, along with his or her relationship to the missing person, shall be recorded. If possible, include them in photographs and/or videotapes of the incident scene. By interviewing each person privately, officers may be able to uncover information that is instrumental in resolution of the case.
- 16.** Conduct a thorough search of the scene. With the assistance of additional personnel, a systematic, thorough search of the incident scene shall be conducted. If appropriate, officers shall obtain written permission to search houses, apartments, outbuildings, vehicles, and other property that might hold information about the person's disappearance. When possible officers shall also search a missing child's school locker as well as any computer or electronic messaging systems to which a child has access. Searchers shall also be alert for any surveillance or security cameras in the vicinity that may have captured information about the person's disappearance.
- 17.** Secure and safeguard the area as a potential crime scene. If unusual circumstances exist, first responders must take control of the immediate area where the incident occurred and establish an appropriate perimeter to avoid destruction of vital evidence. In addition

to external crime scenes, the missing person's home, and particularly his or her bedroom, shall be secured and protected until evidence and identification material such as hair and fingerprints are collected.

B. The supervisor assigned to the report of a missing person shall:

1. Obtain a briefing from the first responder(s) and other agency personnel at the scene. This briefing allows the supervisor to determine the scope and complexity of the case and develop an appropriate response. The briefing shall be conducted away from family, friends, or any other individuals who may be present.
2. Determine if additional personnel and resources are needed to assist in the investigation. Depending on the situation, a supervisor may determine additional personnel, including specialized units, should be called to the scene or otherwise assist in the investigation. It is the supervisor's responsibility to ensure the investigation Division has been notified and are responding to the correct location.
3. Consider activation of the AMBER Alert system and/or other immediate community notification methods. If circumstances indicate the chances for the child's safe recovery would be increased by immediate public awareness, a supervisor shall promptly implement such efforts.
4. Establish a command post if needed. As a general rule the command post shall be close enough to the center of activity to facilitate control and coordination, but sufficiently apart to allow a free exchange of ideas among responders. Using the victim's home as a command post is not recommended.
5. Organize and coordinate search efforts. A supervisor may appoint a search operation coordinator who can oversee the search effort while the supervisor remains available to manage the entire investigation.
6. Establish a liaison with the victim family. Families of a missing person will experience extreme stress. Supervisors shall establish a liaison with the victim family who can explain what investigative actions are being employed and what they can do to assist in the search.
7. Enlist the assistance of the Department's public information officer to assist with the media. Many missing-person investigations, especially those involving large-scale search efforts, are likely to draw media attention.

C. The investigator assigned to the report of a missing person shall:

1. Obtain a briefing from agency personnel at the scene. This briefing shall be conducted prior to interviews with family members of the missing person or witnesses who may have been identified during the initial stage of the case.
2. Verify the accuracy of all descriptive information. The verification process shall include all details developed during the preliminary investigation. During the interview process the investigator shall be alert to facts or statements that conflict with those gathered by the first responder.

3. Initiate a neighborhood investigation if appropriate. A thorough canvass of the neighborhood shall be conducted without delay. A record shall also be made of all vehicles parked within the neighborhood and any other conditions that may have future investigative value. Access shall also be made to the Sex Offender Registration list to determine if individuals designated as sexual predators reside, work, or might otherwise be associated with the area.
4. Obtain a brief history of recent family dynamics. Information about family dynamics, obtained from police reports, family members, neighbors, teachers, classmates, employers, coworkers, friends, and witnesses, can offer valuable insights into what may have happened to the missing person and where he or she may be found.
5. Evaluate the need for additional resources and specialized services. The complexity of many missing-person incidents may necessitate the use of resources and services both from within the agency and from other organizations as well. Input can be obtained from resources such as the FBI; NCIC; and the National Center for Missing & Exploited Children — in particular Team Adam, which is a rapid-response team of experienced law enforcement investigators.
6. Update descriptive information. If it appears the case will not be promptly resolved, investigators shall ensure the descriptive record, especially that entered into the NCIC Missing Person File, is updated to include dental characteristics, scars, marks, tattoos, and fingerprints along with additional articles of clothing, jewelry, or unique possessions. Note: The National Child Search Assistance Act — enacted in 1990 and amended by the PROTECT Act in 2003 — mandates the entry of descriptive information for all persons, birth through 20 years of age. These entries are required to be made no more than 60 days after the report is taken.

VI. Procedure: Recovery of a Missing/Unidentified Person

- A. An officer assigned to the report of an unidentified person, whether living or deceased shall:
 1. Obtain a complete description. Officers who are assigned to this task shall utilize the NCIC Unidentified Person File Worksheet.
 2. Enter the unidentified person's description into the NCIC Unidentified Person File. This file is compared daily with the contents of the NCIC Missing Person File. Entries with common characteristics are flagged and both agencies are informed.
 3. Utilize all available resources to aid in identification of the person. The National Center for Missing & Exploited Children and state medical examiners may be of assistance in the identification.
 4. Cancel all notifications after identification is confirmed.
- B. An officer assigned to the recovery or return of a missing person shall:
 1. Verify the located person is, in fact, the reported missing person. An officer shall personally verify all returns. The benefits of this practice

include assessing the person's safety, gaining intelligence about possible predators, and helping to prevent future episodes.

2. Inform, in the case of a missing adult who has been located, the located person he or she is the subject of a missing-person investigation. If the located person is a competent adult, the officer shall determine the person's willingness for law enforcement to reveal his or her whereabouts. To the extent possible, a person's desire to remain hidden shall be honored.
3. Notify the initial reporting person(s) of the well-being and, if permissible, the whereabouts and contact information of the person who has been located.
4. If needed, secure intervention services. During the verification process, officers shall be alert for indications that additional services may be needed before a located person can be safely reunited with his or her family. These services may include mental and/or physical health examinations and arrangements for family counseling.
5. Arrange, in the case of a runaway or missing child from within department jurisdiction who has been located and who is not wanted on a warrant or other law violation, the return of the child to his or her legal guardian or to an appropriate children's shelter. Officers shall conduct a reunification interview with all children or juveniles that return from runaway status.
6. Place, in the case of a runaway from another jurisdiction or from out-of-state who has been located and for whom a warrant exists or for whom an NCIC missing person "hit" is verified, the child in custody and transport him or her to the appropriate facility for admission.
7. Complete the appropriate supplemental reports and cancel all outstanding notifications. Along with cancellation of the NCIC Missing Person File entry and other notifications regarding the case, a supplemental report shall be completed that describes the person's activities while missing and circumstances of the recovery/return.

VII. Procedure: Abandoned dependent person

- A. Abandonment of a dependent person shall be defined as a person who is the father, mother, or some other person having custody of a child, or of any other person who by reason of mental or physical disability is not able to care for the person's self, who knowingly or recklessly exposes such person to a hazard or danger against which such person cannot reasonably be expected to protect such person's self or who deserts or abandons such person, knowing or having reason to believe the person will be exposed to such hazard or danger (see Iowa code 726.3 Neglect or abandonment of a dependent person).
- B. Abandoned dependent persons who come in contact with department personnel shall be accompanied and safeguarded at all times. Where possible, the abandoned dependent person shall be cared for by a sworn officer while in agency custody.

- C. Immediately following the recovery of an abandoned dependent person, the investigating officer shall ensure the Iowa Department of Human Services is contacted for assistance in caring for and placement of the dependent person into protective custody. The dependent person shall be cared for by department personnel until custody is relinquished as directed by the Department of Human Services.
- D. The Criminal Investigation Division shall be responsible for investigating the circumstances surrounding the abandonment of the dependent person. If warranted based on the investigation and with the approval of the prosecuting attorney with jurisdiction over the incident, criminal charges may be filed against the persons responsible for abandoning the child/dependent person.
- E. The State of Iowa does provide a safe haven law. The law allows a new born infant to be left at certain facilities. The law has many provision and shall be consulted directly to determine if it applies to the situation being investigated (See Iowa Code 233).

VIII. Procedure: Amber Alert System

- A. The Amber Alert system is a voluntary, cooperative program between law enforcement and local broadcasters to send an emergency alert to the public when a child has been abducted and it is believed the child is in danger of serious bodily harm or death. Under the Amber Alert system, area radio and television stations shall interrupt programming to broadcast information about the missing child using the Emergency Alert System (EAS), formerly known as the Emergency Broadcast System.
- B. The following criteria shall be met before activating the Amber Alert System:
 - 1. Law Enforcement must confirm a child has been abducted and entry has been made into the IOWA/NCIC Systems identifying the child as missing.
 - 2. The individual is under the age of eighteen (18).
 - 3. Law Enforcement believes the circumstances surrounding the abduction indicate the child is in danger of serious bodily harm or death.
 - a. What causes you to believe the child is in danger?
 - b. When you locate the child and whoever they are with, will you make an arrest and file charges?
 - 4. There is enough descriptive information about the child, abductor, and/or suspect's vehicle to believe an immediate broadcast alert will assist in the safe recovery of the child.
- C. After confirming the above information, the officer shall immediately inform their supervisor of the circumstances of the disappearance. The supervisor or designee shall fill out the Amber Alert packet of information (located in the Department forms folder) and fax the same to Westcom Communications and the Department of Public Safety Communication Center. Included in the Amber Alert packet will be the following forms:

1. Facsimile Transmission Sheet.
 2. Two page Emergency Notification Message.
 3. Liability Agreement.
 4. Authorization for Release of Juvenile Information.
 5. Cancellation Form.
- D.** Prior to activating the alert, the supervisor shall inform their division commander who will notify the Chief of Police. If the division commander cannot be immediately reached the supervisor shall initiate the Amber Alert. The chain of command notification process shall not delay the activation of the Amber Alert.
- E.** Copies of the Amber Alert Notification shall be maintained in the main case file.
- F.** Department of Public Safety Communications shall send the information to all designated alert stations. The alert stations shall activate the plan through the EAS.
- G.** The below checklist shall determine if the Amber Alert System shall be activated:
1. Is the abducted child under the age of eighteen?
 - a. If "yes" - go to #2
 - b. If "no" - do not activate
 2. Was the incident witnessed by anyone?
 - a. If "yes" - go to #4
 - b. If "no" - go to #3
 3. Did the incident involve acts of violence?
 - a. If "yes" - go to #4
 - b. If "no" - go to #4
 4. Is there enough descriptive information available for the broadcast to enable the public to assist?
 - a. If "yes" - go to #5
 - b. If "no" - Do not activate
 5. The abducted child in danger of serious bodily harm or death?
 - a. If "yes" - activate
 - b. If "no" - Do not activate
- H.** Upon activation of an Amber Alert, the Investigation Division shall immediately respond to begin working the investigation and follow any leads generated.
- I.** Upon activation of an Amber Alert, the Support Services Division shall support the Investigation Division by answering phone lines established in the Alert or in any other capacity as deemed necessary.
- J.** Department Responsibilities:
1. At least one designated point of contact (POC).
 2. Multiple phone lines or the ability to answer a multitude of phone calls. Assistance may be gained through Westcom Communications.
 3. With the assistance of Westcom Communications, statewide NLTS messages to all agencies.
 4. Adoption of a written procedural policy.

- 5. Periodic training on implementation of the plan.
- K. Following the activation, the Department shall plan for the following:
 - 1. Overwhelming increase in calls.
 - 2. Demands from callers.
 - 3. Possible criticism from involved parties.
- L. Activation of the Amber Alert System shall be subject to an administrative review. Overuse of the plan will cause it to become ineffective.

IX. Procedure: Alert Iowa

- A. ALERT IOWA is an emergency notification system that notifies persons in an established alert area by sending a call by voice, email, text, or other types of instant messaging. ALERT IOWA is a voluntary service allowing anyone to sign up to receive messages.
- B. The criteria for utilizing the ALERT IOWA Emergency Notification System shall be any significant events where the timely notification of an affected population or geographic area is essential or desirable to include missing persons, evacuation notices, and environmental or manmade disasters. The system shall not be used for routine, non-emergency use.
- C. When encountering a missing person incident, a supervisor may request an ALERT IOWA notification be initiated by WestCom. If utilizing the ALERT IOWA system for any incident, the supervisor's chain of command will be notified immediately. If able, based on the circumstances, the supervisor shall make notifications and contact support personnel from the Investigation Division and Support Services Division prior to initiating the alert. Notifications shall not delay the use of the alert system.
- D. The ALERT IOWA system allows for the alert area to be modified based on the needs of each incident. When utilizing the system, the size of the alert area shall be determined by the supervisor requesting with the assistance of WestCom. Supervisors shall ensure the alert area is large enough to capture all citizens that may be of assistance in finding the missing person but not so large the Department and WestCom become overwhelmed with calls or information from citizens that are not useful in resolving the incident.
- E. The following information will be requested by WestCom when activating the ALERT IOWA system:
 - 1. The location utilized to initiate the ALERT IOWA. This may be different than the location of the call for service.
 - 2. The radius of the notification.
 - 3. The information to be included in the message. The message must start with the words Urgent or Emergency or Critical.
 - 4. A specific phone number for the public to call. This may be WestCom, 911 or an administrative line monitored at the Department.
- F. Upon activation of ALERT IOWA, the Investigation Division shall immediately respond to begin working the investigation and follow any leads generated.

- G.** Upon activation of ALERT IOWA, the Support Services Division shall support the Investigation Division by answering phone lines established in the alert or in any other capacity as deemed necessary.

Chapter 5: Law Enforcement Operations
Section 41: Patrol
Subsection 2: Operations



Policy/Procedure #: 7
Title: Response to Persons with Mental Illness
CALEA Reference #: 41.2.7

I. Policy: Response to Persons with Mental Illness

Department personnel shall afford people with mental illnesses the same rights, dignity and access to police services provided to all citizens. The Americans with Disabilities Act (ADA) requires equal treatment for people with disabilities in all state and local government services, including law enforcement. The ADA requires law enforcement agencies to make reasonable adjustments and modifications in policies, practices, or procedures. If a person exhibits symptoms of mental illness, personnel may need to modify routine practices and procedures by taking more time and showing more sensitivity to extend services or protections. This policy is intended to address the most common types of interactions with mentally ill persons and provide guidance to department personnel when dealing with such individuals.

II. Procedures: Guidelines

- A.** The terms "mental illness," "emotional illness," and "psychological illness," describes varying levels of a group of disabilities causing disturbances in thinking, feeling, and relating.
- B.** Mental Illness is the impairment of an individual's normal cognitive, emotional, or behavioral functioning caused by social, psychological, biochemical, genetic, or other factors such as infection or brain injury.
- C.** Many people with mental illness manage symptoms successfully with the proper use of medications, while others may experience psychiatric difficulties when they do not have access to mental health services, fail to take their medications, or simply do not recognize they are ill.
- D.** Employees must ensure people with mental illness receive the necessary assistance to access services. This requires time and patience beyond what is normally provided.

- E. Individuals with a mental illness may be detained or arrested and require transport, and processing. Officers must familiarize themselves with the proper methods of transport, arrest, and detention to ensure employee safety while providing all reasonable support for the person's mental illness.

III. Procedure: Common Symptoms/Encounters

- A. Symptoms of mental illness may vary but mentally ill persons have thoughts, feelings, or behavioral characteristics which may result in an inability to cope with the ordinary demands of life. While a single symptom or isolated event does not necessarily indicate mental illness, professional help should be sought if symptoms persist or worsen. The following may prove useful in recognizing signs of mental illness:

- Social withdrawal
- Withdrawal from family, friends; abnormal self-centeredness
- Dropping out of activities such as occupations and hobbies
- Decline in academic or athletic performance
- Loss of interest in once pleasurable activities
- Expression of hopelessness, helplessness, inadequacy
- Changes in appetite, weight loss or gain
- Behaviors unrelated to events or circumstances
- Excessive fatigue or inability to sleep
- Pessimism and perceiving the world as "dead"
- Thinking or talking about suicide
- Inability to concentrate or cope with minor problems
- Irrational statements, poor reasoning, memory, judgment
- Expressing ideas of being harassed or threatened
- Nonsensical speech, word repetition, extremely slow speech
- Argumentative, belligerent or hostile behavior
- Inability to cry or excessive crying
- Nonverbal expressions of sadness or grief
- Hyperactivity or inactivity
- Deterioration in personal hygiene and appearance
- Drug or alcohol abuse
- Forgetfulness or loss of valuable possessions
- Inappropriate use of household items, e.g. aluminum foil covering windows
- Hoarding: accumulation of trash, newspapers, etc.
- Disorientation in time, place
- Inability to find way in familiar settings

- B. The degree to which these symptoms exist varies from person to person. Many of these symptoms represent internal, emotional states that are not readily observable from a distance but may be noticeable in conversation with the person.

- C. Employees must recognize responses from people with certain mental illnesses may resemble those of people who have abused substances such as alcohol or drugs. Individuals may exhibit signs they are intoxicated when in fact they have not taken their prescribed medications.
- D. Employees should be prepared to encounter a person with a mental illness at any time. Common situations in which employees may encounter such individuals include but are not limited to the following:
 - 1. Wandering aimlessly or engaged in repetitive or bizarre behaviors in public places.
 - 2. Mentally ill persons are more subject to seizures and may be found in medical emergency situations.
 - 3. Disturbances when caregivers are unable to maintain control over mentally ill persons engaging in self-destructive behaviors.

IV. Procedure: Response

- A. Family members or friends may prove valuable in calming an individual exhibiting unusual behavior as a result of mental or emotional impairment.
- B. The following guidelines detail how to approach and interact with people who may have mental illness and who may be a crime victim, witness, or suspect. These guidelines should be followed in all contacts, whether on the street or during more formal interviews and interrogations. While protecting their own safety, the safety of the person with mental illness, and others at the scene, employees shall:
 - 1. Speak calmly, as loud, stern tones will likely have either no effect or a negative effect on the individual.
 - 2. Use non-threatening body language and if possible keep your hands by your sides.
 - 3. Eliminate to the degree possible, all loud sounds, bright lights, sirens, and crowds and attempt to move the individual to a calm environment.
 - 4. Keep animals away as persons with mental illnesses are often alarmed by barking dogs and other large animals.
 - 5. Look for personal identification or medical tags which often provide a contact name and telephone number.
 - 6. Contact the caregiver. They are often the best resource for specific advice on calming the person and ensuring employee safety until they can arrive.
 - 7. Unless there is an emergency, allow time to interact with mentally ill persons. If they are rushed they may quickly become overloaded.
 - 8. Repeat short, direct phrases to eliminate confusion and distractions.
 - 9. Mentally ill persons may have sensory impairments that make it difficult to process information. Employees should avoid touching the person unless absolutely necessary; use soft gestures, avoid quick movements and do not automatically interpret odd behavior as belligerent.

10. Be conscious of different forms of communication as mentally ill persons often use signals or gestures instead of words to communicate.

11. Maintain calmness and patience.

12. Maintain a safe distance.

C. Once sufficient information is collected about the nature of the incident and the situation is stabilized, Employees may exercise a wide range of options when selecting an appropriate disposition.

1. Release of the person.

2. Request assistance of the Department's mental health Crisis Intervention Team (CIT).

3. Contact the Mobile Crisis Response Team (MCRT) for on scene assistance.

4. Refer or transport the person for medical attention if injured or abused.

5. Release to care of family, caregiver, or mental health provider.

6. Refer or transport to substance abuse services.

7. Assist in arranging voluntary admission to a mental health facility.

8. Transport for involuntary emergency psychiatric evaluation if the person's behavior is a danger to themselves or others.

V. Procedure: Interview and Interrogation

A. Officers attempting to conduct an interview or interrogation with a person that is obviously mentally ill should consult the appropriate County Attorney's office to determine a course of action.

B. If the mentally ill person is a witness, officers should:

1. Not interpret lack of eye contact or strange actions as indicative of deceit.

2. Use simple and straightforward language

3. Be prepared to alter common interview techniques. Do not suggest answers or attempt to complete thoughts of persons slow to respond.

4. Recognize the mentally ill persons might be easily manipulated and highly suggestible.

VI. Procedure: Detention

A. If an individual with a mental, emotional, or psychological illness is detained, officers shall make reasonable efforts to use the least restraint possible to protect the subject and others from injury. The overall circumstances and the person's potential for violence will determine if handcuffs should be used as a temporary measure to prevent injury to the person or the officer. Officers may consider transport by Fire/Rescue personnel and utilization of the waist restraint device (See Chapter 8 Section 70.1.1 of the Operations Manual).

B. In minor incidents where a person is suffering from mental illness, officers should seek non-arrest resolutions. The most desired resolution is voluntary admission to an appropriate mental health facility or treatment. When public safety is at issue, officers shall be responsible for ensuring the person is detained for an involuntary emergency evaluation.

- C. When a mentally ill person is being transferred to another agency or facility, the transporting officer shall be responsible for notifying the agency or facility of the risk in advance of their arrival. This will allow the agency or facility to make needed preparations for accepting the detainee (See Chapter 8 Section 72.5.1 of the Operations Manual).
- D. **VOLUNTARY ADMISSION:** The following scenarios would indicate minimal officer involvement:
1. Persons who appear to be in need of psychiatric evaluation and do not appear to pose an imminent danger to themselves or others should be referred to the Department's CIT, MCRT or a mental health facility. (A family member or other responsible person is often available to assist the disturbed person in seeking such treatment and should be provided with the information and assistance necessary to secure the needed help.)
 2. When possible, persons who have been or are under the care of a private physician should be referred to the physician. The CIT or MCRT may assist in contacting the appropriate physician.
 3. Persons who voluntarily agree to psychiatric evaluation shall be taken to hospital or another appropriate facility. Again, the CIT or MCRT may assist with this process.
 4. When necessary, the Department shall assist with transportation of mentally ill persons.
- E. **INVOLUNTARY ADMISSION:** A higher level of law enforcement intervention is required when officers encounter the following scenarios:
1. The person is an imminently dangerous to self or others.
 2. The person is unable to care for self (unable or refuses to accept intervention which would meet minimum needs for food, clothes, shelter or physical well-being).
 3. The person is suffering substantial physical deterioration and shows an inability to function if not treated immediately.
 4. Officers can respond with the most appropriate of the following alternatives for involuntary admission for psychiatric care:
 - a. When the person in question poses no apparent immediate threat to themselves or others, a relative, caregiver, CIT, or a MCRT member may petition a judge to order the detention and a hearing for the person who is believed to be in need of psychiatric hospitalization.
 - b. Officers or the CIT who personally observe the actions of the individual and have reason to believe that the person is in clear and imminent danger of causing personal harm to himself or others shall be transported to a hospital or other appropriate facility. Once at the hospital or facility, trained staff shall be informed of the situation by the officer or CIT and conduct their own evaluation. When situations warrant, hospital staff, CIT or other trained professionals shall petition the court for an involuntary committal for psychiatric care.

- c. The officers involved shall complete an incident report detailing circumstances of the event which led to the involuntary committal.

VII. Procedure: Available Resources

- A. The Department's Crisis Intervention Team (CIT): The CIT was designed to support police officers on calls related to a mental health crisis or other mental health issues. The Department's CIT is comprised of a sworn officer and a mental health professional specifically assigned to assist persons in a mental health crisis as well as offering other mental health resources and referrals.
- B. Mobile Crisis Response Team (MCRT): The MCRT is designed to assist police officers on calls related to mental health issues. MCRT is a collaborative effort where registered psychiatric nurses and mental health professionals are dispatched at the request of law enforcement to complete assessments and stabilize situations with on-site crisis counseling, provide one time medication management and referral for services, and assist with psychiatric hospitalizations. MCRT shall be utilized when the Department's CIT is not available to respond.
- C. The assistance of the CIT and MCRT provides the following benefits:
 - 1. Saves time by allowing officers to return to other duties as quickly as possible.
 - 2. People with mental health issues avoid unnecessary incarcerations and hospitalizations.
 - 3. Most importantly, CIT and MCRT facilitates appropriate treatment and follow up to address the mental health needs of clients.
- D. Area hospitals: The officer can utilize this resource for voluntary or involuntary admissions. Broadlawns is the preferred hospital; however, most area hospitals have trained staff to treat mental illness.
- E. Mind Spring Mental Health Alliance or the National Alliance for the Mentally Ill (NAMI) of Greater Des Moines. Both organizations offers support and education for families dealing with mental illness and advocates for needed services.

VIII. Procedure: Training

- A. Response to mental illness training shall consist of the following:
 - 1. Recognition of persons suffering from mental illness.
 - 2. Guidelines for employees to follow in dealing with persons they suspect are mentally ill, especially during contacts on the street as well as during interviews and interrogations.
- B. Entry level crisis intervention training shall be conducted by the Iowa Law Enforcement Academy and during the field training program for sworn personnel. Non-sworn personnel shall receive entry level training as part of their departmental orientation training.

- C. Annual refresher training shall be conducted for all Department employees. The training shall meet the requirements established by the Iowa Law Enforcement Academy.

Chapter 5: Law Enforcement Operations
Section 41: Patrol
Subsection 2: Operations



Policy/Procedure #: 7(A)
Title: Mental Health Crisis Intervention Team
CALEA Reference #: 41.2.7

I. Policy: Mental Health Crisis Intervention Team

The Urbandale Police Department shall deploy a mental health crisis intervention team (CIT) to address mental health related calls for service. The CIT shall be utilized to offer an in-depth response to mental health related incidents and provide a connection to additional mental health related services for community members experiencing a mental health crisis. In addition to mental health related calls for service, CIT shall offer assistance to individuals experiencing homelessness.

II. Procedure: Assignment

- A.** The CIT shall be comprised of a sworn police officer trained in response to individuals experiencing a mental health crisis and a civilian mental health co-responder.
- B.** The Support Services Division shall administer CIT and their assignments.
- C.** With the assistance of the Patrol Division, CIT shall handle mental health related calls for service. During established work hours, the top priority for CIT will be responding to mental health crisis related calls for service as they occur. Outside of established work hours for CIT, the Patrol Division shall respond to mental health crisis related calls for service as established in Chapter 5 Section 41.2.7 of the Operations Manual.
- D.** The CIT officer is a specialized assignment within the department and selection for the position shall follow the procedures established in Chapter 2 Section 16.2.1 of the Operations Manual.
- E.** The Support Services Division shall set the work hours for CIT with consideration for call volume and the need to provide follow up services. Generally, CIT shall provide 40 hours of service during the work week. The department may require the services of the CIT team members for training, emergency situations, and/or to assist with other police matters at any time.

- F. CIT shall be required to report to the Support Services Division for briefings and updates on a schedule established by the Support Services Division Commander.
- G. The CIT officer shall be required to carry the same equipment when responding to a call for service as a patrol officer to include a protective vest and a body worn camera. The uniform worn by the CIT officer shall identify them as an Urbandale Police officer but may be more subdued than a traditional uniform in an effort to build trust with the mental health client.
- H. The mental health co-responder shall be required to wear a protective vest when responding to a call for service. The uniform worn by the mental health co-responder shall clearly identify them as a member of CIT for the Urbandale Police Department.
- I. The mental health co-responder assigned to the CIT is not a certified police officer in the State of Iowa and is not authorized to make an arrest or utilize force against individuals. The mental health co-responder may utilize force in limited situations to protect themselves or others from immediate harm and will be provided basic self-defense training to that effect.

III. Procedure: Duties and Responsibilities

- A. The CIT officer and the mental health co-responder shall perform the following duties:
 - 1. Respond to mental health crisis related calls for service within the City of Urbandale and other jurisdictions in which the department has established an agreement for services. The mental health co-responder shall not respond to calls for service without the CIT officer or a designated alternative officer.
 - 2. Be a direct and accessible liaison between the mental health community and the Urbandale Police Department.
 - 3. Complete mental health follow-ups with identified consumers or referrals from officers and staff.
 - 4. Complete assessments of individuals in a mental health crisis to determine appropriate mental health services.
 - 5. Provide transportation to identified resources best suited for the person requesting/requiring hospitalization.
 - 6. Develop and maintain a region-specific resource guide linking all the community stakeholders involved in mental health services.
 - 7. Coordinate with mental health resources for continuity of care.
 - 8. Represent Urbandale CIT in meetings with local facilities, hospitals, courtroom workgroups, jails and holding facilities as needed.
 - 9. The CIT officer shall produce quarterly reports to department administration pertinent to the program to include but not limited to:
 - Number of calls

- Type of calls
 - Number and type of referrals
 - Dispositions
 - Client demographics
 - Call demographics
10. The mental health co-responder shall provide pertinent statistical information to the department as requested.
 11. Participate in required training to maintain and improve qualifications and quality of service.
 12. Provide continuing training and education on mental health to employees of the department.
 13. Provide education on the CIT program and mental health to the community.
 14. Provide services and resources the department regarding homelessness response.
 15. Perform other duties or assume other responsibilities as assigned.
- B.** The CIT officer and the mental health co-responder shall maintain all training certifications and qualifications in accordance with department policy and applicable state laws.

IV. Procedure: Response

- A.** All calls determined by WestCom or the department to be mental health crisis related shall require a minimum of two sworn officers to respond. These calls shall include but not be limited to mental health, psychiatric patients, suicide threats/attempts, and intentional overdose. Officers may ask for CIT assistance on any call for service that has a mental health, substance abuse crisis, or homelessness component. CIT will be considered a one-officer unit when answering calls for service. The CIT officer or other officers dispatched on mental health crisis related calls can use discretion to move the call to a one-officer response. Safety for all parties including responding officers and mental health co-responder shall be the top priority, and officers are reminded mental health crisis situations can change rapidly.
- B.** When available, CIT shall be dispatched as one of the responding units when the call is determined to be mental health crisis related. CIT shall be considered the primary unit on the call. CIT will have primary responsibility for providing a mental health assessment and any needed services whether the services be immediately needed or on a follow up/referral basis.
- C.** When CIT is not available, responding officers will have responsibility to determine the level of mental health services needed whether they be immediate or on a follow up/referral basis. Responding officers may request the assistance of mobile crisis from Polk or Dallas County, or a CIT team from a neighboring jurisdictions; however, other agencies or

service providers have no obligation to respond. Officers utilizing outside resources shall be required to document the call for service in accordance with department policy. All mental health crisis related calls for service that occur without the assistance of the CIT shall be referred to CIT for evaluation and follow up/referral services utilizing the department's records management system crisis intervention form. This form can be utilized as a CIT referral only, or to document cases with a mental health crisis component. Pursuant to Iowa Code, this report is not a public record. Upon request, this report shall be made available to the person who is the subject of this report. This report may also be provided to a mental health treatment provider, substance-related disorder treatment provider, homeless service provider, or any other appropriate service provider in connection with a referral of service.

- D. As part of their duties, CIT will provide follow up services to persons involved in mental health related calls. Follow up services may include welfare checks, appointment reminders, providing transportation, and other services. Based on the assessment of CIT, calls for service involving follow up with a person that is not currently in crisis may be handled by CIT without an additional officer. CIT shall always err on the side of caution when determining the need for an additional officer and must be able to clearly articulate why an additional officer is not needed. If at any time during the follow up services the situation changes, CIT shall immediately request additional officers to respond.
- E. As the intent of CIT is to build trust and rapport with persons experiencing a mental health crisis, if criminal charges will be filed and the person arrested, other officers assisting CIT shall be responsible for all appropriate case work and reporting requirements unless the situation dictates otherwise. In addition to all appropriate case work required for a criminal case, officers shall complete a CIT referral form (when CIT is not present at the scene).

V. Procedure: Training

- A. Officers assigned to the CIT position shall complete a minimum of 40 hours of crisis intervention training as established by the department.
- B. Ongoing training in crisis intervention response and related mental health topics shall be required of the CIT officer as established by the department. Recommended training includes the following:
 - 1. Trauma informed investigations.
 - 2. Assisting individuals in crisis.
 - 3. Group crisis intervention (CISM).
- C. The mental health co-responder assigned to CIT shall be required to review and acknowledge receipt of the Urbandale Police Department Operations Manual with specific field training in the following areas:
 - 1. Police radio operation

2. Self defense
 3. Overview and familiarization with Urbandale Police Department use of force policies and procedures.
 4. Overview and familiarization with Urbandale Police Department firearms and less lethal equipment to include limited hands-on instruction for familiarity.
 5. Overview and familiarization with basic police vehicle operation with hands on instruction on use of the mobile computer, radio, and emergency lights/siren. Mental health co-responder is not authorized to operate a police vehicle during any type of emergency response but will be authorized to operate the vehicle during normal driving situations.
 6. In-car and body worn camera policy and procedures.
 7. Transporting detainees.
 8. Processing and temporary detention.
 9. Property and evidence control.
 10. Other areas of police operations deemed necessary for successful integration of the mental health co-responder into the operation of CIT.
- D.** All training for the CIT officer and the mental health co-responder shall be documented according to department policy.
- E.** Training for the mental health co-responder shall meet any requirements established by the State of Iowa. The department may require training in addition to requirements established by the State.

Chapter 5: Law Enforcement Operations
Section 41: Patrol
Subsection 2: Operations



Policy/Procedure #: 8
Title: Alarm Response
CALEA Reference#: 81.2.13

I. Policy: Alarm Response

It shall be the policy of the Urbandale Police Department to respond to all alarm calls for service throughout the city. Financial institution and holdup alarms indicating a robbery shall require a specific response to enhance the possibilities of the arresting the suspects and to observe proper precautions for the safety of officers, employees, and the general public.

II. Procedure: General

- A.** All calls for service to respond to an alarm shall be handled by WestCom Emergency Communications (WestCom).
- B.** WestCom shall dispatch two officers to respond to all alarms. Officers or supervisors may advise communications they will “check and advise” on security alarms indicating they will check the exterior of the structure and advise if additional units are needed. An officer shall not enter a structure found unsecure without proper backup.
- C.** Security alarm dialers will not be allowed to enter the emergency 911 phone lines. Alarm owners will be advised to have dialers ring in to non-emergency phone lines.
- D.** Upon receipt of a security alarm, officers shall be dispatched and communication personnel shall attempt to notify a key holder. When the alarm is through a private alarm service, the service should attempt to contact the key holder.
- E.** False alarm calls for service shall be billed according to the City of Urbandale ordinance. The Office of the Chief of Police shall be responsible for documentation and proper billing for false alarms.

III. Procedure: Financial and Holdup Alarms

- A.** Upon receipt of a financial institution or holdup alarm, a minimum of two patrol units shall be assigned and the patrol supervisor shall be notified.

- B.** Responding officers may use appropriate vehicle warning devices when approaching the scene, but the siren will not be used within the hearing range of the reported robbery.
- C.** Responding units to the scene shall be observant of any suspicious vehicles leaving the scene as well as other vehicles or persons outside the facility who may be serving as lookouts, cover, or drivers for a robbery team.
- D.** The first unit on the scene shall serve as the primary unit until relieved by a supervisor and shall take a position in front of the facility that provides good observation without being easily visible to those inside. The primary unit shall report on observable conditions at the location to the communication center, but shall not approach the building.
- E.** The primary and all subsequent units arriving at the robbery location shall report their arrival and positions to the communication center. The primary unit or supervisory officer shall direct responding units into positions that will establish a building perimeter covering all exits and entrances.
- F.** Once the building perimeter has been established and no notice of a false alarm has been received, the primary unit or supervisor on the scene shall determine whether communication personnel shall telephone the establishment. If a call is made, the communication operator shall identify themselves and inquire whether a robbery is in progress. If the call is not answered or a questionable response is provided to the inquiry, officers at the scene shall be informed of these facts and informed a possible robbery is in progress.
- G.** If a robbery in progress is suspected, the primary unit or supervisory officer shall determine whether to request additional backup and whether specialized units shall be alerted to include canine or the Suburban Emergency Response Team (SERT). Unless otherwise directed, officers shall wait until suspects have exited the building and are at low risk for attempting to reenter before attempting apprehension. This helps avoid the development of a hostage situation.
- H.** Once suspects have left the area or been apprehended, the crime scene shall be secured by officers in preparation for processing by crime scene technicians, departmental investigators, and/or federal agents.
- I.** If a robbery has been committed and the suspects have left the scene, the primary unit shall begin preparation of the initial report by identifying witnesses, caring for any injured parties, securing the crime scene and obtaining information regarding the suspects for supplemental broadcasts. Remaining units shall initiate the search for suspects on likely escape routes, being alert to unusual activities and circumstances.
- J.** If communication personnel notify the officers they have been in contact with an employee of the institution and there does not appear to be a robbery in progress, officers shall determine the identity and description of

the employee and wait for them to exit the building and approach the officers. Officers shall accompany the employee into the institution in order to verify the situation and shall notify the communication center once the verification is complete.

- K.** If the alarm is received after business hours and the institution is not occupied, responding officers shall assume positions in the front and rear of the building and jointly conduct an inspection of the facility for signs of forced entry. If signs of forced entry exist, the officer shall follow procedures for conducting a building search. If the building is secure, communication personnel shall be notified to contact the owner or the institution's designated contact person to meet them at the location.
- L.** The community relations officer shall assume responsibility for providing all employees of banks, financial institutions, and related establishments with training on their responsibilities in the event of a robbery and conduct follow-up with those who fail to comply with departmental requirements. In particular, employees should be familiarized with the following:

 - 1.** Departmental procedures in response to a financial institution alarm.
 - 2.** Employees' responsibilities for protecting their safety and the safety of others.
 - 3.** The proper use of decoy money and explosive money packages.
 - 4.** Tips to avoid hostage taking, i.e. closing establishment doors immediately after the suspects exit and appropriate actions if one is taken hostage.
 - 5.** Use of the silent alarm.
 - 6.** The use of signals or placards when approaching officers.
 - 7.** Protection of evidence.

Chapter 5: Law Enforcement Operations
Section 41: Patrol
Subsection 3: Equipment



Policy/Procedure #: 8
Title: In-Car & Body Worn Recording Systems
CALEA Reference#: 41.3.8, 41.3.10

I. Policy: In-Car & Body Worn Recording System

The philosophy of the Urbandale Police Department is to utilize advances in audio/video technology to accurately document police/citizen interactions and to provide quality law enforcement services. A policy is established to provide direction to officers in the use of the in-car and body worn camera systems. The policy is intended to provide officers and supervisors with instruction on when and how to use in-car and body worn cameras so they may reliably record their contacts with the public. Officers shall activate in-car and body worn cameras when such use is appropriate to the proper performance of his or her official duties as established in this policy. The policy does not govern the use of surreptitious recording devices used in covert operations.

II. Procedure: Use

A. The primary objectives of the in-car and body worn cameras are as follows:

- 1.** Accurate documentation of police-citizen contacts, arrests, and critical incidents.
- 2.** Enhance the accuracy of reports and testimony in court.
- 3.** Enhance the Department's ability to review probable cause for arrest, officer and suspect interaction, and to obtain evidence for investigative and prosecutorial purposes.
- 4.** To provide additional information for officer evaluation and training.
- 5.** Documentation of crime and accident scenes or other events including the collection and documentation of evidence.
- 6.** Other legitimate law enforcement purposes as determined by a supervisor.

- B.** All uniformed officers assigned to the Patrol Division utilizing a marked patrol vehicle for their duties shall be deployed in a vehicle with an in-car camera and use it as established in this policy. Exceptions to this requirement may be made by a supervisor if there are no marked vehicles with operable in-car camera systems available. The command vehicle assigned to the patrol division commander will not be required to have an in-car camera system.
- C.** Except for officers performing administrative functions, all sworn personnel shall be issued a body worn camera and be required to use it as established in this policy. A supervisor may grant an exception to this requirement if there are no body worn cameras available for deployment.
- D.** Any officer assigned to a patrol vehicle shall be required to synchronize their body worn camera to the patrol vehicle's system. The officer shall maintain the synchronization for the duration of their shift to ensure all available camera features and triggers are enabled. Inability to synchronize the body camera to the patrol vehicle system shall be reported to a supervisor immediately.
- E.** All officers and supervisors utilizing in-car and body worn cameras shall be trained in their proper use and the policy requirements.
- F.** All cameras and related equipment shall be tested for proper functioning at the beginning of each officer's shift. Any deficiencies with the camera shall be reported to a supervisor immediately and a repair/service form shall be forwarded to the support services division. Any time the camera is determined to be malfunctioning, it shall be replaced by an operable camera as soon as possible. Officers are responsible for the proper care of cameras assigned for use and will immediately report any loss or damage to the camera to their chain of command. Supervisors shall be responsible for inspection of the cameras as part of their vehicle and personnel inspections outlined in Chapter 6 Section 53.1.1 of the Operations Manual.
- G.** Cameras shall be deployed in a manner that best captures the totality of the incident. For in-car cameras, the view shall be towards the front of the patrol car and the rear seat. Officers are allowed to manipulate the in-car camera to capture specific events. The body worn camera shall be worn center mass in a vertical position on the torso. Officers are allowed to mount the body worn camera in an offset location on the torso to accommodate uniform or clothing configurations but shall ensure the body worn camera is still able to accurately record all incidents encountered. Officers are allowed to manipulate the body worn camera to capture specific events.
- H.** The in-car camera and body worn cameras shall be set to automatically record in the following situations:

1. Upon activation of the emergency lighting equipment facing the front of the patrol vehicle (position 2 or 3 of the light bar activation switch).
 2. When speeds in the patrol vehicle reach 70 mph if utilizing a WatchGuard in-car camera system. Data 911 in-car camera systems will activate the in-car system when the vehicle reaches 70 mph but will not activate the body camera system.
 3. When the vehicle experiences a significant shock or jolt to the system if utilizing a WatchGuard in-car camera system. Data 911 in-car camera systems will activate the in-car system when the vehicle experiences a significant shock or jolt to the system but will not activate the body camera system.
 4. When activating one camera within range of the other camera if utilizing a WatchGuard in-car camera system.
- I. Regardless if the officer is the primary or secondary unit(s), the in-car camera shall be manually activated in the following situations:
1. During all traffic stops.
 2. To document the erratic operation of a vehicle by a person suspected of driving impaired.
 3. During contacts with any person suspected of criminal activity.
 4. When a person is detained and placed in the rear of a patrol vehicle.
 5. Pursuit situations.
 6. Any emergency response to a call for service.
 7. Based on officer discretion, any other incident deemed necessary or beneficial.
- J. Regardless if the officer is the primary or secondary unit(s), the body worn camera shall be activated in the following situations:
1. All traffic stops.
 2. All calls for service.
 3. All interviews or interrogations unless conducted within an interview room equipped with functioning audio/video recording equipment.
 4. Except as noted in this policy, during all official police interaction with the public to include victims, witnesses, and suspects.
 5. During any enforcement activity to include search warrants, arrests, and all SERT operations.
 6. During all search and seizure activity associated with a search or arrest warrant.
 7. Based on officer or supervisor discretion, any other incident deemed necessary or beneficial.
- K. Officers are not required to utilize an in-car or body worn camera when participating in community outreach events.
- L. Officers are not required to inform the public they are being recorded but shall disclose recording equipment use upon inquiry. Non law

enforcement personnel shall not be allowed to view recordings at the scene.

- M.** The cameras shall be activated prior to the officer exiting their vehicle or as soon as practical during an event requiring use. Except as noted in this policy, once an officer activates a camera, they shall continue to record until the completion of the event.
- N.** Officers that fail to properly record an incident shall immediately begin recording if the incident is still in progress. Immediately upon completion of the incident, the officer shall notify a supervisor of the failure to record. Based on the incident, the supervisor shall determine if an attempt to retrieve the unrecorded video utilizing the camera system's recovery features. If the determination is made there should be an attempt to recover the video, support services division personnel shall be notified immediately to aid in the recovery.
- O.** Body worn cameras shall not be used in the following situations:
 - 1. With supervisory approval, during situations in which the victim or witness of a crime requests not to be recorded. The request not to record shall be captured on the camera prior to turning the device off.
 - 2. With supervisory approval, during incidents of a sensitive nature that may be hampered by recording the situation (e.g. person wanting to become a confidential informant).
 - 3. During transport or booking procedures if they are captured by an in-car camera or the camera system in any holding facility or jail setting. If no in-car camera or facility recording equipment is present, the body camera shall be utilized during transport and booking procedures.
 - 4. During student counseling sessions performed by the School Resource Officer. The School Resource Officer will be required to utilize a body worn camera during the enforcement of school policy or other law enforcement related enforcement (parking complaints, truancy, and other law infractions).
 - 5. With supervisory approval, any prolonged incident that requires extended time to complete or wait for outside assistance (e.g. holding the perimeter at a secure crime scene).
- P.** In-car and body worn cameras are intended to supplement department reports. Submitted reports are still required to capture the totality of the incident.

III. Procedure: Review

- A.** Officer shall use media captured via the in-car and body worn cameras to assist with the investigation and completion of reports.
- B.** Unless otherwise restricted by the chief of police or designee, officers involved in a use of force incident to include an officer involved shooting may review media captured from the in-car and body worn cameras prior to making any statements.

- C. Unless otherwise restricted by the chief of police or designee, officers may review media captured via the in-car or body worn camera prior to making any statements in an administrative or criminal investigation.
- D. With division commander approval, officers may use media captured via the in-car or body worn camera for training purposes unless restricted by the chief of police or designee. Use of the media for training shall not hinder administrative or criminal investigations.
- E. When a complaint on an employee is received, any recording from the in-car and/or body worn camera as well as any other evidence (e.g. photos) that is relevant to the complaint shall be noted in the investigating supervisor's report for potential review by other supervisory personnel involved in the complaint review process.
- F. When a use of force incident is captured on the in-car or body worn camera, the first line supervisor of the officer(s) involved in the incident shall note in the use of force review form the existence and location (date, time, vehicle, officer, etc.) of the media files and any other relevant evidence (e.g. photos) for review by other supervisors in the chain of command.
- G. An annual administrative review of the in-car/body worn camera program shall be completed by the support services division commander or designee and provided to the chief of police for review.

IV. Procedure: Restrictions

- A. Except when necessary in a criminal investigation or approved by the chief of police, employees shall not make surreptitious recordings of other employees.
- B. Employees shall not use the in-car or body worn cameras to intentionally intercept communications that are privileged under the law.
- C. During non-enforcement related activities, in-car and body worn camera shall not be intentionally activated to record communications with fellow employees with or without their knowledge.
- D. When a camera is being utilized and when practical, officers shall advise other employees and law enforcement personnel. Employees involved in an incident shall assume recording devices are being utilized.
- E. Employees shall not record the following situations:
 - 1. Employee breaks.
 - 2. Report writing.
 - 3. Discussion of a case with other officers.
 - 4. Other administrative functions.
 - 5. General discussion with employees.
 - 6. Personal activities.
- F. In-car and body worn cameras shall not be utilized to record confidential informants or employees acting in an undercover capacity unless approved by a supervisor for specific reasons.

- G. Accessing, copying, posting, or releasing in-car or body worn recordings for other than law enforcement purposes is prohibited.
- H. Recordings from in-car and body worn cameras may be subject to open records laws as provided by the Iowa code. If the requirement for public release is not evident, legal counsel shall be consulted prior to release.

V. Procedure: Data Storage and Retention

- A. Data from the in-car and body worn cameras is automatically downloaded to a secure server for storage. The equipment records to an internal hard drive and has no removable media. All recordings are uploaded wirelessly to a secure server at the Urbandale Police Department.
- B. Officers shall be required to mark all audio/video captured on the in-car and body worn cameras with one of the following categories to indicate if the recording is evidentiary or non-evidentiary. Retention parameters on any recording may be changed to indefinite by a supervisor based on a complaint, potential liability, litigation, investigation, etc.
 - 1. Indefinite retention (evidentiary) - Felony Incident/Arrest, Pursuit/Use of force, SERT operations.
 - 2. 25 month retention (evidentiary) - Misdemeanor arrest, Traffic accident, Traffic stop, OWI, Citizen contact/call for service.
 - 3. 30 days (non-evidentiary) - Trash, system test, accidental activation, etc.
- C. If a recording is related to more than one category, officers shall select the category with the longest retention period (e.g. a misdemeanor arrest turns into a use of force).
- D. Retention periods for data shall be extended to indefinite for any of the following reasons:
 - 1. To maintain data relevant to an active/pending investigation.
 - 2. To maintain data through the conclusion of any criminal investigation, criminal prosecution, or pending appeal.
 - 3. To maintain data through the conclusion of any civil action involving the City of Urbandale or one of its employees.
 - 4. To maintain data associated with an active arrest warrant.
- E. Officers shall be required to enter any case number associated with a recording in the system for future reference.
- F. The support services division shall periodically review files marked for indefinite retention. Files no longer needed shall be purged from the system.
- G. At any time, an officer may request support services division personnel place a recording from the in-car or body worn cameras in property/evidence control based on the circumstances of a specific incident.

VI. Procedure: Security and Access

- A.** All recordings created on the in-car or body worn cameras shall be the property of the Urbandale Police Department and will be used for official departmental purposes only. Except in the following situations, recordings shall not be released without authorization of the chief of police or designee:

 - 1.** The recording has been requested by the city attorney, county attorney, the Iowa Attorney General's Office, or the United States Attorney's Office as part of a criminal prosecution.
 - 2.** The recording has been subpoenaed by an attorney and the release has been approved by a supervisor after checking with the appropriate prosecutor.
- B.** All recordings on department equipment are subject to investigative review by supervisory personnel for organizational integrity, training purposes, and administrative or criminal investigations.
- C.** As part of the personnel inspection process (monthly for officers and periodically for supervisors), a minimum of one incident that required the use of the in-car camera system and one incident that required the use of the body worn camera system shall be reviewed by a supervisor to ensure policy compliance.
- D.** The in-car and body worn cameras and the audio/video file server/viewing program shall be configured to prevent unauthorized deletion or editing of video files.
- E.** Each officer shall have access to view recordings they create with the in-car and body worn cameras and make copies as needed for evidence and report purposes. Supervisory personnel and designated support services division personnel shall have access to view all recordings and make copies as needed. Under no circumstances shall any employee make a copy of an audio/video file for personal use.
- F.** Officers shall be prohibited from viewing the data captured on an in-car or body worn camera of another officer except when necessary for a criminal or administrative investigation or for other purposes as stated in this policy.
- G.** All officers utilizing in-car or body worn cameras shall receive training on the procedure to mark or retrieve their stored recordings on the server, the conversion process from proprietary formatting to standardized format, and the procedure to copy the recording to a disk or other type of storage device. All requests for copies of in-car and body worn camera recordings will be derived from the original file in the in-car or body worn recording system.
- H.** If the recording has been copied to disk or other type of storage device and placed in evidence and the original file in the in-car or body worn camera system no longer exists, the disk/storage device copy will be

considered the original and all requested copies will be made from said original.

- I. Upon request by an officer or supervisor, it shall be the responsibility of the support services division to convert the file, create a disk/storage device containing the recording, and place into evidence.
- J. City of Urbandale Information Technology Department (IT) shall be designated as the system administrator. The system administrator shall have full access rights to the in-car and body worn camera systems, including managing the systems and assigning user access rights, managing files within the systems, conducting routine audits, and maintaining and updating the system as needed. IT administrators shall not delete any files from the system without the approval of the support services division commander or the chief of police.
- K. The secure server that stores the in-car and body worn camera files will track all user activity on the system, to include but not limited to; system log on, file viewing, and file format conversion in preparation for copying to disk/storage device.
- L. Employees shall not tamper with the recording equipment, change any settings, disconnect any cable or wiring, or perform any other action that will disable the equipment or limit its capabilities. Employees are prohibited from manipulating any data stored on the secured server except for making copies as noted above.
- M. Annually, the support services division shall conduct an administrative review and audit of the in-car and body worn camera program to ensure department policy up to date with current practices, security settings are intact, no unauthorized deletions have occurred, and any other relevant issues are noted. The review and audit report shall be submitted to the chief of police on departmental memorandum. Any unauthorized activity on the system shall be investigated by the Internal Affairs Administrator or designee.
- N. When a recording from the in-car or body worn camera is requested and/or subpoenaed, the request/subpoena shall be handled by support services division. The support services division shall take the following action:
 - 1. **Recording in the system or in evidence:** The support services division shall make a copy of the recording and forward to the person requesting. If the requesting party is not the city attorney, county attorney, attorney general, or U.S. Attorney's Office, the support services division personnel handling the request shall receive supervisory approval prior to release. If the recording is subpoenaed relevant to an active case, prior to the release, the supervisor shall confirm with the prosecuting attorney the need to turn over said recording. If the recording is requested as an open records request

from the media or other party, the chief of police or designee shall make the determination if the recording will be released. Barring a court order, the chief of police or designee shall have the final decision on whether to release an in-car or body worn camera recording. The support services division shall produce a copy of the recording to satisfy the request/subpoena following the approval procedures listed in this policy.

2. **Recording not in the system or in evidence:** If the request for a recording is made and there was no recording of the incident or the incident has been purged from the system due to the current retention schedule, support services division personnel shall inform the requester the recording does not exist.
- O. Support services division personnel shall notify the support services commander any time they are searching for recording of an incident that was required to be recorded on the in-car or body worn camera system but was not and/or the incident was not properly marked in the system. The support services division commander shall forward the information to the division commander of the employee involved.

Chapter 5: Law Enforcement Operations
Section 41: Patrol
Subsection 3: Equipment



Policy/Procedure #: 9

Title: License Plate Recognition Systems and Traffic Camera Recording System

CALEA Reference#: 41.3.9

I. Policy: License plate recognition systems

It is the policy of the Urbandale Police Department to use license plate recognition (LPR) systems and the city of Urbandale traffic camera recording system to enhance the capabilities of the department to solve crime, increase productivity and effectiveness and enhance officer safety. LPR and traffic recording systems shall be used for the detection, investigation, and enforcement duties of police officers and criminal investigators performing official investigations into traffic or criminal violations.

II. Procedure: LPR systems use

- A.** The LPR systems utilized by the department include a series of stationary license plate reading cameras positioned at strategic locations throughout the city of Urbandale and programmed to capture rear images of vehicle license plates and limited vehicle information that may include make, model, color, and other physical descriptors as they travel on public roadways. LPR systems also include access to data bases containing LPR data from other public and private entities.
- B.** The LPR systems use National Crime Information Center (NCIC) information and law enforcement agency information for official use only and shall be considered confidential and law enforcement sensitive. Any misuse of a LPR system shall result in disciplinary action.
- C.** Alerts on LPR systems DO NOT constitute reasonable suspicion or probable cause for enforcement action and will not be acted upon without development of reasonable suspicion or probable cause.
 - 1.** The user shall verify any information from an alert matches the vehicle in question.

2. All alerts from a LPR system associated with NCIC information shall be confirmed through WestCom or independently by the officer.
 3. Upon receiving an alert from a LPR system, officers shall establish reasonable suspicion or probable cause prior to initiating contact or taking any enforcement action.
 4. Vehicle occupants at the time of the alert may not be the subject(s) associated with a specific crime or criminal activity that prompted the alert to be entered into a LPR system. Officers must develop reasonable suspicion or probable cause prior to initiating a traffic stop or any type of detainment.
 5. All alerts from a LPR system acted on by the patrol division shall be documented in the CAD unit history under an incident number. The incident comments will include "LPR Alert" as well as any applicable notes by WestCom or the officer. The incident notes shall contain the LPR system utilized, the type of alert, and disposition of the stop.
 6. If an officer takes enforcement action as a result of a LPR system alert or information, they shall document the alert or information received as part of the case report or in the notes of any ticket issued.
- D. Vehicle license plate information may be entered in a LPR system for inclusion on a department hotlist. A department hotlist contains agency entered license plate and vehicle information that is associated with a person(s) that are or may be involved or associated with criminal activity. The following shall apply to all license plate information entered into a LPR system by the department on a hotlist:
1. The criminal investigation division shall be responsible for and actively manage the department's hotlist. The department hotlist entries must be associated to an active criminal investigation.
 2. If vehicle license plate information is entered into NCIC for association to a criminal violation, amber alert, etc., it will no longer be included in the department hotlist.
 3. When appropriate to the investigation, patrol supervisors shall be allowed to enter vehicle plate information on the department hotlist for forcible felonies and exigent circumstances (i.e. incidents where public safety is critical). All other entries on the department hotlist shall be reviewed and entered by the CID division commander or designee.
 4. All supervisors shall have the authority and responsibility to remove a department hotlist entry when determining they are no longer needed or valid.
 5. If a patrol supervisor makes an entry or removal from the department hotlist, they will send notification to CID by utilizing the specific email account established for notification.
 6. Upon receiving a LPR alert from a department hotlist entry, officers shall establish reasonable suspicion or probable cause prior to initiating contact or taking any enforcement action.
 7. Vehicle occupants at the time of the alert from a department hotlist entry may not be the subject(s) associated with a specific crime or

criminal activity. Officers must develop reasonable suspicion or probable cause prior to initiating a traffic stop or detaining the vehicle or occupants.

8. Once contact is made with a vehicle or associated person(s) with department hotlist entry, the supervisor of the officer(s) making contact shall evaluate if the vehicle license plate information shall be immediately removed or kept in the department hotlist. If determined the vehicle is no longer needed in the department hotlist, the supervisor shall remove the information immediately from the hotlist.
 9. As removal of department hotlist alerts will be critical to lawful use of LPR systems. Officers shall be required to notify a supervisor when making contact with a vehicle or person(s) associated with a department hotlist.
 10. The CID division commander or designee shall audit the department entered hotlists monthly to ensure any vehicle plate information entered is still active and appropriate based on the incident or investigation prompting the hotlist entry.
- E. An analysis or search of LPR systems data for specific license plate information shall only be conducted pursuant to a traffic or criminal investigation.
 - F. Successful use of the information obtained from a LPR system shall be documented by the appropriate division commander and reported to the chief of police on an annual basis citing specific cases. The specific LPR system utilized shall be noted.

III. Procedure: City of Urbandale traffic camera recording system use

- A. The city of Urbandale traffic camera recording system records traffic at various intersections throughout the city of Urbandale. The system does not interface with NCIC or other software programs to produce alerts.
- B. The city of Urbandale traffic camera recording system is restricted to official use only and may be considered confidential and law enforcement sensitive based on its use. Any misuse of the city of Urbandale traffic camera recording system shall result in disciplinary action.
- C. An analysis or search of city of Urbandale traffic camera recording system data for information shall only be conducted pursuant to an administrative action, traffic or criminal investigation.
- D. Records requests for city of Urbandale traffic camera recording system data shall be administered by the support services division.

IV. Procedure: Data security and access

- A. Data and images from a LPR system and recordings from the city of Urbandale traffic camera system are for official use only. Only authorized department employees utilizing secure log-in credentials shall have

access to LPR systems and city of Urbandale traffic camera recording system.

- B.** Only department personnel that are certified to access NCIC information and that have been trained in the proper operational procedures and interpretation of information from a LPR system or the city of Urbandale traffic camera recording system shall be granted access to the systems. This shall include all sworn officers as well as civilian support personnel that receive authorization from a division commander or the chief of police.
- C.** Data and images copied or downloaded from a LPR system and the city of Urbandale traffic camera recording system shall be the property of the Urbandale Police Department and shall be considered evidence. Accessing, copying, or releasing files or portions thereof, for non-law enforcement purposes is strictly prohibited unless specifically authorized by the chief of police or designee.
- D.** Data sharing with other law enforcement agencies shall be authorized by the chief of police, CID division commander or designee.
- E.** A documented review of LPR systems utilized by the department shall be completed annually by the investigation division commander or designee to ensure compliance with established policy and procedures.

V. Procedure: Training

- A.** Only department employees who have received approved training will be authorized to use and access LPR system and city of Urbandale traffic camera recording system data.
- B.** Training on the LPR systems and city of Urbandale traffic camera recording system shall include the following:
 - 1. Secure access and data use restrictions.
 - 2. Alert notifications and verification requirements.
 - 3. Department hotlist use and requirements.
 - 4. Procedures to download and transfer data and images to evidence.
 - 5. Search capabilities.
 - 6. Regional sharing functionality.
 - 7. Other system features as needed.

VI. Procedure: Data storage and retention

- A.** All images and data captured by the Flock LPR system shall be stored within the Flock LPR system for 30 days. After 30 days images and data shall be deleted from the LPR system.
- B.** All images and data captured by the city of Urbandale traffic camera recording system shall be stored for 60 days. After 60 days images and data shall be deleted from the system.
- C.** Data and images to be used as evidence in any criminal or traffic violation from LPR systems and city of Urbandale traffic camera recording system shall be downloaded and stored on the police production server. Retention shall follow department evidence and record retention schedules.

- D.** Only data and images associated with an incident or a criminal investigation shall be downloaded and saved on the police production server from a LPR system or the city of Urbandale traffic camera recording system.

Chapter 5: Law Enforcement Operations
Section 42: Criminal Investigations and Intelligence
Subsection 1: Administration



Policy/Procedure #: 1

Title: Criminal Investigations

CALEA Reference#: 42.1.1, 42.1.2, 42.1.3, 42.1.4, 42.1.5, 42.2.1, 42.2.2, 42.2.3, 42.2.8

I. Policy: Criminal Investigations

Criminal investigations are performed by uniformed officers as well as officers assigned to the Investigations Division. The guidelines established in this policy shall ensure a uniform response to investigative procedures during initial and follow up investigations.

II. Procedure: General

- A.** The Criminal Investigative Division (CID) of the Department shall provide an on-call detective able to respond twenty four (24) hours a day. The current schedule for the detective that is on-call shall be kept up to date with the communications center for immediate access by the Patrol Division.
- B.** The Patrol Division with the assistance of the Support Services Division shall have the responsibility of conducting all preliminary investigations into criminal incidents. CID may also conduct a preliminary investigation when circumstances warrant.
- C.** CID shall be responsible for follow-up on all criminal incidents.
- D.** The Patrol Division shall be responsible for follow-up investigations on the following:
 - 1.** All traffic related incidents excluding incidents where a motor vehicle was intentionally utilized to commit a criminal offense. Based on the seriousness of the investigation, the Patrol Division may request assistance from CID.
 - 2.** All animal violations (e.g. dog at large, vicious animal, animal bite). The Support Services Division may assist or lead investigations into animal violations.
 - 3.** Nuisance violations (e.g. barking dog, noise ordinance violations, illegal dumping).

- E. Detectives assigned to CID shall periodically attend patrol shift briefings to enhance relationships and provide an open exchange of information. When a detective attends a briefing, the patrol supervisor shall log their attendance in the notes section of the daily roll call sheet.

III. Procedure: Preliminary Investigations

- A. The preliminary investigation will be conducted by the officer initially assigned to the incident. The following steps will be used when an officer conducts a preliminary investigation:
 - 1. Observe all conditions, events, and remarks regarding the incident.
 - 2. Locate and identify witnesses.
 - 3. Maintain the crime scene, including protecting, identify, and securing possible evidence.
 - 4. When necessary, contact their immediate supervisor for guidance and direction.
 - 5. Interview the complainant/victim and any witnesses.
 - 6. Interview and/or interrogate suspects. Caution should be used when questioning suspects in a serious offense as assigned investigators may be hampered in their investigation if the suspect requests an attorney or refuses to answer questions.
 - 7. When needed, request a crime scene investigator and/or a detective for assistance.
 - 8. When appropriate, arrest suspect(s) in accordance with state and local statute violations.
 - 9. Report the incident completely and accurately on the appropriate report form.
- B. Detectives may assist the patrol officer with the preliminary investigation or may be directed by the Patrol Division supervisor or CID supervisor to assume the duties of the preliminary investigation.
- C. Officers and detectives may utilize the report room (#104) to take initial reports and conduct portions of their preliminary investigation. This room shall not be utilized to interview or interrogate suspects. The room is not monitored by video or audio equipment.

IV. Procedure: Follow Up Investigations

- A. The following steps shall be utilized when a detective conducts a follow-up investigation. Not all steps will be utilized for each investigation.
 - 1. Review and analyze all reports completed in the preliminary investigation to include all departmental records and laboratory examination results.
 - 2. Initiate a "second contact" with the principals involved in a case.
 - 3. Conduct additional interviews and interrogations.
 - 4. Seek additional information from uniformed officers, informants, other law enforcement agencies and any other source.
 - 5. Plan, organize, and conduct searches to collect physical evidence.
 - 6. Identify and apprehend suspects.
 - 7. Determine involvement of suspects in other crimes.
 - 8. Check criminal histories/backgrounds of suspects.

9. Arrange for dissemination of intelligence or other appropriate information.
 10. Prepare case for court.
 11. Assist in prosecution.
- B.** All relevant action taken during a follow-up investigation shall be recorded on a supplemental report. Additional reports may be necessary in order to complete a follow-up investigation. These reports include, but are not limited to:
1. Arrest report
 2. Property and evidence report
 3. Voluntary statements
 4. Consent to search.
 5. Advisement of rights.
 6. Results of examinations of physical evidence
 7. Statements by victims, witnesses, suspects
- C.** CID shall maintain an investigative checklist to be utilized for new detectives and during complicated investigations to ensure that critical tasks are not overlooked.

V. Procedure: Interview and Interrogation Rooms

- A.** The Department shall maintain two (2) interview/interrogation rooms (#112, #115). The rooms shall be equipped with a video camera connected to remote video/audio recording equipment and a telephone. The room shall also be equipped with an audible panic alarm. The video/audio recording equipment shall be housed in the adjacent observation room (# 114).
- B.** When interviewing a suspect or potential suspect in an interview room, the following safety procedures shall be in place:
1. Another officer shall be in the interview room or an employee shall be assigned to remotely view the interview within the Investigation Division or the adjacent conference room with the ability to offer assistance or summon assistance from other officers if necessary.
 2. Audible panic alarm to notify personnel of the need for immediate assistance.
 3. Officers shall document the identity of the employee utilized for security monitoring in their supplemental report.
- C.** Under most conditions, no more than two (2) officers should be present in the interview/interrogation room.
- D.** The placard outside the interview rooms shall indicate when the rooms are occupied.
- E.** Officers shall be allowed to carry weapons while utilizing the rooms as appropriate for their assignment.
- F.** Subjects being interviewed in the interview rooms shall be allowed access to the front lobby area for breaks and use of the restroom facilities. When the subject is in custody, any breaks or use of the restroom shall be observed by an officer or detective.

VI. Procedure: Criminal Investigations Case Management

- A.** A supervisor or designee in CID is responsible for assigning criminal cases received for follow-up investigations. The supervisor or designee shall determine the need for further investigation based upon solvability factors, available manpower and resources, and the probability of a successful resolution.
- B.** A CID supervisor shall assign a detective to every incident in which they have follow-up responsibility regardless of the current status of the incident. The detective assigned to the case will be considered the principal investigator. When a case needs more than one detective assigned, CID supervisors shall assign the appropriate number and designate who is the principal investigator.
- C.** The criteria to be used to determine whether or not a case shall continue to receive further investigative attention shall be established by the CID commander or designee with input from the assigned investigator. Cases may require different criteria to determine the need or extent of continued investigative efforts. The CID supervisors will review all cases in which CID has follow-up responsibility to determine appropriate current case status.
- D.** In addition to the criteria identified above, the following solvability factors shall also be considered when assigning cases for follow-up investigations:
 - 1.** Victim and/or witness availability and reliability.
 - 2.** Suspect and/or vehicle description or identity.
 - 3.** Physical evidence/property identifiable or traceable.
 - 4.** Available informant/intelligence information.
 - 5.** Information linking an incident to another incident or to an ongoing investigation.
 - 6.** Significant modus operandi (M.O.).
 - 7.** The quality of the preliminary investigation.
 - 8.** Outside law enforcement agency requests.
 - 9.** Belief that a crime may be solved with publicity and/or reasonable additional investigative effort.
 - 10.** Minor incidents which may attract more than usual publicity or public concern.
 - 11.** Command staff requests for follow-up of incidents of special concern.
 - 12.** Research conducted by the Department through the use of crime analysis and investigative intelligence files.
 - 13.** Research conducted by other law enforcement agencies such as the Iowa Law Enforcement Intelligence Network and Mid-States Organized Crime Information Center.
- E.** The CID commander has the responsibility of determining the amount of manpower and physical resources that will be committed to follow-up investigations.
- F.** CID supervisors shall review all follow-up reports as the case progresses to determine what point the investigation should be suspended due to investigative leads being exhausted.

- G.** CID supervisors shall log all case assignments in a case management system within the computerized records management system. The case management system shall be accessible to CID personnel, administrative services personnel and command staff as needed. The case management system shall contain the following information:
1. Case number
 2. Type of criminal activity
 3. Date case was assigned
 4. Case status
 5. Date of case status
 6. Investigator assigned
- H.** Written supplemental reports generated through follow-up investigations shall be submitted to their supervisor by the case investigator no more than sixty (60) days after assignment. After a review of the investigation, a supervisor may approve a change in case status or continuance of the investigation. No case status may be changed without the approval of a supervisor. Continuances of investigations may be granted by the CID supervisor for a maximum of thirty (30) days at which time another review shall occur to determine if additional investigation is warranted.
- I.** Utilizing the records management system all incidents shall be classified into one of the following categories:
1. Open. The case is active and needs additional investigation or follow-up work.
 2. Unfounded. Upon investigation, it is determined a criminal incident did not occur.
 3. Closed. Status used for noncriminal incidents such as impounds, accidents, found property, etc. when all work on the incident has been completed (e.g. found property has been returned to the owner or return of a runaway/missing person).
 4. Suspended. The case is open but is not actively being investigated. Cases may be suspended under the following conditions:
 - a. Absence of further leads or solvability factors that may bring the case to a successful conclusion with reasonable effort (no witnesses, no identifiable characteristics, serials, etc.).
 - b. Unavailability of investigative resources or leads.
 - c. Degree of seriousness combined with the above.
 5. Exceptionally cleared. Cases may be exceptionally cleared under the following conditions:
 - a. Death of the offender.
 - b. Prosecution declined by the prosecutor for other than lack of probable cause. (e.g. offense falls outside prosecution guidelines by virtue of value of loss, first-time offender etc.) or the investigation established probable cause for an arrest and supports the offense(s) being charged but the officer declined due to other

circumstances (i.e., witness issues, marginal evidence, clearance by other methods, etc.).

- c. Extradition denied.
- d. Victim refused to cooperate in the prosecution. This category may only be utilized if the offender is known.
- e. Juvenile/No custody. The handling of a juvenile without taking him/her into custody, but rather by oral or written notice given to the parents or legal guardian in a case involving a minor offense.
- f. Turned over to other agency.
- g. Arrest warrant issued. Status should be changed to cleared by arrest once the suspect is arrested.
- 6. Cleared by Arrest. Suspect(s) in the incident has been arrested.
- J. A supervisor shall approve all classifications listed above to ensure the report satisfies the criteria for the cessation of investigation.
- K. Each investigator, when assigned a case for investigation, will be provided a copy of the case report and will be required to maintain the copy, as well as copies of other documents generated during the investigation. This "investigative case file" shall be accessible to CID supervisory personnel but maintained in a secure location preventing disclosure to unauthorized personnel and the public. It is the investigator's responsibility to ensure all information uncovered during their investigation is transmitted to the original case file. Once the investigation is complete, the investigator shall transfer all relevant documents to the main case file. All investigative notes taken by the detective during the investigation shall be transposed to a supplemental report and the original note sheets destroyed. Once the investigation is complete and all documents have been transferred to the main case file, the investigator shall purge their investigative file.

VII. Procedure: Habitual Offenders

- A. Iowa Code defines a habitual offender as any person convicted of a class "C" or a class "D" felony, who has twice before been convicted of any felony in a court of this or any other state, or of the United States. An offense is a felony if, by the law under which the person is convicted, it is so classified at the time of the person's conviction.
- B. During arrest processing procedures, officers shall make inquiries into the suspect's criminal background by using NCIC (National Crime Information Center), CCH (Computerized Criminal History), Electronic Data Sharing System per Iowa Code. Upon receipt of this information the officer shall determine if a suspect meets the definition of a habitual offender. The officer shall file all NCIC, CCH, and other information relating to the suspects prior criminal background the main case file.
- C. Officers shall routinely contact and maintain a liaison with the appropriate prosecuting agency of such cases informing them of the habitual violator status and include this information in a supplemental report.
- D. On all indictable arrests, fingerprints will be forwarded to the FBI and the State of Iowa. When either agency notifies the Department that the arrestee's identity is false, records personnel shall forward the information

to the arresting officer for evaluation of criminal history, active warrants, or additional criminal charges. A supplemental report shall document the use of the false identity and the subsequent measures taken to correct the case file and any submissions to other agencies (e.g. FBI, DCI).

- E.** Detectives shall attend regularly scheduled area investigator's meetings with other agencies to share information concerning recent arrests of known habitual offenders.
- F.** Intelligence bulletins shall be generated and/or distributed to appropriate personnel by CID identifying recent arrests of known habitual offenders arrested in the area.

Chapter 5: Law Enforcement Operations
Section 42: Criminal Investigations and Intelligence
Subsection 2: Operations



Policy/Procedure #: 4

Title: Multi-Jurisdictional Investigative Task Forces

CALEA Reference#: 42.2.4

I. Policy: Task Force

The Urbandale Police Department shall participate in various investigative task forces to address specific crime problems in the community. The investigative task force shall have a specific focus and produce statistical information that allows administration to evaluate their success and need for continued operation.

II. Procedure: General

- A.** The Chief of Police shall determine the level of commitment to any long term multi-jurisdictional investigative task force.
- B.** The Criminal Investigation Division (CID) Commander shall be responsible for coordinating and planning all investigative task force activities directed by the Department or when requested to participate in outside agency investigative task force operations.
- C.** Long term task force participation shall be predicated on a clearly stated written agreement between the parties involved. Guidelines for the written agreement are as follows:
 - 1.** Purpose of the task force.
 - 2.** Defined scope of authority, responsibility concerning the type of criminal activity to be investigated and jurisdictional boundaries.
 - 3.** Identifying resources available for use in task force operations to include staffing, equipment, facilities, and funding.
- D.** To ensure officer safety, personnel assigned to a task force shall access to intelligence and officer safety information. If the task force is unable to provide this information internally, assigned personnel from the Department shall have access to departmental officer safety information and intelligence systems and personnel.
- E.** Personnel assigned to a task force shall continue to meet the requirements of the Department identification policy as stated in Chapter 3 Section 22.1.8 of

the Operations Manual. If the task force issues specific identification to members, Department personnel shall be required to carry and produced both forms of identification upon request. Personnel assigned to a task force shall be required to meet Department identification procedures in regards to clothing as outlined in Chapter 8 Section 74.3.1 (Execution of Criminal Process) of the Operations manual. The policy requires officers wear distinctive clothing and/or a police badge that clearly identifies they are a police officer when executing any criminal process. Personnel operating in a undercover or covert capacity that is approved by a supervisor shall be exempt from identification requirements.

- F.** The Chief of Police and/or the CID Commander shall be kept informed of the activities of Department employees under their command participating in a task force and the overall success of the task force. This is accomplished by periodic updates addressing the success of the individuals as well as the overall success of the task force. This may also include annual personnel evaluations on the employees involved. Based on these periodic updates, the Chief of Police or the CID Commander shall evaluate the results and the need for continued operation(s) of the employee assigned as well as overall Department participation.
- G.** When an employee of the Department is working under the direction of a supervisor(s) from another agency in a task force setting, the officer shall keep their respective CID supervisor informed of their activities and abide by the policies of Urbandale Police Department as well as the policies of the task force. If there are conflicting policies, the officer shall abide by the Urbandale Police Department policies and notify their departmental supervisor of the conflict.

Chapter 5: Law Enforcement Operations
Section 42: Criminal Investigation and Intelligence
Subsection 2: Operations



Policy/Procedure #: 5
Title: Polygraph
CALEA Reference#: 42.2.5

I. POLICY: Polygraph

The polygraph examination is a valuable investigative aid as used in conjunction with, not a substitute for, a thorough investigation. The polygraph may be employed, consistent with this policy, to verify, corroborate or refute statements; obtain additional investigative leads; narrow or focus criminal investigations; serve to screen candidates for positions with this and other criminal justice agencies; and, assist in conducting of internal police investigations among other authorized purposes.

II. Procedure: General

- A.** The polygraph is an instrument that records certain physiological changes in a person undergoing questioning in an effort to determine truth or lie. A polygraph simultaneously records a minimum of respiratory activity, skin resistance and conductivity, and cardiovascular activity.
- B.** A polygraph may be performed by an appropriately certified and qualified officer of the Department or by an appropriately certified and qualified law enforcement official from another agency. When performed by an outside agency, the polygraphist shall be required to meet the standards established in this policy.

III. Procedure: Requesting a Polygraph Examination:

- A.** Following approval by the Investigation Division Commander and/or the Chief of Police, investigators for the Department may request a polygraph examination from agency authorized polygraphists.
- B.** Polygraph examinations may be authorized when consistent with State of Iowa law and agency policy. Situations in which authorization may be requested and approved include but may not be limited to the following:
 - 1.** Requests from the prosecutor's office as part of an agreement with the defense attorney or for other investigative purposes.
 - 2.** An element of a background investigation of a candidate for a sworn or civilian position within the agency.

3. Requests from other authorized criminal justice agencies meeting the outside agency requirements, as established by the Chief of Police.
 4. Attempts to verify or reconcile statements of parents or guardians (e.g. in suspicious cases of missing or abused children) as well as witnesses or other individuals when alternative investigative means have been exhausted.
 5. Efforts to confirm or refute an allegation that cannot be verified or disproved by other evidence.
 6. Efforts to establish probable cause to seek a search warrant.
 7. As part of an administrative or criminal internal investigation of an employee in this agency or another criminal justice agency consistent with departmental policy.
- C. A polygraph shall not be used to verify a victim's allegation without sufficient grounds for suspecting the victim has given false or misleading statements.
- D. Requests for polygraph examinations from another law enforcement agency pursuant to an internal investigation must be in writing and approved by the Chief of Police or designee.
- E. Submission to a polygraph examination must be a voluntary action. Polygraph examinations shall not be administered without the person's written approval, waiver, or other instrument as required by law.
- F. No member of the Department shall be ordered to submit to a truth verification test such as a polygraph. Such tests may be offered by the Department in any administrative, civil, or criminal matter. If a polygraph is used, the results shall be used in accordance with federal and state laws. Refusal by the employee to submit to a polygraph will not form a basis for disciplinary action.

IV. Procedure: Preparing for the Polygraph

- A. The requesting officer is responsible for providing the polygraphist with all pertinent information concerning the case and for reviewing, clarifying, or elaborating on the information as the polygraphist may deem necessary. Case facts should be provided to the polygraphist at least twenty four (24) hours prior to the actual examination. Exceptions to the twenty four (24) hour rule may be allowed for special incidents as defined by the Criminal Investigation Division commander (e.g. homicides, robberies, etc.) or the Chief of Police. Case facts forwarded to the polygraphist may include but are not limited to the following:
1. Information obtained in the investigation that supports and justifies the use of the polygraph.
 2. Copies of crime/offense reports and investigative reports.
 3. Background information on the person to be examined, to include criminal record and possible motivation.
 4. Evidence available and withheld from the person.
 5. Any statements made by the person, complainant or witnesses to include alibis, newspaper articles and/or other general information concerning the case.

6. If the person is hearing impaired or does not speak English, the officer shall make arrangements for a sign language interpreter or translator as determined by the polygraph examiner.
7. Under most circumstances, officers shall not interrogate a person the day prior to the polygraph.
8. In any interrogation of a suspect who has agreed to or who may reasonably be asked to agree to a polygraph, officers shall not pursue questions that may reveal information only the perpetrator could know. This includes, but not limited to the following:
 - a. Method of entry.
 - b. Property taken.
 - c. Weapons or type of force used to commit the crime.
 - d. Evidence left at the scene.
 - e. Clothing worn by the suspect during the crime.
 - f. Unusual acts of the suspect during the crime.
 - g. Location from which property was taken.
- B. Officers shall not attempt to explain procedures that will be used in the examination but shall advise the person the procedures will be explained fully by the polygraphist. When possible, a "Polygraph Information Guide" shall be provided to the person with the actual time and date of the examination listed on the guide. The person may be advised of the following:
 1. The examination is voluntary.
 2. Results of the examination are not admissible in a court of law unless all parties agree in advance.
 3. Results of the polygraph examination taken alone do not provide substantiation for a criminal charge.
- C. If possible, the requesting officer shall report with the subject/suspect and any other authorized persons such as attorneys, parents, or legal guardians to the examination location and shall remain on hand until completion of the testing. The polygraphist shall be solely responsible for authorizing any person inside the examination or observation rooms.

V. Procedures: Conducting Polygraph Examinations

- A. Only fully trained, appropriately certified and qualified polygraphists or intern polygraphists under their direction are authorized to administer polygraph examinations.
- B. The polygraphist shall make such inquiries of the person's health, medical history and/or use of medications as necessary to determine his/her ability to take the examination. Polygraph examinations shall not be conducted on any person whom the examiner reasonably believes to be physically or emotionally unsuitable for testing. This may include, but not limited to persons with heart conditions, women who are pregnant, and individuals taking certain types of medication that may interfere with test results. When in doubt, the examiner may seek guidance from medical or psychological professionals as authorized by the Department and/or request the

examinee to obtain a medical certificate from an approved health care provider.

- C. The polygraphist shall not conduct a polygraph examination upon a person if it felt for any reason an unbiased examination cannot be given.
- D. When appropriate, the polygraphist shall read Miranda rights to the subject and explain the voluntary nature of the test. When required, the polygraphist shall obtain a signed consent prior to administering the examination as well as a signed waiver of Miranda rights.
- E. If requested by the person, an examination shall cease immediately.
- F. Prior to the test, the polygraphist shall explain the polygraph procedure to the person and prepare him/her for the examination.
- G. The polygraphist shall be responsible for preparing all questions used in the examination. Prior to the examination, each test question shall be reviewed with the person being tested.
- H. The polygraphist shall independently interpret the chart tracings and render an opinion on findings that include but are not limited to one of the following:
 - 1. Truthful.
 - 2. Lying.
 - 3. Indefinite.
- I. The polygraphist shall determine whether a second polygraph examination is necessary and appropriate. Under most circumstances, Indefinite findings shall be re-tested at a later time and date.

VI. Procedure: Pre-employment Examinations

- A. The polygraphist shall review all relevant applicant-screening reports, applicant personal history summaries, and any prior polygraph examination reports prepared by the Department before conducting the examination.
- B. Polygraph examinations shall not be used as the sole determination of suitability for employment. It shall be prohibited to eliminate a candidate based solely on the results of a polygraph examination. The results combined with other information (e.g. pre-test, test or post-test interviews) may be sufficient to eliminate a candidate from consideration.
- C. When utilizing a polygraph examination as part of the selection process for new employees, candidates shall be provided advance notice as to the areas from which the polygraph questions will be drawn.

VII. Procedure: Equipment and Record Keeping

- A. The polygraphist is responsible for the maintenance, safekeeping, and integrity of the polygraph equipment.
- B. The polygraphist shall provide summary activity or statistical reports as directed by the Chief of Police or his designee.
- C. Unless otherwise provided in this policy or by State of Iowa law, the polygraphist shall maintain copies of each polygraph report, together with polygraph charts and all allied papers, for a period of five (5) years and indefinitely in capital offenses.
- D. The results of all pre-employment examinations conducted by Department polygraphists including chart tracings, polygraph reports, and related

examination results shall be securely maintained by the Human Resources Department for the City of Urbandale.

- E. Tests and interviews shall be conducted in a clean, neat environment free from audible and visual distractions.
- F. Certificates, diplomas, etc. shall be displayed so as not to be in sight of persons during actual testing.
- G. Polygraphists shall be neat and well groomed, and will dress in a manner consistent with standards of the professional business community. Duty uniforms, badges, and other emblems of authority shall not be worn. This does not include departmental identification cards, where required.
- H. Service weapons shall be worn but shall not be openly displayed.

VIII. Procedure: Equipment

- A. Polygraphs used shall be of commercial manufacture and shall have no fewer than three (3) functioning recording channels.
- B. Calibration charts and/or maintenance logs shall be maintained at the instrument's location or with case files.
- C. Calibration checks of instruments shall be conducted at least once per month and whenever the instrument is moved to a different location.

IX. Procedure: Training and Professional Development

- A. Polygraphists shall be required to successfully complete a certified course of instruction by a recognized polygraph institution prior to conducting any polygraph examinations.
- B. Polygraphists are encouraged to participate in career development opportunities and are required to participate in professional recognized annual in-service training.
- C. Polygraphists are encouraged to maintain professional contact with their individual training institute and other area polygraphists.
- D. The polygraphist's training institute and Iowa polygraphist's organizations are considered to be the ideal locals for annual in-service training.

Chapter 5: Law Enforcement Operations
Section 42: Criminal Investigation and Intelligence
Subsection 2: Operations



Policy/Procedure #: 6
Title: Confidential Informants
CALEA Reference#: 42.2.6

I. Policy: Confidential Informants

In many cases, a successful investigation cannot be conducted without the use of confidential informants. While the use of confidential informants is an effective investigative tool, it can be undermined by the misconduct of the confidential informant or the officer utilizing the informant. It shall be the policy of the Urbandale Police Department to take precautions by developing sound informant control procedures.

II. Procedure: Informant Files

- A.** A confidential informant shall be defined as a person not employed as a law enforcement officer and is utilized by a law enforcement agency for active intelligence gathering activity. This person shall freely and voluntarily provide information about criminal activities.
- B.** The Criminal Investigation Division (CID) shall be responsible for developing and maintaining confidential informant files and an indexing system. All confidential informant files shall be maintained in a secure area with restricted access.
- C.** The confidential informant files shall be utilized in order to:
 - 1.** Provide a source of background information on the informant.
 - 2.** Provide a complete history of information received from the informant.
 - 3.** Enable review and evaluation by the appropriate supervisor of information provided by the informant.
 - 4.** To minimize incidents that could be used to question the integrity of investigators or the reliability of the informant.
 - 5.** Provide a record of all currency transactions involving the informant (buys, expenses, payments, etc.).

- D. A file shall be maintained on each informant used by officers. Each file shall be coded with an assigned informant control number and shall contain the following information:
 - 1. Informant's name.
 - 2. Name of the officer initiating the use of the informant.
 - 3. Informant's photograph, prints and criminal history data.
 - 4. Briefs on information furnished by the informant and its subsequent reliability.
 - 5. Signed agreement.
- E. An informant history summary, coded with the informant control number, shall be prepared to correspond to each informant file and include the following information:
 - 1. Pertinent identification data (date of birth, social security number, height, weight, tattoos, etc.).
 - 2. Current address.
 - 3. Current employer.
 - 4. Phone numbers.
 - 5. Vehicles.
- F. In order to protect the identity of confidential informants, they shall be referred to by their assigned number in all case reports and documentation outside of the confidential informant file. Officers shall be conscious when referring to confidential informants in reports using gender neutral terms. Only when requested by the Chief of Police, a CID supervisor, the prosecuting attorney, or a court of competent jurisdiction shall the name of a confidential informant be revealed.
- G. Access to the confidential informant files shall be restricted to the Chief of Police, CID supervisors, and the supervisor in charge of the Alcohol/Tobacco compliance program. Personnel may review a confidential informant file with good cause and upon approval of an above listed supervisor.

III. Procedure: Use of Informants

- A. Before using an individual as a confidential informant an officer must receive initial approval from a supervisor. When the confidential informant is cooperating due to pending criminal charges, approval to use the confidential informant shall be obtained from the appropriate prosecuting attorney's office prior to use. After initial approval, an officer shall open an informant file as established in this policy.
- B. Officers shall compile sufficient information through a background investigation in order to determine the reliability and credibility of the individual.
- C. If a confidential informant file is established and it is later determined the confidential informant is unsuitable for use, their file shall be marked accordingly and their status inactive.

- D. Any officer wishing to use a confidential informant deemed unreliable or unsuitable in the past shall receive prior approval from the CID Commander prior to use.
- E. Juveniles shall only be used as confidential informants if the youth's parents or guardian consents to their use in writing and all parties sign a waiver of liability reference their involvement as a confidential informant. Juveniles utilized for the Alcohol/Tobacco compliance program shall sign all appropriate forms and waivers provided by the program prior to use.

IV. Procedure: Guidelines for Handling Informants

- A. All confidential informants are required to sign and abide by the provisions of the Department's confidential informant agreement. The officer utilizing the confidential informant shall discuss each of the provisions of the agreement with the confidential informant.
- B. It shall be emphasized to the confidential informant they are not law enforcement officers. They have no arrest powers and are not permitted to conduct searches or seizures, nor will they carry weapons.
- C. Except at the direction and control of an officer as part of an investigation, confidential informants found engaging in any illegal activity shall be arrested (if possible) and their cooperation with the Department terminated. They shall receive no special legal consideration.
- D. Confidential informants and officers managing the informant shall ensure they do not engage in entrapment.
- E. No member of the Department shall maintain a social relationship with a known confidential informant while on or off duty or otherwise become personally involved with confidential informant. Members of the Department shall not solicit, accept gratuities, or engage in any private business transaction with an informant. Exceptions may be granted for confidential informants utilized for alcohol/tobacco compliance as they may be relatives or friends of an officer.
- F. Two officers shall to be present when meeting with any confidential informant. Any deviation from this practice shall be approved by a supervisor. Officers are prohibited from meeting alone with confidential informants of the opposite sex.
- G. Officers shall not make promises that will not or cannot be kept.
- H. Confidential informants shall never be allowed to dictate the direction of an investigation and shall only be informed of case details crucial to their successful cooperation.
- I. Officers and CID supervisors shall ensure each informant is handled in accordance with all court mandates, rulings, or policies, regulating their use.
- J. When utilizing an informant, an officer shall take all necessary precautions to ensure their safety to include but not limited to the following:

1. Use of an informant's control number in lieu of their name and the use of general neutral terms in all reports.
2. Actively monitoring any use of the informant by utilizing a covert transmitting device.
3. Physical surveillance by multiple law enforcement personnel during any use of the informant with the ability to respond if the situation becomes life threatening for the informant.
4. Cautioning the informant not to inform anyone they are cooperating with law enforcement.
5. When able, completing case investigations in a manner that will protect the identity of the informant upon arrest of an offender.
6. Specific and clear instructions to the informant prior to any use that may include controlling meeting locations, minimalizing time of the operation, leaving the operation if necessary, and how to summon assistance from law enforcement.

V. Procedure: Use of Probationers and Paroles

- A. Police officers shall not allow a parolee or probationer to become a confidential informant without prior approval of a CID supervisor, and the appropriate prosecuting attorney's office. When applicable, the appropriate prosecuting attorney's office shall obtain approval for a probationer to cooperate from the sentencing court. When applicable, the appropriate prosecuting attorney's office shall obtain approval for a parolee to cooperate from the Department of Corrections. The use of parolees and probationers as confidential informants can only be justified by the most compelling circumstances.
- B. Officers shall not make any promises, threats, or inducements to parolees or probationers for the purpose of involving them in any active intelligence gathering activity.
- C. Federal parolees shall not be used as informants without a waiver from the Federal Parole Commission.
- D. Federal probationers shall not be used as informants without a waiver from a Federal Court.
- E. None of the above shall be construed to eliminate the use of parolees and probationers from providing general information as to criminal activities freely and voluntarily.

VI. Investigation Expense Fund

- A. CID shall maintain close control over all investigative expense fund monies used by the Department and ensure all funds are used for authorized purposes. The investigative expense fund shall be maintained in compliance with the requirements governing cash accounts as stated in Chapter 2 Section 17.4.1 (Accounting) of the Operations Manual.

- B.** The investigative expense fund shall be stored in a secure area with only CID supervisors having access. The currency in the expense fund shall only be accessed when two employees are present.
- C.** The CID commander shall have the following responsibilities with respect to the Department's investigative expense fund:
 - 1.** Maintenance of the fund in accordance with appropriate laws and internal controls.
 - 2.** Proper disbursements and deposits.
 - 3.** Quarterly audits as established by Chapter 2 Section 17.4.1 of the Operations Manual.
 - 4.** Maintenance of all documentation of relevant fund transactions.
- D.** CID supervisors shall make disbursements from the investigative expense fund to authorized personnel for the following purposes:
 - 1.** Payments made directly to confidential informants.
 - 2.** Funds for the purchase of stolen property, illegal drugs, contraband, and other criminal evidence.
 - 3.** Purchase of food and beverages for a confidential informant.
 - 4.** Expenditures for authorized undercover operations.
 - 5.** Flash or front money.
- E.** Criteria for payment of investigative expense funds to confidential informants shall be determined on a case by case basis by a CID supervisor. Payment criteria may include but not be limited to the following:
 - 1.** Usefulness of the information.
 - 2.** Time commitment of the confidential informant.
 - 3.** Amount of information provided.
 - 4.** Whether the confidential informant is receiving any other benefit such as consideration on pending charges.
- F.** Investigative expense funds and transaction records shall be stored in a secure location. Access shall be restricted to CID supervisors in accordance with acceptable standards of accountability and security as established by the CID commander.
- G.** Prior to the issuance of any money from the investigative expense fund, an officer shall present a cash account receipt documenting the use of investigative funds. This receipt shall briefly state the intended use and include an informant number, if applicable.
- H.** If use of the investigative expense fund is approved, a CID supervisor may issue the funds documented on the cash account receipt acknowledging funds were requested and received.
- I.** All officers utilizing investigative funds shall prepare a written report accounting for all monies withdrawn from the fund as soon as practical. The written report with all supporting documentation shall be submitted to the appropriate supervisor for review and approval.

- J. In the case of payments to confidential informants, a signed receipt of payment including a witness signature shall be required.
- K. When able and appropriate, officers utilizing investigative fund monies shall obtain a receipt from the person or business receiving the funds unless such action would jeopardize the operation.
- L. All unexpended funds shall be returned the investigative expense fund as soon as practical. The funds checked out for use shall be kept secure at all times and shall not be taken home by the officer. When unused funds are returned, they shall be documented on the cash account receipt acknowledging their return

VII. Procedure: Task Force Informants

- A. Officers from the Department assigned to long term criminal investigative task force operations shall utilize the policies and procedures established by each respective task force for handling confidential informants and their respective investigative expense funds.
- B. If the policies, procedures, and practices of the respective task force do not meet the general requirements of this policy, the assigned task force officer shall notify their chain of command for resolution.

Chapter 5: Law Enforcement Operations
Section 42: Criminal investigation and Intelligence
Subsection 2: Operations



Policy/Procedure #: 7
Title: Cold Case Investigations
CALEA Reference#: 42.2.7

I. Policy: Cold Case Investigations

It is the policy of the Urbandale Police Department all major cases be investigated until solved including all crimes that carry no statute of limitations.

II. Procedure: Classification

- A.** A cold case is any criminal investigation into a major case that has not been solved for a period of at least one year and has been suspended from active investigation. An investigation may turn into a "cold case" due to a lack of current technology to analyze evidence, uncooperative witnesses, or lack of investigative leads. The CID commander shall maintain a current list of all investigations classified as "cold cases."
- B.** Upon receiving a major case, the assigned detective shall investigate all available leads until the case is solved. After a period of one year, if no new information is received and all leads are exhausted, the case will be classified as a cold case and remain "open" but suspended from active investigation until new information is developed.
- C.** If an investigation meets the criteria to be classified as a cold case while assigned to an investigator, the investigator shall remain on the case for the duration of their tenure in the Criminal Investigation Division (CID) or until the CID commander chooses to reassign the case. If the assigned investigator transfers from CID, the case will be reassigned at that time.
- D.** Any request for outside access to cold case investigation(s) shall only be approved by the CID commander or the Chief of Police.

III. Procedure: Evaluation Criteria

- A.** The CID commander shall review cold cases on an annual basis. This review shall be based on, but not limited to:
 - 1.** Legal considerations such as changes to the statutes of limitation.

2. Technological considerations such as the nature and condition of the evidence and the advancement of new technology in solving a crime.
 3. Practical considerations such as the availability of witnesses, age of the case, etc.
 4. Resource considerations such as time, money, and personnel available for investigation and forensic analysis.
- B.** If the case is reviewed and not reassigned for investigation, the CID commander shall document in the case file the date of the review and the evaluation criteria utilized to make the decision. A copy of this review shall be provided to the Chief of Police.
- C.** If a case is reviewed and is reassigned for investigation, the CID commander shall reassign an investigator based on the following criteria:
1. Experience of the investigator.
 2. Investigator's area of expertise and training.
 3. Investigator's current caseload.
 4. Availability of witnesses, suspect(s), and original investigator(s).

IV. Procedure: Recording Investigative Actions and Activities

- A.** When a cold case is reassigned, the CID commander shall review with the assigned investigator all areas of the case that warrant action. At a minimum, the assigned investigator shall address these areas of concern during their reassigned investigation.
- B.** Investigators assigned to a cold case shall review the original case files and determine if there is any new information or technology available that would provide new leads.
- C.** Investigators shall document all activity including review of the existing case file on supplemental reports. Copies of all supplemental reports shall be forwarded to the CID commander for review.
- D.** Upon completion of a reassigned investigation, the CID commander shall provide the Chief of Police a summary of investigative action and current disposition of the case.

Chapter 5: Law Enforcement Operations
Section 42: Criminal investigation and Intelligence
Subsection 2: Operations



Policy/Procedure #: 9

Title: Line-ups and Show-ups

CALEA Reference#: 42.2.9, 42.2.10

I. Policy: Line-ups and Show-ups

It is the policy of the Urbandale Police Department to conduct photographic lineups and show-ups in a manner that reduces the risk of mistaken identification and aids in the detection and conviction of the guilty. Officers shall adhere to the procedures set forth in this policy to maximize the reliability of witness identifications, minimize identification of innocent persons, and produce evidence that is reliable and conforms to established legal procedure.

II. Procedure: Definitions

A. Photographic Line-up: An identification procedure in which a photograph of the suspect of an offense and additional photographs of persons not suspected of the offense are displayed to an eyewitness for the purpose of determining whether the eyewitness identifies the suspect as the offender.

B. Physical Line-up: A physical line-up is the placing of a suspect among people not suspected of committing the crime and asking the eyewitness if they can identify the offender. The Urbandale Police Department does not conduct physical line ups.

C. Show-up: An identification procedure in which an eyewitness is presented with a single suspect within a short time following the commission of a crime for the purpose of determining whether the eyewitness identifies the individual as the offender.

III. Procedure: Photographic Line-ups

A. The following procedure shall be utilized when using a printed lineup or the line-up software program. When using a printed line-up, the photographic line-up form is required.

- 1.** Include only one suspect in each identification procedure.

2. Select a photograph of the suspect that resembles the suspect's appearance at the time of the incident.
3. Select other persons to be included in the line-up that resemble the suspect in significant features. If utilizing the line-up software program, the software program will produce an array of non-suspect photographs based on the parameters entered.
4. Include a minimum of five non-suspects per identification procedure. Complete uniformity of features is not required. Officers shall avoid using persons that too closely resemble the suspect.
5. If there is more than one witness, each witness will be shown the line-up separately. Witnesses will not be permitted to communicate with each other until after the line-up procedure has been completed.
6. If a witness has previously viewed a photographic line-up in connection with the identification of another person suspected of involvement in the offense, the non-suspects in the line-up shall be different from the ones used in any prior line-ups.
7. When showing a photographic line-up to a witness, the following information shall be provided:
 - a. Inform the witness not to assume the offender's picture is included among the photographs.
 - b. Inform the witness hair style and length as well as other characteristics may have changed since the photographs were taken.
 - c. Inform the witness they are under no obligation to choose a photograph.
 - d. Inform the witness not to tell any other witnesses they have or have not been able to identify anyone.
8. Officers must not, by word or gesture, make suggestion to any witness concerning the guilt or innocence of a suspect in any identification procedure. Witnesses making inquiries about an officer's opinion shall be informed of this restriction.
9. Document the level of confidence expressed by the witness in their identification of suspect. Have the witness describe how they know they have identified the right person.
- B. When conducting a line-up, the identification shall be video and/or audio recorded. Exceptions to recording may be granted by a supervisor. The line-up software program will audio and video record the entire identification procedure.

IV. Procedures: Show-ups

- A. An officer may arrange a show-up between a witness and a suspect when there is reasonable suspicion to believe the suspect committed a crime and the detention occurs soon after the crime was committed. Officer

conducting a show-up are required to use the Show-up form to guide them through the proper procedures.

- B.** A suspect cannot be detained for longer than a reasonable period of time to confirm or refute whether the suspect is the offender.
- C.** Officers at the scene and in contact with a witness shall obtain a detailed description of the offender before the suspect is shown to the witness. The witness must advise the officers they will be able to recognize the person who committed the crime prior to the show-up. Once confirmed they will be able to identify the suspect, the officer shall inform the witness they have detained someone matching the description provided and would like them to confirm if the person detained is the suspect they have described.
- D.** The suspect shall be inconvenienced as little as possible during a detention and show-up. This means the witness shall be brought to the suspect. The suspect shall not be taken to the witness if there is a reasonable alternative. Police vehicles shall be utilized to transport the witness to the show-up location.
- E.** When possible, avoid any indications the suspect is in custody (handcuffs, placement in the back seat of the patrol car, Suspect in a frisk position, etc.); however, officers may take any action that is reasonable for their safety. If the suspect is handcuffed, take measures to conceal this fact from the witness when possible.
- F.** Officers shall avoid saying anything to the witness just prior to the identification that might be considered suggestive (e.g. we think we caught the guy, the suspect has victim's property, etc.). Additionally, officers shall avoid saying anything suggestive after the identification (e.g. you picked the right or wrong person, etc.). This could have a corrupting effect on all subsequent identifications and result in their suppression.
- G.** Show-ups shall not be conducted with more than one witness present at a time. Witnesses shall not hear others accounts as they may be influenced by the information. If there is more than one witness, the show-up must be conducted separately for each witness, and witnesses shall not be permitted to communicate before or after any show-up regarding the identification of the suspect. The same suspect shall not be presented to the same witness more than once. Multiple witnesses shall be transported to the show-up separately.
- H.** When there are multiple suspects, they must be separated and subjected to separate show-up procedures.
- I.** Document the level of confidence expressed by the witness in their identification of suspect. Have the witness describe how they know they have identified the right person.
- J.** In emergency circumstances, such as when a witness or a suspect is in danger of imminent death, an immediate show-up may be conducted. In

these situations, time and location limitations contained in the preceding guidelines may be disregarded. If there is doubt about the need for an emergency show-up, a supervisor should contact the appropriate prosecuting attorney for guidance.

- K. Once a suspect has been detained based on probable cause, they have no right to refuse to participate in a show-up and no right to have an attorney present.
- L. When possible, show-ups and the results shall be documented utilizing the in-car and/or body worn video system.

V. Procedure: Documenting Line-ups and Show-ups

- A. All information regarding photographic line-up identification procedures shall be documented. The documentation shall include but not be limited to the following:
 - 1. Identify the person preparing the photographic line-up.
 - 2. Document the names of all persons and/or photographs used.
 - 3. If the witness identifies someone as the suspect, have the witness circle the person they have identified and sign/ initial the line-up next to the photograph.
 - 4. Document how the witness described they knew the person they have identified is the right person.
 - 5. Note confidence statements made by the witness. Do not suggest they use percentages.
 - 6. Record identification and non-identification results.
 - 7. Document time, date and location of identification.
 - 8. Document if the witness wear glasses or contacts and did they have them on at the time of the line-up.
- B. Document to whom the photographic line-up was shown on the top of the actual photographic line-up including date and time. Also include the information for the officer presenting the line-up.
- C. When utilizing a printed line-up, place a copy of the line-up in the case file and place the original document into evidence.
- D. If utilizing the line-up software program, the video file of the identification process shall be saved to the police production server.
- E. All information regarding show-up procedures shall be documented in the officer's report. The reports shall include but not be limited to the following:
 - 1. Document the lighting conditions (e.g. spotlight, flashlight, full sun, cloudy).
 - 2. Note the approximate distance of the witness to the detained person.
 - 3. Document where the witness was during the identification (e.g. backseat of patrol car).
 - 4. Estimate the length of time the witness looked at the subject before making the identification.

5. Document how the witness described how they knew the person they have identified is the right person.
6. Note confidence statements made by the witness. Do not suggest they use percentages.
7. Document officers and other persons present during the show-up.
8. If clothing is identified, it may be taken as evidence.
9. Record identification and non-identification results.
10. Document time, date and location of identification.
11. Document if the witness wear glasses or contacts and did they have them on at the time of the show-up.

Chapter 5: Law Enforcement Operations
Section 43: Vice, Drugs and Organized Crime
Subsection 1: Administration and Organization



Policy/Procedure #: 1

Title: Vice, Narcotics, and Organized Crime

CALEA Reference#: 43.1.1, 43.1.2, 43.1.3, 43.1.4, 43.1.5

I. Policy: Vice, Narcotics, and Organized Crime

The Urbandale Police Department recognizes the serious nature of vice, narcotics and organized crime offenses, which constantly threaten the social, financial, health and well-being of a community. It is the policy of the Department that every member shall share in the responsibility to suppress all forms of vice, narcotics, and organized crime activities. Departmental efforts shall be directed toward identifying persons engaged in these types of crimes, gathering intelligence on the individuals involved, and assisting in the prosecution of such offenders.

II. Procedure: Responsibilities

A. The Criminal Investigation Division (CID) commander shall have the primary responsibility for the administration, coordination, and direction of departmental activities concerning narcotics, vice, and organized crime to include:

- 1.** Identifying and investigating activities involving narcotics, vice, and organized crime.
- 2.** Intelligence gathering concerning narcotics, vice, and organized crime activities.
- 3.** Disseminating narcotics, vice, and organized crime information (e.g. intelligence bulletins, roll call briefings, etc.) to other department members and divisions.
- 4.** Maintaining a liaison with other law enforcement agencies engaged in narcotics, vice, and organized crime suppression (e.g. investigator's attendance at local area weekly and monthly intelligence meetings, etc.).

B. CID is not limited to using the resources of the Department. They may also seek assistance from other local law enforcement agencies, the Iowa Department of Public Safety, and federal law enforcement agencies. The

Department shall work with all law enforcement agencies to maximize resources and avoid duplication of investigative efforts.

- C. Supervisors and officers assigned to narcotics, vice, and organized crime efforts shall include but not be limited to unlawful activities by persons or groups engaged in or promoting the following:
 - 1. Illegal possession and trafficking of controlled substances and weapons.
 - 2. Supplying illegal goods and services such as gambling and prostitution.
 - 3. Gang activity.
 - 4. Loan sharking.
 - 5. Racketeering.
- D. When an employee of the Department is working under the direction of a task force, the officer shall keep their respective supervisor informed of their activities and abide by the general requirements of this policy as well as the policies of the task force. If the policies are conflicting, the officer shall abide by the Urbandale Police Department policies and notify their departmental supervisor of the conflict.

III. Procedure: Receiving and Processing Complaints

- A. When an officer of the Department receives information of narcotics, vice, or organized crime activity, they shall use the following procedures:
 - 1. The officer shall be required to complete a task force lead sheet containing the information received in the complaint. A complaint shall be any information received from a citizen or from an outside law enforcement agency.
 - 2. The lead sheet will be forwarded to the CID commander for review.
 - 3. The CID commander shall forward the complaint to the supervisor assigned to the MINE task force. The supervisor shall assign the complaint for a follow up investigation or if outside the jurisdiction of the task force, forward the complaint to the appropriate agency for follow up. A record of all complaints, including complaints forwarded to other agencies for follow up shall be maintained by the supervisor assigned to the MINE task force and include the following:
 - a. Tracking Number
 - b. Detective assigned or agency information forwarded to
 - c. Date received
 - d. Date assigned
 - e. Disposition
 - f. Date of disposition
 - 4. The supervisor assigned to the MINE Task force shall be responsible for the timely investigation of all vice, narcotics, and organized crime complaints received by the Department. If the information received is reference activity outside the jurisdiction of the task force, the

supervisor shall ensure the information is forwarded to the appropriate agency for investigation in a timely manner.

- B. The supervisor assigned to the MINE task force shall produce a quarterly report for the CID commander and the Chief of Police summarizing activity on all vice, narcotics, and organized crime complaints as well as completed and current investigations occurring within the City of Urbandale or with ties to Urbandale.

IV. Procedure: Maintenance of Narcotics, Vice, and Organized Crime Records

- A. Active narcotics, vice, and organized crime investigations shall be secured in separate files from other police records and have restricted access. These files shall be maintained at the MINE Task Force.
- B. Once a complaint is fully investigated, it shall be filed in one of the following areas:
 - 1. Original case file (Records Division)
 - 2. Intelligence Files (intelligence information)
- C. All complaint records shall be purged based on the following:
 - 1. If entered in the main case file in police records, the information shall be purged in accordance with procedures established in Chapter 9 Section 82.1.1(Records) of the Operations Manual.
 - 2. If entered in the intelligence files the information shall be purged in accordance with the procedures establish in Chapter 5 Section 40.2.1 (Intelligence Information) of the Operations Manual.

V. Procedure: Investigative Expense Fund

- A. The Department shall budget annually for funds to cover expenses incurred to conduct investigations. The fund shall be managed as established in Chapter 5 section 42.2.6 (Confidential Informants) and Chapter 2 section 17.4.1(Accounting) of the Operations Manual.
- B. When assigned to a task force, officers shall follow the specific prescribed procedures for managing the task force investigative fund.

VI. Procedure: Undercover & Surveillance Equipment

- A. All undercover and surveillance equipment owned by the Department shall be stored and maintained in working condition by CID.
- B. Inventory and inspection of undercover and surveillance equipment shall be conducted as prescribed in Chapter 2 Section 17.5.1(Agency Property) of the Operations Manual.
- C. When undercover and surveillance equipment is assigned to CID rather than a specific officer and the equipment is being deployed, a log shall be maintained to record authorization, distribution, and use. The log shall contain the following information:
 - 1. Case number
 - 2. Officer

3. Equipment description (type and if multiple of the same item, serial number).
4. Description of use
5. Authorizing supervisor or designee.
6. Date issued
7. Date returned.

VII. Procedure: Covert Operations

- A. When deemed appropriate, the Department will conduct covert operations in an attempt to gather evidence leading to the arrest and prosecution of individuals involved in narcotics, vice, organized crime, and other types of crimes.
- B. Covert operations may include decoy, undercover, and surveillance activities designed to infiltrate and establish an association with those individuals suspected of being engaged in criminal activity.
- C. Covert operations will be coordinated by a supervisor and operated in a legitimate manner seeking advice from the appropriate prosecuting attorney.

VIII. Procedure: Surveillance Guidelines

- A. Surveillance operations shall not be initiated without the approval of a supervisor. During the approval process, the supervisor shall determine if the surveillance operation requires a supervisor be present.
- B. No surveillance operation shall be initiated unless there is a strong suspicion the person or location to be placed under observation is involved in criminal activity. The appropriate supervisor or designee shall be responsible for formulating a plan and shall take the following actions:
 1. An analysis of the type of incident(s) and victim(s).
 2. Identification of probable offender(s), their habits, associates, vehicles, modus operandi, etc.
 3. Time limitations.
 4. The determination of operational procedures for observation, surveillance, search warrants, arrests, and high risk entries.
 5. Familiarizing participating officers with the target, vantage points for observation, and if appropriate, the preparation and distribution of diagrams, photographs, etc.
 6. Ensuring adequate officers are available for officer safety and identifying all participating personnel to all members involved in the operation.
 7. Vehicle assignments.
 8. Determination of communication channels or other communication methods.
 9. Alternate plan should an arrest become necessary.
 10. Manpower assignment and rotation.
 11. Availability of expense funds for participating members.

12. Legal considerations.
13. Designating a single person as supervisor and/or coordinator.
14. Designating personnel responsible for documenting the activities observed during the surveillance.

- C. If pertinent observations are made during the surveillance, the case officer shall document the observations in a supplemental report to include:
1. Date and time of observation
 2. Personnel observing each specific activity
 3. Activity observed
 4. Descriptions of persons, vehicles, and locations.

IX. **Procedure: Undercover and Decoy Operation Guidelines**

- A. Decoy or undercover operations shall not be enacted without the approval of a supervisor.
- B. Supervisory personnel shall be present during decoy and undercover operations. Exceptions may be granted by a supervisor based on the circumstances of the investigation (e.g. alcohol/tobacco compliance checks).
- C. A supervisor is responsible for briefing the on duty patrol supervisor reference any decoy or undercover operation that will likely involve patrol personnel.
- D. All undercover or decoy operation shall be coordinated by a supervisor who will ensure safety of all involved by completing and reviewing an operations plan with all participants. The following shall be taken into consideration:
1. The analysis of the type of incident(s), victim(s), and crime location.
 2. The identification of probable offenders, their habits, associates, vehicles, modus operandi, etc.
 3. The use of informants to gain as much knowledge about the suspect(s) as possible.
 4. Supplying the appropriate equipment and expense funds for involved members.
 5. Ensuring adequate officers are available for officer safety and identifying all participating personnel to all members involved in the operation.
 6. Assuring involved members are familiar with the target area and analyze points for observation including the preparation and distribution of diagrams, photos, etc., to members assigned to the operation.
 7. Developing an arrest plan in the event an arrest becomes necessary. The circumstances of each particular operation vary and the possibility of changing situations occurring during the operation shall be considered and evaluated.
 8. Vehicle assignments.

9. Providing for communication channels or other communication methods, including emergency communications.
 10. Discussing legal, public and political ramifications of the operation and preparing for same.
 11. Supplying officers with false identity/credentials and ensuring the confidentiality of any such false identity.
- E. Upon completion of an undercover or decoy operation, the case officer shall be responsible for documenting all activity occurring in a supplemental report.

X. Procedure: Search Warrant and Raid Guidelines

- A. Search warrants/raids shall not be initiated without the approval of a supervisor and the appropriate prosecuting attorney.
- B. Search warrants/raids shall not be conducted unless a supervisor or designee is on the scene to provide direction.
- C. Prior to initiation, all raids or search warrants shall be coordinated by a supervisor who is responsible for formulating a plan taking into consideration the following aspects of the activity:
 1. Determining operational procedures by completing an operational plan for the execution of the search warrant/raid including use of the S.E.R.T. Risk Analysis/Threat Assessment for Planned Operations as stated in Chapter 5 Section 46.2.2 (SERT) of the Operations Manual. In addition to completing the above documents, the supervisor or designee should consider the following when appropriate:
 - a. Approach and escape/exit avenues.
 - b. Entry techniques.
 - c. Perimeter and interior security.
 - d. Provisions for body armor, shields, and other officer survival tactics.
 2. Ensuring an adequate number of officers and proper equipment are available for the operation.
 3. Preparing and distributing appropriate diagrams, available photos, etc. of:
 - a. Involved suspects and other persons
 - b. Target area.
 - c. Interior and Exterior building layout.
 4. Assuring all involved officers are familiar with the tactical plan(s), intended target area, offender(s), and likelihood of resistance.
 5. Assignment of vehicles.
 6. Determining communication channels or other communication methods.
 7. Assuring the proper use of force and arrest techniques is discussed with participating personnel.
 8. Selection of and provisions for communication with support units, paramedic ambulance crews, evidence technician, etc.

- D.** When entry is gained and the situation is stable, the on-scene supervisor is responsible for the following:
 - 1.** When necessary, summoning medical assistance.
 - 2.** Assigning members to the following duties:
 - a.** Prisoner security.
 - b.** Room searches.
 - c.** Collection, inventory, and photography of evidence. When practical an evidence technician may be utilized.
 - d.** Prisoner transport.
 - e.** Removal of all equipment, exit, and security of the premises upon completion of the operation.
- E.** The supervisor coordinating the search/raid is also responsible for assuring the above elements are thoroughly documented in the appropriate report. Additionally, the supervisor may review the actions completed and hold an after action review with personnel involved.

Chapter 5: Law Enforcement Operations
Section 44: Juvenile Operations
Subsection 1: Administration



Policy/Procedure #: 1

Title: Juveniles

CALEA Reference#: 44.1.1, 44.1.2, 44.1.3, 44.2.1, 44.2.2, 44.2.3

I. Policy: Juveniles

The Urbandale Police Department is committed to the development, implementation, and support of programs designed to prevent and control juvenile delinquency. The responsibility for participating in or supporting the Department's juvenile initiatives is shared by all divisions and personnel. It shall be the Department's policy to refer juveniles to both public and private social service agencies within the limits of Iowa Code Chapter 232, in order to direct non-serious juvenile offenders and/or troubled juveniles away from the formal juvenile justice system. This will enable the Department to utilize local resources in the solving of local community problems.

II. Procedure: Responsibility

- A.** The Criminal Investigation Division (CID) shall be responsible for any needed follow up investigation of criminal incidents involving juveniles.
- B.** The Support Services Division shall be responsible for follow-up investigations of criminal incidents involving juvenile offenders occurring at the Urbandale School systems. Based on the scope of the investigation Support Services may request assistance performing investigations from CID and the Patrol Division.
- C.** The Support Services Division shall be responsible for design and implementation of programs intended to prevent and control delinquent behavior by juveniles.
- D.** The Support Services Division commander shall submit an annual review and evaluation of all enforcement, prevention, and education programs relating to juveniles to the Chief of Police for approval. The review shall include:
 - 1.** Recommendations to continue or end existing programs.
 - 2.** Recommendations to add new programs.

3. Recommendations to modify existing programs due to changes in the juvenile justice system or the Iowa Code.
- E. In the event of any significant changes in state law, juvenile court procedures, etc., the Support Services Commander shall forward input and recommendations for any needed changes to Department policy and procedure to the Chief of Police.
- F. All officers in the Department are able to detain a juvenile offender for a criminal act based on probable cause and make a referral to juvenile or adult court as established in this policy. All officers shall maintain a working knowledge of the juvenile justice system and Chapter 232 of the Iowa Code, as it pertains to the handling of juveniles.
- G. The Support Services Division and the Investigation Division shall act as the liaisons between the Department and other elements of the juvenile justice system. Through these liaisons, other elements within the juvenile justice system will be encouraged to review and provide comment on the Department's procedures and policies relating to juveniles.

III. Procedure: Juvenile Custody

- A. In deciding on a course of action for a juvenile offender the following shall be considered:
 1. The nature of the offense
 2. The age of the offender.
 3. The circumstances of the offender.
 4. The offender's record.
 5. Availability of community based rehabilitation.
 6. Recommendations by the complainant(s) or victim(s).
- B. When dealing with juvenile offenders, officers shall use the least coercive among all reasonable alternatives consistent with protecting the juvenile's rights and fulfilling the mission of the Department. The following disposition options are listed in order of severity from least to most severe:
 1. Released without charges to parent or guardian. This action shall only be used in very minor incidents or in cases where charges may not be substantiated.
 2. When permissible by Iowa Code, issuing of a citation(s) in lieu of taking the juvenile into custody
 3. Releasing a juvenile offender to their parent or guardian at the scene of the offense or immediately following a required booking process in lieu of continued custody. Officers shall be required to complete the booking process including fingerprints and photographs of a juvenile offender being charged with a serious misdemeanor or above criminal offense. The following cases shall be referred to juvenile court:
 - a. The act would constitute a felony if committed by an adult.
 - b. The act involves the use of a weapon or the threat of bodily harm.
 - c. Aggravated assault or battery.

- d. Gang related offenses.
 - e. Operating while intoxicated
 - f. The juvenile is currently under court supervision or probation for another offense, or already has a case pending before the court.
 - g. The juvenile is a repeat offender.
4. Held at juvenile detention center pending a hearing by the appropriate court.
5. When a juvenile is arrested for an excluded offense, warrant or original charge, during normal court hours, they shall be taken to the courthouse of the county of their residence for initial appearance. When the arrest occurs outside of normal court hours, they shall be taken to the juvenile detention facility (Centralized Intake) until the next day where they will appear at jail court (Polk County resident) or weekend arraignment (county court of their residence) for initial appearance. The Department shall be responsible for transporting the juvenile to court even if the juvenile is held at centralized Intake overnight.
6. Juveniles, who are 16 or 17 years of age, that commit the following crimes are excluded from the jurisdiction of the juvenile court and will be held as stated above:
- a. Murder
 - (1) 1st Degree - 707.2
 - (2) 2nd Degree - 707.3
 - (3) Voluntary Manslaughter - 707.4
 - (4) Attempted Murder - 707.11
 - b. Assault
 - (1) Assault while participating in a Felony - 708.3
 - (2) Willful Injury - 708.4
 - (3) Terrorism (forcible) - 708.6
 - c. Sexual Abuse
 - (1) 1st Degree - 709.2
 - (2) 2nd Degree - 709.3
 - (3) 3rd Degree - 709.4
 - d. Assault w/intent to commit Sex Abuse, Injury or Serious Injury occurring during assault - 709.11
 - e. Kidnapping
 - (1) 1st Degree - 710.2
 - (2) 2nd Degree - 710.3
 - (3) 3rd Degree - 710.4
 - f. Robbery
 - (1) 1st Degree - 711.2
 - (2) 2nd Degree - 711.3
 - g. Arson 1st Degree - 712.2

- h. Burglary 1st Degree - 713.3
 - i. Criminal Gang Participation with Possession of a Weapon - 723.A.2
 - j. Possession of Weapons
 - (1) Possession of an offensive weapon - 724.3
 - (2) Possession of a firearm on school property - 724.4B(1)
 - (3) Trafficking in stolen weapons (firearms) - 724.16 (A)
 - (4) Giving false information when acquiring - 724.21
 - (5) Making firearms available to minors (2nd offense) - 724.22
 - (6) Felon possessing a firearm - 724.26
 - (7) Reckless use of a firearm (serious injury or bodily injury occurs) - 724.30
 - k. Felonious Child Endangerment - 726.6
 - l. Possession w/intent to deliver, while armed - 124.401(1)(e) firearm, (f) offensive weapon
- C. Diversion alternatives for juveniles shall only be administered by Juvenile Court Services (JCS) as described below after a case has been referred to JCS by the Department:
1. JCS works towards balancing community safety, victim/community restoration, accountability and rehabilitation for juveniles by assessing their risk of re-offending. There are circumstances and offenses based on a juvenile's risk level, where JCS would prefer to afford the juvenile an opportunity to address charge(s) informally by agreeing to complete a short term diversion intervention/class or by agreeing to an **Informal Adjustment Agreement (IAA)**. This allows two opportunities to resolve complaints informally and avoid the collateral consequences of formal court processing and adjudication (**filing a petition**):
 - a. JCS Diversion- depending on circumstances and level of charge, JCS utilizes the following researched based diversionary practices: warn and release and short term light touch interventions which are utilized for many first time offenders and some simple misdemeanor level offenders.
 - b. **Informal Adjustment Agreement-** IAA is an alternative to filing a petition for formal court processing. If the juvenile successfully completes the IAA, the case will be dismissed. If the juvenile does not successfully complete the IAA, a petition may be requested. Depending on circumstances and level of charge, juveniles committing more serious offenses presenting safety concerns may be afforded an IAA, which would subject them to informal supervision by an Juvenile Intake Officer and if required, participation in services for up to six months. Agreeing to an IAA is a productive way of resolving complaints that do not threaten public safety without formal court intervention.
 2. **Petition Request-** When there is no admission of guilt during the Intake Interview (used to determine whether an IAA would be most

appropriate) or the level of charge warrants a petition being requested. The Intake Officer will submit a petition request to the county attorney, which describes the nature of the delinquent act alleged and triggers formal court proceedings.

- D.** The following procedures are required when a juvenile is taken into custody:
1. Determine whether the juvenile is alleged to have engaged in a criminal or a status offense (a status offense is non-criminal behavior such as truancy or runaway). Juveniles in custody solely for status offenses shall not be handcuffed or held in a locked room or cell unless the juvenile is a threat to harm themselves or others.
 2. Determine whether the juvenile is alleged to have been harmed or is in danger of harm.
 3. When applicable, advise a juvenile in custody of Miranda Warnings. Miranda Warnings are mandated for juveniles under the same conditions that would require such warnings for adults (see other requirements for interrogation of a juvenile in Section III. D of this policy).
 4. Ensure the constitutional rights of the juvenile are protected.
 5. As soon as possible, make reasonable attempts to notify the juvenile's parent/ guardian.
 6. Without unnecessary delay, release the juvenile to a parent or guardian or bring to a juvenile intake facility as stated below (unless the juvenile is in need of emergency medical treatment).
 7. Complete all necessary reports.
 8. Fingerprint and photograph the juvenile if applicable under Iowa Code Chapter 232.148 for a public offense other than a simple misdemeanor.
 9. When needed, contact a detective for follow-up investigation. When there is no detective on duty, the supervisor in charge shall determine whether the case warrants contacting an on-call detective.
- E.** Non-custodial interviews of juveniles do not require a Miranda rights notification and waiver; however, officers shall be cautious as court interpretation of custody may differ from adults based on the juvenile's age, mental capacity, educational background and other mitigating factors. When interviewing a juvenile that is not in custody the following procedures shall apply:
1. The officer shall clearly identify themselves as a police officer.
 2. The officer shall ensure their actions do not establish custody. If the situation changes resulting in the need for custody, continued questioning will be considered custodial and require Miranda Rights notification and parental involvement as established below.

3. The officer shall evaluate the juvenile and the circumstances to determine if the juvenile is able to understand they are not in custody and are free to respond or not respond.
 4. When appropriate, a detailed report of the interview and all factors relevant to determining custody and juvenile capacity to understand the situation shall be completed.
- F. Upon ensuring a juvenile is afforded all of their constitutional rights, a juvenile in custody for a delinquent act may be interrogated by the police only after the juvenile and their parent have waived the juvenile's Miranda rights. If reasonable attempts to contact a parent or guardian have been made, juveniles that are sixteen (16) or seventeen (17) years of age may waive their Miranda rights without parental consent. Detailed documentation of the attempts to contact the parents or guardian is required. When an interrogation is necessary or desirable, the following procedures shall apply:
1. Limit the duration of the interrogation to a reasonable period and afford appropriate breaks as needed.
 2. Limit the number of officers involved in the interrogation to as few as possible.
 3. Prior to the interrogation of a juvenile, age, mental capacity, educational background and other mitigating factors shall be considered to determine if confessions obtained will be admissible in future court proceedings. The prosecuting attorney responsible for the case may be consulted prior to the interrogation to confirm admissibility based on all factors present.

IV. Procedure: Referrals to Juvenile Court

- A. The following procedures shall be followed by officers when referring a juvenile to court without continued detention:
1. Notify the juvenile court screening department of the county of residence of the referral.
 2. Notify the juvenile's parent or guardian of the referral to Juvenile Court.
 3. Forward copies of all police reports to the juvenile court screening department of the county of residence.
- B. The following procedures shall be followed by an officer when a juvenile is detained at the juvenile detention center (Centralized Intake) pending a referral to juvenile court:
1. Contact the Polk or Dallas County Juvenile Court Intake. Inform the juvenile court official of the nature of the charge, juvenile's history, etc.
 2. When necessary, assist the juvenile court in notifying the parent or guardian of the location, time, and date of the detention hearing and nature of the allegations.
 3. Provide juvenile intake personnel with required copies of all reports and petitions.

- C. When necessary, it is the responsibility of the officer to obtain medical attention for a juvenile prior to admission to the juvenile detention center. A juvenile, who is injured, seriously ill, under the influence of drugs or alcohol, or displays unusual behavior, must be examined at a hospital prior to admission to the juvenile detention center. Approval for admission to the detention center must be obtained prior to transport.

V. Procedure: Restraint of Juveniles

- A. Officers may use approved restraints as stated in Chapter 8 Section 70.1.1 on a juvenile in custody as long as one of the following conditions exist:
 - 1. The juvenile physically resists.
 - 2. The juvenile threatens physical violence when being taken into custody.
 - 3. The juvenile is being taken into custody for an act of violence against another person.
 - 4. In the reasonable judgment of the officer, the juvenile presents a risk of injury either to themselves or another person.
- B. Any officer restraining a juvenile shall articulate the specific reasons in their incident report.

Chapter 5: Law Enforcement Operations
Section 44: Juvenile Operations
Subsection 2: Operations



Policy/Procedure #: 4
Title: School Resource Officer
CALEA Reference#: 44.2.4

I. Policy: School Resource Officer

The Urbandale Police Department's school resource officer (SRO) is intended to provide support to specific school districts within the City of Urbandale through a contractual agreement. Other schools within the jurisdictional boundaries of the City of Urbandale shall receive assistance upon request by the appropriate division. The SRO shall assist in and around the school environment to maintain a safe, peaceful, and an orderly atmosphere in which students pursue their education and engage in extracurricular activities. The SRO position is established to create a positive working relationship between the community, schools, and the department, building trust and cooperation. The SRO shall provide guidance, counseling, and support where necessary to assist students, parents, and school staff while dealing with legal and police matters. The expertise of the SRO will assist school administrators in taking immediate action and will provide direct and immediate access to police assistance and services.

II. Procedure: Assignment

- A.** The SRO shall abide by the department and school district policies and shall consult with and coordinate activities through the school administrator or designee but shall remain fully responsive to the department's chain of command. In those instances where department policy and school district policy conflict, department policy shall take precedent.
- B.** The support services division shall administer the SRO positions and their assignments.
- C.** The SRO, with the assistance of the patrol division, shall handle calls for service involving students where a contractual agreement between the district and the department exists. The patrol division shall be

responsible for calls for service at all other schools within the City of Urbandale. If the SRO assigned to a school district is unavailable, the call for service shall be handled by the patrol division with appropriate assistance from the criminal investigation division.

- D.** School sanctions will be handed down by the appropriate school administrator, not the SRO. If school administration believes an incident is a violation of the law, they shall contact the SRO for assistance. The SRO, with supervisory assistance, shall determine whether law enforcement action is appropriate.
- E.** The SRO is a specialized assignment within the department and selection for the position shall follow the procedures established in chapter 2 section 16.2.1 of the Operations Manual. School administrators may be allowed to participate in the selection process for a SRO but the final selection shall remain with the chief of police.
- F.** The support services division shall set the work hours for the SRO positions with consideration for school hours and needs. Generally, the SRO shall provide forty (40) hours of services during the workweeks the school is in session for students. The hours may be adjusted to accommodate the needs of school district with five (5) days advance notice to the department. During times when school is not in session, the SRO's assignments are dependent upon the needs of the department as established by the support services commander or the chief of police. The department may require the services of the SRO for training, emergency situations, and/or to assist with other police matters at any time.
- G.** When the SRO is requested by the school district to work sporting events and other special programs outside their normal work hours, they shall be compensated at an overtime rate by the department that shall be reimbursed by the district. When the SRO is unable to cover an event at their assigned school, other officers shall be allowed to work the event following the contracted duty employment policy of the department as established in chapter 3 section 22.2.4 of the Operations Manual. The school district shall be invoiced by the department for provision of these services.
- H.** Request for time off shall be directed through the support services division supervisor. Generally, time off should occur when school is not in session so as not to affect the SRO's responsibilities at the school.
- I.** The SRO shall be required to report to the support services division for briefings and updates on a frequency established by the support services division commander.
- J.** The SRO shall be allowed to wear civilian or uniform attire as appropriate to their duties for the day. Specific dress requirements shall be established by the support services division commander with consideration for the school district's needs.

III. Procedure: Duties and Responsibilities

A. The SRO shall perform the following duties:

- 1.** Provide a positive congenial interaction with students while maintaining a high visibility throughout the school campus and grounds. This shall including random presence in hallways, bus loading areas, school grounds, and meal areas, especially during times of high concentration of students.
- 2.** Establish communication with school district staff, students, and their families.
- 3.** Promote a positive relationship between the department, the school district, and the community.
- 4.** Create programs and presentations that benefit the school district and the department, including providing resource material to supplement teachers' classroom activities and, as appropriate, be a guest presenter in the classroom, presenting at staff in-service meetings, parent education meetings, and at other school related community events.
- 5.** Be a positive role model for school staff and students.
- 6.** Provide safety measures for school district staff, students, and others on school grounds and surrounding public areas. The SRO shall assist school administrators in developing plans and strategies to prevent and/or minimize dangerous situations that may occur on campus or during school sponsored events.
- 7.** Accompany school district staff for home visits related to school situations, as appropriate.
- 8.** Support enforcement of school district rules and regulations, including those prohibiting violence, tobacco, alcohol, drugs, and bullying/harassment.
- 9.** Document and investigate criminal offenses committed on school district property.
- 10.** When appropriate, issue citations and take police actions.
- 11.** Perform other preventative and enforcement activities as needed.
- 12.** Maintain communication with school district juvenile court liaison officer, juvenile court services officers, tracking officers, placement officers, and the Polk County Attorney's juvenile bureau chief and attorneys.
- 13.** Meet with department supervisors concerning information on juvenile delinquency issues as well as work proactively with all law enforcement agencies.
- 14.** Maintain records of activities, programs and projects, including official statistical information and other written reports as required by the department and as reasonably requested by school district administrators.

- 15.** Attend monthly area school resource officers meetings.
- 16.** Perform other duties deemed appropriate and necessary by the department.
- B.** The SRO may utilize their discretion when handling misdemeanor cases within the school (with appropriate review by the department). All felony cases shall be referred to the juvenile court of the applicable county.
- C.** In the event of a major disturbance, after summoning any needed emergency assistance from the patrol division, a support services division supervisor shall be immediately notified. Should the situation warrant, the supervisor shall inform the chief of police and other division commanders of the disturbance.
- D.** The SRO shall abide by school district policies, rules and regulations, as appropriate, including specifically, policies, rules and regulations governing the confidentiality of student and staff records and policies, rules and regulations regarding the use of school district facilities and equipment. Department policies shall supersede school district policies, rules and regulations when the SRO is conducting police activities.
- E.** The SRO shall familiarize themselves with all community agencies which offer assistance to youths and their families, such as mental health clinics, substance abuse treatment facilities, delinquency prevention, etc.
- F.** Should it become necessary to conduct a formal law enforcement interview on school grounds with students or staff, the SRO shall abide by departmental policy concerning interviews.
- G.** The SRO may be required to attend training programs that will enhance their abilities in their assignment.
- H.** The SRO shall maintain all training certifications and qualifications in accordance with department policy and all applicable state laws.

Chapter 5: Law Enforcement Operations
Section 45: Crime Prevention and Community Involvement
Subsection 1: Crime Prevention



Policy/Procedure #: 1

Title: Crime Prevention and Community Relations

CALEA Reference#: 45.1.1, 45.1.2, 45.1.3, 45.2.1, 45.2.2, 61.4.4

I. Policy: Crime Prevention and Community Involvement

The personnel of the Urbandale Police Department are committed to establishing close ties with and responding to the needs of the community through a strong crime prevention and community relations effort. The Department shall publically state agency objectives, community problem areas, and successful programs in an effort to involve the community in crime prevention and community involvement activities. Crime prevention and community relations programs allow the Department to respond in a personalized timely manner to community concerns.

II. Procedure: Crime Prevention and Community Involvement

- A.** The Department shall use various available resources to prevent crime, be involved with the community, and enhance public relations. The community relations function is established to fulfill this objective. The community relations function shall assist in developing, organizing, and implementing community involvement activities and crime prevention programs targeted at reducing the opportunity for crime to occur.
- B.** The community relations function shall be assigned to the Support Services Division and shall be the main responsibility of the community relations officer(s). The community relations officer(s) shall report directly to the Support Services Division chain of command and shall be responsible for developing, improving, planning, and coordinating crime prevention and community involvement policy, procedure, and practice.
- C.** The community relations officer(s) shall establish liaisons with existing community organizations as well as assist in establishing new community groups as needed. The community relations officer(s) shall meet periodically with community organizations to receive information important to the operations of the Department as well as distribute crime prevention and traffic safety educational materials and other community interest information. Information or intelligence gathered from the community

organizations by the community relations officer(s) shall be passed on to the appropriate personnel.

- D.** The Support Services Division shall submit a quarterly community relations report that includes the following elements:

 - 1.** Current concerns and problems voiced by the community.
 - 2.** A description of potential problems that have a bearing on law enforcement activities within the community.
 - 3.** Recommended actions that address the concerns and problems that have been voiced or identified.
 - 4.** Progress made towards addressing previously identified concerns and problems.
- E.** Although the community relations officer(s) is responsible for crime prevention programming and community involvement initiatives, each member of the Department shall make crime prevention and community involvement part of their daily work activity within the community. Department members shall have a general knowledge of all programs offered by the community relations function. When a department member observes an opportunity to employ a crime prevention technique or engage in a situation where community involvement could make a difference in the outcome, they shall take appropriate action including notifying the community relations officer(s) for any needed follow-up action.
- F.** Determining where crime prevention and community involvement efforts will be most effective is essential to success. Crime analysis statistics based on crime type and geographic area shall be utilized to determine what programs will be developed to combat particular crimes in affected areas.
- G.** Often community perception of crime dictates the response to situations. The community relations officer(s) shall utilize crime prevention programs to target misconceptions about crime in the Urbandale service area reflecting a true account for criminal activity and ways the community can assist in preventing criminal behavior.
- H.** Information received from community relations contacts by members of the Department shall be forwarded to the community relations officer(s) via email or inter-office memorandum to assist in the development of programs to address the community's perceptions of crime.
- I.** The community relations officer(s) shall develop a relationship with and provide information to the City of Urbandale Engineering Department reference the development of zoning policies, building codes, fire codes, and residential/commercial building permits that employ crime prevention techniques. The community relations officer(s) shall also provide input to new and existing residential and commercial developments on how to prevent criminal activity through environmental design or aspects of crime free multi-housing.
- J.** The Support Services Division Commander or designee shall meet with the community relations officer(s) to evaluate all crime prevention

programs at a minimum every two (2) years. The report shall be forwarded to the Chief of Police for review. The evaluation shall examine all crime prevention programs for effectiveness and relevance. The evaluation may suggest changes to, formation of, or elimination of crime prevention programs. The evaluation should focus on community oriented policing approaches and programs.

- K. The community relations officer(s) shall advance communication efforts between the police and citizens through personal contacts, telephone, internet and social media. Communication with citizens shall include a focus on citizen involvement for reporting crime and or suspicious activity on a community wide basis. Events such as "National Night Out" shall highlight the importance of citizen involvement in building and sustaining safe communities.
- L. The community relations officers shall assist in organizing crime prevention groups in residential and business areas by use of social media apps, group presentations, and crime prevention programing.

III. Procedure: Citizen Survey

- A. One method of tracking progress in crime prevention and community involvement activities is through a citizen survey. The Department shall conduct a citizen survey at least once every two (2) years. The survey shall include the following information:
 - 1. Overall Agency Performance.
 - 2. Overall competence of agency employees
 - 3. Citizens' perception of officers' attitudes and behavior
 - 4. Community concern over safety and security
 - 5. Citizen's recommendations and suggestions for improvement
- B. At a minimum, a written summary of the citizen survey results shall be provided to the Chief of Police for review.

IV. Procedure: Accreditation Public Comment

- A. At least annually, the Department shall notify the community about the availability for the public to provide comment, commendation, and other information on the Urbandale Police Department's quality of service or other information relative to the accreditation process through the CALEA public access portal. The portal will be available at all times on the Urbandale Police Department's official website.
- B. Comments, commendations, and other information submitted through the portal will be flow directly to CALEA. The Department will gain access to this information from the assigned CALEA regional program director.

Chapter 5: Law Enforcement Operations
Section 45: Crime Prevention and Community Involvement
Subsection 3: Volunteers



Policy/Procedure #:1

Title: Volunteers

CALEA Reference#: 45.3.1, 45.3.2, 45.3.3

I. Policy: Volunteers

The Urbandale Police Department encourages and provides opportunities for citizens to become involved in different activities within the Department through volunteer programs. Volunteer personnel are not sworn officers and are not authorized to be utilized in a law enforcement role. Volunteers do not have the authority to make a full custodial arrest. They shall work under the direct supervision of a sworn officer or a full-time employee.

II. Procedure: General

- A.** A volunteer is a civilian affiliated with the Urbandale Police Department in a non-sworn capacity without compensation due to their interest in contributing to the agency's role or their interest in learning about the criminal justice system. Volunteers may be utilized for but not limited to the following duties:
 - 1.** Clerical work
 - 2.** Special event activities
 - 3.** Emergency activities
- B.** The Support Services Division shall be the liaison between volunteers and the Department and shall be responsible for assigning volunteers to duties that do not require police officer status. A list of volunteers, their contact information, and their current status (active or inactive) shall be maintained by the Support Services Division.
- C.** Prior to assignment to any duties, a background investigation shall be completed on all volunteers to determine suitability for the position. The Chief of Police shall give final approval of all volunteers.
- D.** Based on their assignment, volunteers may be provided a city identification card indicating their volunteer status.

- E.** Unless sworn as a regular or reserve police officer, volunteers are not law enforcement officers and shall possess no law enforcement authority other than that of a private person.
- F.** Volunteers shall not be authorized to carry any weapons while volunteering for the Department unless specifically authorized by the Chief of Police. If authorized, carrying of any weapons will only occur after appropriate training has been received.
- G.** Police chaplains shall be considered volunteers for the Department and this policy shall apply to their assignments. Due to their specialized role, Chaplains shall also follow the procedures outlined in Chapter 2 Section 16.4.1(Police Chaplains) of the Operations Manual. When in conflict, the chaplain policy shall supersede this policy.
- H.** Volunteers shall receive training appropriate to their assignment and may include:
 - 1.** Hands on instruction
 - 2.** Classroom instruction
 - 3.** Document review
- I.** Volunteers shall not be issued a uniform. They shall present a well-groomed and appropriately dressed appearance based on their assignment. Clothing shall be clean and in good condition. If provided a department shirt with logo, the shirt shall only be worn to approved events.

Chapter 5: Law Enforcement Operations
Section 46: Critical Incidents, Special Operations and Homeland Security
Subsection 1: Critical Incidents



Policy/Procedure #: 1

Title: Critical Incidents

CALEA Reference#: 46.1.1, 46.1.2, 46.1.3, 46.1.4, 46.1.5, 46.1.6, 46.1.7, 46.1.8, 46.1.9

I. Policy: Critical Incidents

A policy is established to govern the implementation of the incident command system (ICS) following the National Incident Management System (NIMS) guidelines. Department members will follow the ICS outlined in this policy to facilitate an orderly and effective response to emergencies requiring coordination with other city departments and/or outside agencies. This policy shall coincide with the City of Urbandale multi-hazard emergency operations plan.

II. Procedure: General

- A.** All critical incident planning shall be based on ICS and shall utilize the City of Urbandale multi-hazard emergency operations plan.
- B.** The ICS shall employ several functions to include command, operations, planning, logistics and finance/administration. Not all functions will be needed for all incidents. If an incident involves multiple city, county or state departments, the Urbandale Police Department will respond as part of the City of Urbandale's multi-hazard emergency operations plan.
- C.** The size of the incident will determine the extent in which the ICS is implemented. The procedures in this policy will be subservient to the City of Urbandale multi-hazard emergency operations plan. If the incident is smaller in nature and can be handled internally or with marginal assistance from outside agencies, the Department will implement the ICS internally as established in this policy.
- D.** When the ICS is initiated, all division commanders and the Chief of Police shall be notified and may be required to respond to the incident.

- E. Support Services Division shall ensure the following training on the City of Urbandale Multi-Hazard Emergency Operations Plan to include use of the Incident Command System:
 - 1. Annual training for all affected Department personnel.
 - 2. Biennial training consisting of a table top, functional or full-scale exercise to assess the Department's capabilities.
- F. The Support Services Division shall be responsible for semi-annual inspections for operational readiness of all needed equipment to respond to a critical incident.

III. Procedure: Command Function

- A. Every employee in a critical incident may potentially be in command at some point during the response. The first arriving unit on the scene will be in command until relieved by a higher ranking officer and will transmit a brief initial radio report to communications. The highest ranking officer on the scene may initiate the ICS based on their evaluation of the scene. When possible, a supervisor or designee shall assume command as soon as possible and be responsible for implementing the ICS. During any change of command, the outgoing commander will briefly outline operational and strategic information to the incoming commander before assuming a new role.
- B. Based on the incident, the command function may rise to the highest level of the Department. During large incidents in which outside law enforcement agencies are involved, the command function shall be the responsibility of the Chief of Police or designee.
- C. During critical incidents, the command function shall have the following responsibilities:
 - 1. Evaluate the situation and if appropriate, activate the ICS.
 - 2. Establish a safe and effective area for the command post.
 - 3. Initiate the mobilization of additional personnel and make appropriate notifications.
 - 4. Obtain support from other agencies.
 - 5. Establish a unified command, if necessary.
 - 6. Identify and communicate a safe location for a staging area.
 - 7. Provide public information and maintain media relations.
 - 8. Maintain the safety of all personnel involved in the incident.
 - 9. Prepare an after action report.
- D. The Department's public information officer may be assigned to the command function when an incident requires the release of public information or media relations activity.
- E. The incident commander shall assign a safety officer to act as an independent observer of all activities for potential threats to the safety of personnel. The safety officer shall be responsible for tracking all personnel and their location during the incident. The safety officer shall

report any unsafe activity to the incident commander. The incident commander will evaluate the activity and stop any action deemed too hazardous to proceed.

IV. Procedure: Operations Function:

- A.** Command of the operations function shall be assigned to the Patrol Division commander or designee.
- B.** When the ICS is implemented, the operations function shall be the responsibility of the Patrol Division. Based on need, the chief of police or designee may assign additional personnel to supplement the operations function.
- C.** The operations function will provide a workable incident action plan to the command function. The plan may provide for multiple solutions to address the situation.
- D.** All tactical operations conducted as part of a critical incident response shall be coordinated by the operations function. When utilized, the suburban emergency response team (SERT) or other tactical team's command element shall assist in the planning an appropriate response to the incident.
- E.** At the conclusion of the incident, the operations function shall also recommend strategies to close the incident and withdraw resources.
- F.** During critical incidents, the operations function shall have the following responsibilities:
 - 1. Eliminating or containing the threat.
 - 2. Establishing a perimeter.
 - 3. Conducting Evacuations.
 - 4. Maintaining command post and scene security.
 - 5. Providing detainee transportation, processing and confinement.
 - 6. Directing and controlling traffic.
 - 7. Close the incident and withdraw resources.

V. Procedure: Planning Function

- A.** Command of the planning function shall be assigned to the Criminal Investigation Division commander or designee.
- B.** The planning function shall collect, evaluate and disseminate all incoming information and intelligence about the incident, the status of resources and any anticipated needs.
- C.** The post incident investigation and crime scene processing of any criminal activity shall be assigned to the Investigation Division.
- D.** Administrative personnel may be assigned to the planning function based on need.
- E.** The planning function may assist the operations function and logistics function, as needed.

VI. Procedure: Logistics Function

- A. Command of the logistics function shall be assigned to the Support Services Division commander or designee.
- B. The logistics function of the ICS shall be tasked with equipping responding personnel.
- C. The logistics function shall establish a means for all responding personnel to communicate.
- D. The logistics function shall provide any needed supplies, equipment or transportation needs for the incident.
- E. The logistics function shall coordinate with the Urbandale Fire Department to provide needed medical support.
- F. When needed, the logistics function shall initiate the Department's continuity of operation plan (COOP) to assure the capability exists to continue essential agency functions throughout any emergency situation. The objective of a COOP may include:
 - 1. Ensure continuous performance of Department essential functions.
 - 2. Protect essential facilities and assets.
 - 3. Reduce or mitigate disruptions to operational activity.
 - 4. Minimize damages and losses.
 - 5. Facilitate decision-making during the emergency.
 - 6. Timely and orderly recovery from the emergency.
 - 7. Resumption of full service to the community.

VII. Procedure: Finance/Administration Function

- A. Command of the finance/administration function shall be assigned to the Office of the Chief of Police or designee. When additional manpower is needed, administrative personnel from the Support Services Division shall be assigned to assist.
- B. The finance/administration function of the ICS shall be responsible for documenting personnel time, procurement of additional resources and tracking all expenses.
- C. Any liability issues or injuries resulting from the incident shall also be documented.
- D. Any post incident cost accounting, including necessary documentation for reimbursement, shall be handled by the finance/administration function.

Chapter 5: Law Enforcement Operations
Section 46: Critical Incidents, Special Operations,
And Homeland Security
Subsection 1: Critical Incidents



Policy/Procedure #: 11

Title: Crowd Management and Control

CALEA Reference#: 46.1.2, 46.1.11, 46.1.12

I. Policy:

The Urbandale Police Department shall strive to effectively manage crowds during demonstrations or civil disturbances to prevent loss of life, injury, or property damage and minimize disruption to persons who are uninvolved. Officers encountering such incidents shall protect life, property, and the exercise of First Amendment rights. In rare circumstances involving emergencies and in widespread highly volatile civil unrest with the potential for widespread violence, the incident commander (IC) may temporarily suspend any policy, provision, or guideline contained herein when such action is determined to be the only reasonable alternative for the prevention of loss of life or major property damage.

II. Procedure: Definitions

A. Demonstration (lawful assembly): A lawful assembly of persons organized primarily to engage in First Amendment activities. Free speech and assembly are lawfully protected activities. These may be scheduled events that allow for law enforcement planning. They include but are not limited to speeches, marches, rallies, picketing, public assemblies, protests, celebratory events, and other assemblies intended to attract attention. Officer shall be aware lawful demonstrations can devolve into civil disturbances that necessitate enforcement action.

B. Civil Disturbance (unlawful assembly or riot): A gathering that constitutes a breach of the peace or any assembly of persons where there is a threat of collective violence, destruction of property, or other unlawful acts. Such a gathering may also be referred to as an unlawful assembly or a riot.

1. Unlawful assembly- Assemblies may be dispersed when they are violent or pose a clear and present danger of violence or the group is breaking some other law in the process. If a crime is occurring, action may be taken to stop it before giving an order to disperse. Per Iowa Code 723.2 an unlawful assembly is three or more persons assembled together with them or any of them acting in a violent manner and with the intent they or any of them will commit a public offense.
 2. Riot- Per Iowa Code 732.1 a riot is three or more persons assembled together in a violent manner to the disturbance of others and with any use of unlawful force or violence by them or any of them against another person or causing property damage.
- C. Crowd Control:** Techniques used to address civil disturbances, to include a show of force, crowd containment, dispersal equipment and tactics and preparations for multiple arrests.
- D. Crowd Management:** Techniques used to manage lawful assemblies before, during, and after the event for the purpose of maintaining their lawful status through event planning, pre-event contact with group leaders, issuance of permits when applicable, information gathering, personnel training and other means.
- E. Chemical deterrent:** An irritating agent which can rapidly produce sensory irritation or disabling physical effects which disappear within a short time following termination of exposure. These may include but are not limited to riot control agents such as CS and oleoresin capsicum (OC). Riot control agents generally cause victims to disperse or be temporarily compromised by the pain and irritation they cause to the eyes, skin and mucous membranes. Their effects generally disappear within a short time after exposure and victims normally recover without the need for medical attention.
- F. Electronic Control Device:** Electronic control devices (ECD) are designed to immobilize a suspect by means of an electrical current. The electrical current causes the muscles in the body to involuntarily contract causing the suspect to become virtually helpless while the less-lethal electronic control device is activated.
- G. Striking Instruments:** Striking instruments shall be a straight baton constructed of metal, polycarbonate, or wood. If an officer is faced with a deadly force situation, officers may use anything at their disposal as a striking instrument.

III. Procedures: General Management and Organizational Principles

- A.** The Department may impose reasonable restrictions on the time, place and manner in which persons engage in First Amendment activity. The Department shall place only those limitations and restrictions on demonstrations necessary to maintain public safety and order and to the

degree possible, facilitate uninhibited commerce and freedom of movement.

- B.** The organization of responsibility shall be as follows:
 - 1.** The Chief of Police or designee shall assign themselves or another as the incident commander (IC) responsible for overall control of a demonstration or civil disturbance. In accordance with Chapter 5 Section 46.1.1 (Critical Incidents) of the Operations Manual, the IC shall implement an incident action plan.
 - 2.** In the case of a widely dispersed demonstration, disturbance, or event with multiple locations, multiple ICs may be assigned at the discretion of the Chief of Police or designee.
- C.** As delineated in Chapter 5 Section 46.1.1 (Critical Incidents) of the Operations Manual, Incident command system (ICS) protocols shall be used in crowd management and civil disturbances to ensure control and unified command.
- D.** The primary objectives of the IC at a civil disturbance shall be as follows:
 - 1.** Protect persons, regardless of their participation in the disturbance, and protect property.
 - 2.** Disperse disorderly or threatening crowds in order to eliminate the immediate risks of continued escalation and further violence.
 - 3.** Arrest law violators and remove or isolate persons inciting violent behavior.
- E.** Unless absolutely necessary, mass arrest shall be avoided.
- F.** It is vital to audio and video record the incident to capture the actions of the officers and law violators.
- G.** Officers shall be briefed on what to expect and appropriate responses. They shall be informed the IC or designee(s) shall be responsible for ordering any response deemed appropriate.
- H.** Protective helmets shall be marked for identification purposes. Issuance of protective helmets and other equipment for use by personnel responding to an incident shall be logged by a supervisor or designee.
- I.** Sworn officers and reserves shall receive training in how to respond to crowd control situations.

IV. Procedure: Use of Force

- A.** Unless exigent circumstances justify immediate action, officers shall not independently make arrests or employ force without command authorization.
- B.** All officers providing assistance to this agency through mutual aid agreements, contracts, or related means shall be informed they are under the direction and control of the Urbandale Police Department's command and supervisory personnel.
- C.** When reasonably possible, a warning shall be given prior to use of force.

- D.** In addition to all the restriction applicable to each weapon system as delineated in Chapter 1 Section 1.3.1 (Use of Force), the following restrictions and limitations on the use of force shall be observed during demonstrations and civil disturbances. In all cases, weapons shall be carried and deployed only by trained and authorized officers:
- 1.** Canine teams may respond as backup when appropriate but shall not be deployed for crowd control (i.e., containment or dispersal). Canines shall remain in patrol vehicles or other secure locations and, whenever reasonably possible, out of the view of the crowd. Canines may be deployed in appropriate circumstances related to bomb detection, pursuit of suspects in buildings, and related situations.
 - 2.** Motor vehicles may be used to surround and move persons as appropriate but shall not be brought into contact with persons.
 - 3.** Electronic control devices (ECD) may be used during civil disturbances for purposes of restraint or arrest of actively resistant individuals when alternative less forceful means of control are not available or are unsuitable and only when the individual can be accurately targeted. ECD shall not be used to gain compliance from persons who are exhibiting passive resistance, unless there is a reasonable expectation it will be unsafe for officers to approach within contact distance of the person and all other options are not practical or effective. ECDs shall not be fired indiscriminately into crowds.
 - 4.** Chemical deterrent spray may be used against specific individuals engaged in unlawful conduct or actively resisting arrest, or as necessary in a defensive capacity when appropriate.
 - 5.** Large canisters of chemical deterrent are designed for and may be used in civil disturbances against groups of people engaged in unlawful acts or endangering public safety and security when approved by the IC. Large canisters of chemical deterrent designed for crowd control shall not be used indiscriminately against groups of people where bystanders would be unreasonably affected, or against passively resistant individuals.
 - 6.** CS (2-chlorobenzalmalononitrile) chemical agents are less lethal weapons that shall be used with the utmost caution. CS may be deployed defensively to prevent injury when lesser force options are either not available or would likely be ineffective. Such munitions shall be deployed at the direction of the IC and only when avenues of escape are available to the crowd. CN (phenacyl chloride) shall not be used in any instance.
 - 7.** A striking instrument shall be used primarily as a defensive weapon; as a means of overcoming resistance (e.g., used in the two-hand horizontal thrust on a police line); as a show of force; or as a means to contain or disperse a crowd.

- E. Because of the unique logistical and safety concerns presented by civil disturbances, the Department's internal affairs (IA) or professional standards unit shall comply with the following protocols during such events:
 - 1. All force related information and complaints and shall be recorded by the command post or designee.
 - 2. Officers shall be required to complete use of force reports for review by supervisory personnel for all use of force incidents.
 - 3. Supervisors reviewing use of force reports shall utilize any video or photographic evidence available to view officer and crowd actions.

V. Procedure: Demonstrations (Lawful Assembly)

- A. Every effort shall be made to make advance contact with the leaders of a demonstration, gain cooperation, and to gather information about the event to ensure accurate assignment of personnel and resources. Liaison with other stakeholders to include businesses and community members affected shall also be included in pre-event planning.
- B. The IC or a designee shall prepare a written action plan subject to the approval of the Chief of Police or designee. Personnel preparing the written action plan shall utilize the UPD event operation plan form. Necessary information may include:
 - 1. What type of event is involved?
 - 2. When is it planned?
 - 3. What is the history and risk of the group?
 - 4. Will the event coincide with other routine, large scale events (e.g. sporting events)?
 - 5. Is opposition to the event expected? How many participants are expected?
 - 6. What are the assembly areas and movement routes?
 - 7. What actions, activities, or tactics are anticipated, to include use of demonstrator devices designed to thwart arrest (e.g., dragon sleeves and u-locks)?
 - 8. What if any critical infrastructures are in the proximity of the event?
 - 9. Have permits been issued?
 - 10. Have other agencies such as Fire and EMS been notified?
 - 11. Is there a need to request mutual aid?
 - 12. Will off-duty personnel be required?
 - 13. What is the past history of conduct at such events and whether group leaders are cooperative?
 - 14. What are the specific rules of engagement and use of force guidelines as applicable?
- C. The action plan shall address provisions for the following and be distributed to all affected command and supervisory officers:
 - 1. Command assignments and responsibilities

2. Identify and assign resources. Personnel, unit structure, and deployment.
 3. Liaison with demonstration leaders. Use facilitation not confrontation.
 4. Monitoring and continuing assessment of crowd behavior
 5. If applicable, separation of opposition groups
 6. Liaison with outside agencies
 7. Release of information to the news media
 8. Transportation, support, and relief of personnel
 9. Staging points for additional resources and equipment
 10. Traffic management
 11. Demonstrator devices, extrication teams, and equipment
 12. First aid stations established in coordination with emergency medical service providers
 13. Transportation of prisoners
 14. Prisoner detention areas
- D. Officers shall be deployed to monitor crowd activity. Specific direction and expectations shall be conveyed to officers prior to deployment at mission briefing. Sufficient resources to handle multiple unruly persons shall be available depending on the fluidity of the situation and degree of actual or likely disruption.
 - E. Unless assigned to covertly monitor group activity, personnel shall wear their badges and nameplates or other identification in a visible location on their person at all times.
 - F. Officers shall not engage in conversations or be prompted to act in response to comments from demonstrators. Officers shall maintain a courteous and neutral demeanor.
 - G. Persons who reside, are employed, or have emergency business within the area marked off by a police line shall not be prevented from entering the area unless circumstances suggest their safety would be jeopardized or their entry would interfere with law enforcement operations.
 - H. When possible, on scene supervisors shall establish and maintain communication with demonstration leaders and relay information on crowd mood and intent to the IC.
 - I. Supervisors shall maintain close contact with their assigned officers to ensure compliance with orders, monitor behavior and disposition, and ensure they are aware of any changes in crowd behavior or intent.

VI. Procedure: Isolated unlawful behavior

- A. Isolated unlawful behavior by individuals or small groups within a crowd should not automatically form the basis for declaring an assembly unlawful. This behavior may include isolated destruction of property, isolated acts of violence, isolated object (rocks, bottles) throwing, and individual sit down demonstrators. The Department shall consider the following response:

1. Use organizers and monitors to gain voluntary compliance
2. Isolate, arrest, and remove law violators as quickly as possible
3. Use amplified sound to communicate or gain compliance
4. Do not increase crowd tension by unnecessary aggressive behavior or appearance
5. When not possible to make an immediate arrest, identify and track suspects using cameras, observation posts, or shadow teams
6. Continue to assess; escalate and deescalate as behavior changes
7. Use low profile tactics when possible

VII. Procedure: Response to civil disturbances- Unlawful assembly, and Riots.

A. The first officer to arrive on the scene of a spontaneous civil disturbance shall:

1. Observe the situation from a safe distance to determine if the gathering is currently or potentially violent.
2. Notify communications of the nature and seriousness of the disturbance, particularly the availability of improvised or deadly weapons, the location and estimated number of participants, current activities (e.g. blocking traffic), direction of movement, and ingress and egress routes for emergency vehicles.
3. Request the assistance of a supervisor and necessary backup.
4. If approaching the crowd would not present unnecessary risk, instruct the gathering to disperse by using amplified communications (e.g. PA, bullhorn).
5. Attempt to identify crowd leaders and agitators engaged in criminal acts.

B. The first supervisor in charge at the scene shall:

1. Deploy officers at vantage points to report on crowd actions;
2. Establish a control force to establish a perimeter sufficient to contain the disturbance and prohibit entrance into the affected area.
3. Ensure uninvolved civilians are evacuated from the immediate area of the disturbance.
4. Establish a temporary command post.
5. Provide ongoing assessment to communications.

C. In the area outside the perimeter, the IC shall ensure the following actions are taken:

1. Move and reroute pedestrian and vehicular traffic around the disorder.
2. Control unauthorized ingress and egress by participants.
3. Prevent attempts to assist or reinforce the incident participants from outside the area.
4. Ensure adequate security is provided to Fire and EMS personnel in the performance of emergency tasks.
5. Ensure support and relief of personnel is available.

6. Establish and maintain a secure staging area for emergency responders and equipment.
7. Liaison and staging points for media representatives are established and available information is provided as appropriate.
8. An event log is created for documenting activities and actions taken during the course of the incident.
9. Where possible, photographs are taken and video recordings of event proceedings are made.
10. The need for full mobilization of sworn officers and the recall of off-duty officers is determined.
11. Identify dispersal routes.
12. Determine if it is feasible to arrest those who are failing to disperse or are conducting illegal activity being cognizant that mass arrest should be avoided.
13. Track and contain groups involved in illegal behavior using cameras, observation posts or shadow teams
14. Ensure escalation and de-escalation of force is proportional to the response of the crowd.
15. With proper approval, deploy less lethal munitions as needed to defend control force or to disperse the crowd.
16. Remain present in the area and through deployment of forces, discourage groups from reforming.

VIII. Procedure: Crowd Dispersal

- A. Prior to ordering a forced dispersal of a civil disturbance, the IC shall determine whether lesser alternatives may be effective. These alternatives include the use of containment and dialogue, as follows:
 1. Establish contact with crowd leaders to assess their intentions and motivations and develop a mutually acceptable plan for de-escalation and dispersal.
 2. Communicate to the participants their assembly is in violation of the law and the Department wishes to resolve the incident peacefully, but acts of violence will be dealt with swiftly and decisively.
 3. Negotiate with crowd leaders for voluntary dispersal, or target specific violent or disruptive individuals for arrest.
- B. Prior to issuing dispersal orders, the IC shall ensure all potentially necessary law enforcement, Fire, and EMS equipment and personnel are on hand to successfully carry out tactical operations and that logistical needs for making mass arrests are in place.
- C. When the IC has made a determination an unruly gathering is present and crowd dispersal is required, they shall direct unit commanders, where time and circumstances permit, to issue warnings prior to taking action to disperse the crowd.

1. The warning shall consist of an announcement citing the offenses or violations being committed, an order to disperse, and designated dispersal routes. A second and a third warning shall be issued at reasonable time intervals before designated actions are taken to disperse the crowd. Where possible, the warnings shall be audio or video recorded and the time and the names of the issuing officers recorded in the IC's event log.
2. Specific crowd dispersal tactics shall be ordered as necessary where the crowd does not heed warnings. These include, but are not limited to, any one or combination of the following:
 - a. Display of forceful presence to include police lines, combined with law enforcement vehicles, bicycle units and mobile field forces
 - b. Crowd encirclement
 - c. Multiple simultaneous arrests
 - d. Use of crowd control chemical agents
 - e. Law enforcement formations and the use of batons for forcing crowd movement

IX. Procedure: Mass Arrest

- A. In a civil disturbance it may be necessary to make arrests of numerous individuals over a relatively short period of time. For this process to be handled efficiently, safely, and legally, the following shall be observed:
 1. When practical, mass arrests shall be conducted by designated groups of officers.
 2. Adequate secure area shall be designated for holding prisoners after initial booking and while awaiting transportation. If the volume of arrests is more than the Polk and/or Dallas County Jail can accommodate, arrangements shall be made with other area holding facilities to assist.
 3. Arrest teams shall be advised of the basic offenses to be charged in all arrests. All arrestees shall be advised of their charges.
 4. Arrestees who agree to walk shall be escorted to the transportation vehicle for processing. Two or more officers shall carry those who refuse to walk. Officers may utilize a stretcher or other means to move extremely heavy individuals.
 5. Prisoners shall be searched incident to arrest for weapons, contraband, and evidence of the crime in which they are being arrested.
 6. A field arrest form shall be completed on all arrestees. The Polk County jail booking sheet shall serve as a field arrest form. All arrestees shall have their photograph with a placard number taken at the time of arrest. The placard number shall be added to the comments section of the Polk County booking form.

7. Accounting for arrestee property shall follow normal department policy and procedure.
8. Injured prisoners and those who request medical attention shall be provided medical attention as soon as possible. Photographs shall be taken of all injuries.

X. Procedure: Deactivation

- A. When the disturbance has been brought under control, the IC shall ensure all personnel engaged in the incident shall be accounted for and an assessment and documentation completed on all personal injuries.
- B. Witnesses, suspects, and others shall be interviewed. Personnel shall be debriefed as necessary.
- C. Personnel shall complete written reports as soon as practical after the incident. Comprehensive documentation of the basis for the incident, the Department's response to the incident, with a statement of impact to include the cost of equipment, personnel, and related items shall be completed.

Chapter 5: Law Enforcement Operations
Section 46: Critical Incidents, Special Operations,
And Homeland Security
Subsection 1: Critical Incidents



Policy/Procedure #: 13
Title: Continuity of Operation
CALEA Reference#: 46.1.13

- I. **Policy:** The Urbandale Police Department shall be prepared to respond to the communities needs during an event that disrupts or degrades the capabilities of the Department by establishing a plan to maintain the ability to meet the essential needs of the community. The Department is committed to the safety of its employees, operations, and assets. This plan, in conjunction with the City of Urbandale Business Continuity Plan and the City of Urbandale All Hazards Plan, provides personnel a framework designed to minimize disruptions during an emergency event. The Continuity of Operations Plan (COOP) is designed to enable units within the Police Department to effectively maintain their primary functions during a disaster/emergency which may disrupt critical operations and services.
- II. **Procedure: General**
 - A. The Department's COOP is one component of the City of Urbandale's comprehensive emergency management program that addresses the preparation for; mitigation of; and response to recovery from all hazards. By developing a plan to continue the essential functions of the Department, the COOP plan ensures the Department will continue to operate even in the wake of a major hazardous event. The Department may face a variety of natural, technological, and human related events that offer a significant threat to the Department and the City of Urbandale.
 - B. The COOP shall address the following:
 1. Identify mission-essential functions that must be maintained regardless of the challenges posed by an emergency situation.
 2. Determine the personnel, facilities, equipment, systems, information, and other resources necessary to support those essential functions

and ensure the ability to maintain the essential functions with minimal disruption.

3. Address COOP activation management and succession.
 4. Compile information to facilitate quick and effective communication and decision making.
 5. Facilitate the recovery/resumption of normal operations.
 6. Establish procedures to implement actions resulting in continued essential functions within the recovery time objectives for up to 30 days.
- C. The COOP is predicated upon a realistic approach to problems likely to be encountered during a major emergency or disaster, and is based on the following assumptions:
1. An emergency or disaster may occur at any time of the day or night, weekend, or holiday, with little to no warning.
 2. During an emergency or disaster, the Department leadership will coordinate with the City of Urbandale leadership to determine, prioritize, mobilize, and direct resource needs as part of the City's All Hazards Plan.
 3. Many normal operations may be suspended or canceled to allow resources to be directed to saving lives, relieving human suffering, and sustaining survivors.
 4. Department staff may be called upon to support the city's broader emergency response efforts in addition to maintaining or resuming normal police activities.
 5. Some or all normal programs and activities, other than those identified as essential functions, may be suspended or reduced, depending on available resources and staffing. Even for essential functions, it may not be possible to maintain normal levels of service.
 6. All records and documents needed to restore and maintain essential functions will be maintained in such a manner they are accessible from alternative locations.
 7. Disasters may affect other jurisdictions of the region, as well as state and federal agencies, and contractors/vendors. Delays in receiving government or contracted services, support, or supplies may occur and may last for multiple days or weeks depending upon severity of the incident.

III. Procedure: Duties

- A. The Chief of Police is responsible for overseeing the Department's response to any disaster or emergency and shall have the following duties:
1. Activation of the COOP.
 2. Provide policy direction, guidance and objectives.
 3. Consult and advise various city officials.

4. Serve as the principal representative to external entities unless delegating the duty to a subordinate.
- B. Division Commanders are responsible for implementing the COOP at all levels of the Department and shall have the following duties:
 1. Ensure adequate staffing to accomplish COOP directives. Based on the incident, this may entail temporary transfer of sworn personnel to Patrol functions.
 2. Evaluate divisional needs and make recommendations on level of service to be delivered in the near term and projected out over a specific period.

IV. Procedure: Plan Activation

- A. The COOP may be activated under the following conditions:
 1. All or a portion of the Department's operations are disrupted at the current facility with limited or no disruptions to other city operations. The most likely cause is a fire, mechanical failure, loss of utilities, etc.
 2. Catastrophic incident affecting a geographic region within the city that causes a disruption to numerous city operations and may include widespread displacement of the community. Disruption is expected to be prolonged.
 3. A pandemic related disruption of the workforce for the Department leaving manpower to perform essential functions severely depleted.
- B. The Chief of Police or designee may activate the COOP when the ability to maintain the Department's essential functions are significantly challenged or compromised.
- C. The Support Services Division Commander shall be the main point of contact for COOP plan implementation.

V. Procedure: Reconstitution

- A. Reconstitution focuses on restoring operations to normal. Planning for reconstitution shall occur as soon as possible once the COOP has been initiated.
- B. The Support Services Division shall be responsible for reconstitution planning and implementation.

VI. Procedure: Plan Maintenance & Training

- A. The COOP shall be reviewed at minimum annually for needed changes and/or updating of information and shall be the responsibility of the Support Services Division.
- B. Training on the COOP shall occur as needed with an exercise of the plan every four (4) years.

Chapter 5: Law Enforcement Operations
Section 46: Critical Incidents, Special Operations and Homeland Security
Subsection 2: Special Operations



Policy/Procedure #: 1

Title: Rapid and Immediate Deployment

CALEA Reference#: 46.1.10, 46.2.1

I. Policy: Rapid and Immediate Deployment

Rapid and Immediate Deployment (RAID) is defined as the swift and immediate deployment of law enforcement resources to an active threat in which lives are in imminent danger and a delayed deployment may result in death or serious injury to innocent people. The Urbandale Police Department shall employ rapid and immediate deployment techniques to various situations in order to reduce the loss of life and contain the suspect(s) involved.

II. Procedure: General

A. Rapid and Immediate Deployment (RAID) tactics are not a substitute for conventional response tactics to a barricaded gunman or hostage situation in which the victims are not being actively killed or seriously injured.

B. RAID shall be utilized in the following situations:

1. An "active threat". An active threat is an individual or group actively engaged in the killing or attempted killing of people.
2. The placing and/or detonation of explosive devices by a suspect.
3. A citizen or officer is gravely wounded and delayed recovery may result in their death.
4. A suspect not actively involved in an assault; however, an assault is imminent and immediate intervention is critical.
5. Any other dangerous situation likely to result in imminent death or serious injury to innocent persons.

C. The Support Services Division shall conduct a documented annual review of this policy including any training needs.

III. Procedure: Responsibilities of the Initial Responding Officer

- A. The initial responder may be a person of any rank but is most likely to be a patrol officer. The officer's quick analysis and action is critical.
- B. The senior officer on the scene will assume responsibility of the incident commander until relieved by appropriate authority.
- C. Consideration must be given to establishing a perimeter and containing the suspect(s) in a specific location (i.e. building, structure, area, etc.).
- D. The initial responder must quickly determine and request appropriate resources which may include:
 - 1. Additional patrol units / departmental personnel
 - 2. Suburban Emergency Response Team (SERT)
 - 3. Bomb Squad (determined by Incident Commander)
 - 4. Fire Department / Emergency Medical Services (EMS)
 - 5. Mutual Aid from other public safety departments (determined by the incident commander or the Chief of Police)
 - 6. Public Works.
- E. Other responding units shall be advised of the following information when available:
 - 1. Exact location of the incident
 - 2. Number of suspects and their location
 - 3. Type(s) of weapon involved
 - 4. Safe approach route
 - 5. Course of action for responding units
 - 6. Location of rally point.

IV. Procedure: RAID Contact Team

- A. Determination to deploy a contact team will be made by the incident commander with primary consideration being the immediate neutralization of the threat.
- B. There are no minimums for a contact team to be deployed. If only one officer is on scene and the situation calls for immediate action, the officer will deploy and make contact with the threat. Three (3) to (4) officers are the preferable number for a contact team but response will not be overly delayed for personnel to arrive. Depending on the situation and number of personnel, the team will travel in a "T" or "Y" formation as described below:
 - 1. Flank - acts as left and right contact officers.
 - 2. Team Leader - communicates with the responding units during deployment, delegates team member responsibilities, formulates and implements plan.
 - 3. Rear Security - Provides cover during entry and exit if necessary.
- C. The team's priorities are to make contact with the suspect(s) as quickly as possible and:
 - 1. Ensure the safety of those in proximity to the active threat.
 - 2. The safety of the citizens in the area of the event.

3. The safety of the police officers.
4. Neutralization of the suspect as soon as possible.
5. Containment of the suspect(s).
6. Communications with multi-officer, multi-agency response.
7. Provide preliminary assessment and continuous updates regarding:
 - a. Team progress.
 - b. Victim(s), location and medical needs (prioritize if possible).
 - c. Explosives - Types and location. If an explosive device is encountered or suspected move past or around the device(s) and discontinue use of communication radios.
 - d. Suspect(s) description and location.
 - e. Types of weapons (if known).

V. Procedure: Deployment of Rescue Team/ Rescue Task Force

- A. During or immediately after deployment of the contact team, the incident may require a rescue team and/or a Rescue Task Force be organized and deployed.
- B. There is no minimum number of officers needed for the formation of a rescue team. If only one officer is available and the situation calls for immediate action, the officer shall deploy. The size of the team shall vary depending on the scope of the mission and the availability of manpower. When a rescue team is deployed, officers may be utilized as follows:
 1. Point - act as the contact officer.
 2. Team Leader - communicates with responding units during deployment, delegates team member responsibilities, formulates and implements plan.
 3. Rescue Officers - general purpose, is to search for and handle recovery of victims, or engage suspect(s) if necessary.
 4. Rear Guard - provides cover during entry and exit.
- C. This team will be equipped similar to the contact team, with rescue officers being equipped with appropriate first aid supplies. The team shall be utilized when moving victims from the hot zone (inner perimeter) to the warm zone (casualty collection point) or even evacuation to the cold zone (outer perimeter) depending on the situation.
- D. The priority of the rescue team is the rescue and recovery of victim(s) and shall be accomplished as follows:
 1. Enter and/or approach location to locate victim(s)
 2. Report "new" suspect(s) location if applicable
 3. Extract victim(s) to a safe area and notify the incident commander
 4. Notify medical personnel if necessary
 5. Coordinate action with the contact team and incident command.
- E. Rescue Task Force Terminology:

1. Rescue Task Force: A combination of law enforcement and Fire/EMS personnel providing a coordinated effort of getting rapid medical care to victims located inside the warm zone.
 2. Hot Zone: A threat exists in the area, law enforcement contact teams are deployed in the area, Fire/EMS will not typically operate inside this area. The hot zone may also be called the inner perimeter.
 3. Warm Zone: The area has been cleared by law enforcement but not secured. There is minimal threat to the area, a rescue task force may deploy into this area to treat or evacuate victims. Law enforcement will determine where warm zones are located.
 4. Cold Zone: There is no threat to the area, this area is where the incident command post and other support functions are staged, and this area may also be called the outer perimeter.
 5. Casualty Collection Point: A forward location where victims can be assembled for movement from areas of high risk to triage/treatment areas.
- F. The deployment of a rescue task force shall take place when there is a need to treat and evacuate victims from within the warm zone. The decision to deploy a rescue task force shall be made by the incident commander.
- G. The deployment of a rescue task force requires a minimum of one officer and two Fire/EMS personnel. The size of a rescue task force can vary. The rescue task force shall have enough officers to adequately protect Fire/EMS personnel assigned to the rescue task force. An incident may have multiple rescue task force units operating at one time.
- H. The officers' role in the rescue task force:
1. Lead the rescue task force into the warm zone and determine areas that are safe to operate in during the incident.
 2. Provide security for rescue task force members.
 3. Generally does not assist with care, evacuation, or lifting of victims.
 4. Shall maintain direct line of sight and communication with rescue task force members.
 5. The decision on victim care and evacuation shall be the responsibility of Fire/EMS.

VI. Procedure: Arrival of Suburban Emergency Response Team (or other special operations units)

- A. When tactical team personnel arrive on scene, they are generally better equipped and trained to resolve crisis situations. Continued assistance by initial responders is critical. The contact team will maintain command and control of the interior situation until transition of responsibilities can be made to the tactical team.
- B. The tactical team leader will assume responsibility after making direct contact with the contact team leader.

- C. The tactical team leader will advise the contact team to assist with containment responsibilities or redirect their assistance to the rescue team and/or rescue task force.

VII. Procedure: Evacuation

- A. In some situations, it will be necessary to implement an evacuation of a school, business, church, gym, etc. When it becomes necessary to evacuate a large area, the following procedures will be followed:
 - 1. Do not use the fire alarm system to cause evacuation.
 - 2. All hallways and staircases should be cleared by police personnel.
 - 3. All exit routes to be used shall first be inspected and declared “clear” and usable for evacuation by police personnel.
 - 4. Evacuate in order of priority:
 - a. Initial target area first (if possible) for the evacuation of injured persons.
 - b. Floor above and floor below.
 - c. Top – down.
 - d. Inside – out.
- B. Evacuate to at least 500 feet from target area in area providing cover and concealment.
- C. Schools pose unique situations and should be handled as follows:
 - 1. Teachers and classes will be notified of evacuation by police personnel and in some cases utilizing the school’s intercom system.
 - 2. If classes are notified in person by police personnel, instructions are to be followed explicitly.
 - 3. If notification is by intercom, specific instructions will be given.
 - 4. As students and staff evacuate, they shall be instructed to move swiftly and quietly.
 - 5. No student will be permitted to go to their locker or any other location following the announced evacuation route.
 - 6. School staff should be the last to leave their assigned areas.
 - 7. Leave door and windows open. Open all shades and blinds.
 - 8. Leave all room/building lighting alone.
 - 9. As the students leave, supervisors should try to turn off all electrical apparatus such as typewriters, calculators, fans and computers.

VIII. Procedure: Incident Command System

- A. Command and control issues are paramount when dealing with large-scale crisis events, such as disseminating information and coordinating resources. The quick and prompt establishment of the incident command system will enhance the probability of a swift resolution and shall occur simultaneous to or shortly following the organization and deployment of contact and rescue teams.

- B.** The incident commander shall immediately implement the incident command system as established in Chapter 5 Section 46.1.1 of the Operations Manual to include the following:
 - 1.** Establish a secure perimeter to maintain containment of the incident.
 - 2.** Establish a secure location for public sheltering of any persons evacuated due to the incident.
 - 3.** If necessary, obtain support from other public safety agencies and other resources.
 - 4.** Establish a command post.
 - 5.** Initiate the notification of the following functions as needed:
 - a.** Operations Function.
 - b.** Planning Function.
 - c.** Logistics Function.
 - d.** Finance/Administration Function.
 - 6.** Establish a staging area for any additional personnel.
 - 7.** Utilized the public information officer to provide public notification for awareness and safety as well as handling all media inquiries.
 - 8.** Designate a safety officer to maintain the safety of all personnel.

IX. Procedure: Post Incident

- A.** Once the incident is under control, the incident commander may release resources as appropriate.
- B.** The command element of each function of the incident command system shall complete a detailed after action report summarizing the activity of their function during the incident.

Chapter 5: Law Enforcement Operations
Section 46: Critical Incidents, Special Operations and Homeland Security
Subsection 2: Special Operations



Policy/Procedure #: 2

Title: Suburban Emergency Response Team

CALEA Reference#: 46.2.1, 46.2.2, 46.2.3, 46.2.4

I. Policy: Suburban Emergency Response Team

The Urbandale Police Department shall maintain a team of officers trained to respond and assist with situations in which specialized training can be employed to minimize the risks, injury, or death to law enforcement personnel and citizens. To meet this obligation, the Department shall utilize and be a participating agency of the Suburban Emergency Response Team (SERT). This policy shall establish guidelines for the Urbandale Police Department to utilize and participate in SERT.

II. Procedure: SERT Activation and Deployment

A. The Urbandale Police Department is a participating agency of the Suburban Emergency Response Team. Being a participating agency, the Department will adhere to the policies and procedures outlined in the SERT standard operating procedure.

B. The Urbandale Police Department shall utilize SERT in the following situations:

1. Execution of search warrants and/or arrest warrants that present unusual hazards.
2. Hostage/barricade situations.
3. Riot or civil disturbance.
4. Containment of a civil or natural disaster.
5. V.I.P. protection.
6. Coverage of special events.
7. As deemed necessary by the Chief of Police or designee.

C. Any supervisory personnel may request assistance from SERT for emergency situations. When SERT is requested, the Chief of Police and the division commander of the division requesting assistance shall be

notified as soon as practical. Use of SERT for preplanned activities shall be approved by a division commander or the Chief of Police.

- D. Specifically for preplanned activity, as much advance notice as practical shall be given to SERT.
- E. Requests for assistance from SERT shall be handled per SERT standard operating procedure.
- F. SERT shall be a tactical resource for the incident commander of an event but shall not assume command or manage the event. Command of the event shall remain with the Urbandale Police Department. The SERT commander shall have operational control over tactical deployment. All tactical decisions shall be made by the SERT commander.
- G. SERT members shall notify a supervisor within the division they are currently assigned for normal duties when they are activated for any operation to include scheduled and emergency situations. The supervisor shall approve or deny participation by the SERT member based on manpower needs and other factors. SERT members working in the Patrol Division may utilize the on-duty sergeant to satisfy notification requirements.
- H. All training for SERT operators shall be a scheduled event with set hours. Additional time needed beyond the established schedule shall have pre-approval from the Patrol Division Commander.

III. Procedure: Search Warrant and Arrest Warrant Evaluation

- A. Any officer serving a search warrant or an arrest warrant shall complete the SERT Risk Analysis/Threat Assessment for Planned Operations.
- B. The completed SERT Risk Analysis/Threat Assessment for Planned Operations shall be submitted to a supervisor for review.
- C. The supervisor shall use the threat assessment score as part of the review. The threat assessment score shall be considered in the following manner:
 - 1. 1 - 16 Points: Use of SERT is optional. Circumstances may still warrant use of SERT.
 - 2. 17 - 24 Points: SERT shall be consulted. The SERT commander or designee shall make the final recommendation for use of SERT based on the totality of the situation.
 - 3. 25+ Points: Use of SERT is required. Only exigent circumstances would warrant proceeding without use of SERT.
 - 4. Supervisors may consult the SERT commander and/or request assistance from SERT for any situation regardless of the threat assessment score based on the totality of the circumstances involved.
- D. The following situations do not require SERT Risk Analysis/Threat Assessment for Planned Operations:
 - 1. The location to be searched has already been secured by law enforcement.

2. The location to be searched is known to be vacant or is under control by a third party that offers no threat to law enforcement (e.g. a business, bank, vehicle, etc.).
3. A felony arrest warrant has been acquired but officers are not actively attempting to serve the warrant or are unaware of the location of the suspect.
4. The situation confronting law enforcement was not preplanned (e.g. traffic stop, routine call for service).
5. The arrest warrant is not a felony offense and there is nothing to indicate the subject named in the warrant would present a threat to law enforcement if confronted.

IV. Procedure: Selection of personnel to participate in SERT

- A. Selection of personnel to participate as a member of SERT as an operator, marksman/observer or a crisis negotiator shall be handled as a collateral duty assignment as established in Chapter 2 Section 16.2.1 of the Urbandale Police Department Operations Manual.
- B. All personnel selected for a collateral duty assignment with SERT will also be required to meet all SERT requirements prior to appointment. The Department and SERT selection process shall combine to assess the applicant's potential performance and mental suitability for tactical team assignment.
- C. Officers selected as a member of SERT shall be provided with the appropriate equipment by the Department as established in the SERT standard operating procedure.

Chapter 5: Law Enforcement Operations
Section 46: Critical Incidents, Special Operations and Homeland Security
Subsection 2: Special Operations



Policy/Procedure #: 6
Title: VIP Security
CALEA Reference#: 46.2.6

I. Policy: VIP Security

A policy is established to provide enhanced security of very important persons (VIP). Due to their position or notoriety, VIPs create a special set of circumstances the Department must be prepared to handle. Procedural guidelines shall be established to assist department personnel in the response to a visiting VIP.

II. Procedure: VIP Security

- A.** All requests for VIP security shall be forwarded through the chain of command to the Chief of Police for approval. Relevant information including dates, times, and levels of security needed shall be included in the request.
- B.** Guidelines for providing security for VIP protection shall be as follows:
 - 1.** Advance notice the VIP will be within the jurisdictional area of the Department.
 - 2.** The VIP, due to notoriety or position, clearly faces unusual safety risks.
 - 3.** The ability of the Department to meet the necessary requirements to provide adequate protection for the duration of the visit.
- C.** Once notified, the Chief of Police will review and determine if the Department will determine the level of participation in the security operation. If participating, the Chief of Police will assign responsibility for the security assignment to a particular division. The division assigned the security assignment shall be responsible for coordinating all activities.
- D.** The division responsible for the security of the VIP shall develop a detailed event plan. The plan will be presented to the Chief of Police for review and approval. The plan shall contain but not be limited to the following information:

1. Dates and times of arrival and departure.
 2. Intelligence information including any known threats.
 3. Personnel assignments.
 4. Equipment needs.
 5. Emergency services (e.g. ambulance, medical facility).
 6. Mutual aid assistance.
 7. If needed, method of identification for personnel involved (e.g. lapel pins, special identification cards, etc).
 8. Radio communications.
 9. If needed, maps of known travel routes, structures, or area to be secured.
- E.** The division commander or designee responsible for the security of the VIP shall be the main point of contact between the Department and VIP staff for planning and coordination.
- F.** When provided for and approved in the plan, the division responsible for the security of the VIP may request mutual aid assistance.
- G.** The Suburban Emergency Response Team (SERT) may be utilized to provide various aspects of VIP security. Requests for SERT assistance shall be handled via SERT standard operating procedure.
- H.** When able, the Department shall honor any mutual aid requests for assistance from other law enforcement agencies performing VIP security. The Department shall require agencies requesting assistance to provide a detailed plan prior to assignment of personnel.
- I.** An after action report shall be submitted to the Chief of Police by the division responsible for the security event.

Chapter 5: Law Enforcement Operations
Section 46: Critical Incidents, Special Operations and Homeland Security
Subsection 2: Special Operations



Policy/Procedure #: 7
Title: Special Event Planning
CALEA Reference#: 46.2.7

- I. Policy: Special Event Planning**
A policy is established to ensure certain criteria are met for a special event in which planning is essential to success.
- II. Procedure: General**
 - A.** Written plans shall be drafted for handling of special events that require a planned response.
 - B.** The division with responsibility for the event, as established by the Chief of Police, shall be responsible for the development of the written plan for the event.
 - C.** Letters of instruction shall be distributed to all personnel affected by the plan. When necessary or helpful, letters of instruction shall be distributed to persons outside the Department for coordination of activities.
 - D.** Letters of instruction shall be self-canceling. After the event to which the letter described is over, procedures outlined in the letter of instruction no longer apply.
- III. Procedure: Special Event Plan**
 - A.** The special event plan shall designate a specific person or position as the supervisor and coordinator for each event.
 - B.** The plan shall be completed in advance of the event and vetted through the command staff leaving enough time to make adjustments if needed.
 - C.** The special event plan shall contain the following information:
 - 1.** Dates and times of event and location.
 - 2.** If needed, a written estimate of traffic, crowd control and crime problems expected for any given event.
 - 3.** If needed, contingency plan for traffic direction and control.
 - 4.** Use of personnel and their responsibilities.

5. If needed, procedures for coordinating activities inside and outside the agency that are involved with the event.
 6. If needed, names of persons to be contacted at other involved agencies.
 7. If needed, supplementary materials, such as maps, charts, etc.
 8. Names of department personnel who will work during the special event, their assignments and estimated hours of work.
 9. Designation of department employee(s) that will supervise and/or coordinate personnel handling the event.
 10. Communications procedures, radio identifiers and special communications equipment to be used during the event.
 11. If needed, procedures for providing relief for personnel handling the special event.
 12. If needed, transportation requirements, vehicle assignments and procedures for involved personnel.
 13. Procedures for ending the event and for notifying involved personnel they are released from duty.
 14. Evaluation and after-action report.
- D. An after action report shall be completed by the supervisor in charge of the special event and presented to the Chief of Police for review.

Chapter 5: Law Enforcement Operations
Section 46: Critical Incidents, Special Operations, and Homeland Security
Subsection 2: Special Operations



Policy/Procedure #: 8
Title: Event Deconfliction
CALEA Reference#: 46.2.8

I. Policy: Event Deconfliction

A policy is established to utilize event deconfliction during police investigations to increase the safety of agency personnel, prevent duplication of investigative/intelligence efforts, and enhance case development.

II. Procedure: General

- A.** Event/Target Deconfliction is a mechanism where specifically identified field operational activities are submitted into an approved information sharing system to determine if other law enforcement agencies are investigating the same event or target.
 - 1.** Event – A location that can be deconflicted using an address, an intersection, or latitude/longitude coordinates.
 - 2.** Target – A person, business, phone number, vehicle, or e-mail address.
- B.** All information entered into a deconfliction system will be considered confidential and law enforcement sensitive. Employees shall be held accountable for and must be able to articulate the legitimate law enforcement purpose for the use and dissemination of submitted and received information.
- C.** Notice of a conflict shall not be considered intelligence information for distribution. Contact must be made and approval gained from any contributing agency in which there is a conflict prior to distribution of the information outside of the employees directly involved in the investigation.
- D.** Employees must always use necessary precautions regardless of deconfliction. Deconfliction systems are only able to deconflict received information. Other law enforcement agencies may be pursuing an investigation on the same event or target and fail to submit the information for deconfliction.

- E. If at any time Patrol Division personnel initiate proactive enforcement operations that are considered an event as listed in this policy, they shall contact a criminal investigation division supervisor to deconflict the event. Exempt from deconfliction are active calls for service, misdemeanor warrant service within the City of Urbandale, and situations involving exigency.

III. Procedure: Qualifying event and Contact resources

- A. The Department shall utilize Mid States Organized Crime Information Center (MOCIC) RISSafe for deconflicting all events of a non-drug related nature. To enter an event log onto www.riss.net and complete the necessary fields or call the 24 hour back up phone line 1-800-952-5258. Provide the most accessible contact information (cell phone number, email, or land line) should RISSafe need to make notification of a conflict.
- B. The Department shall utilize High Intensity Drug Trafficking Area (HIDTA) for deconflicting all events of a drug related nature. To enter an event log onto www.watchcenter@midwest-hidta.org and complete the necessary fields or call the 24 hour phone line 1-877-374-8523. Provide the most accessible contact information (cell phone number, email, or land line) should HIDTA need to make notification of a conflict.
- C. An event requiring deconfliction shall be any of the following:
 - 1. Preplanned search warrant
 - 2. Preplanned serving of an arrest warrant
 - 3. Decoy operations
 - 4. Undercover operations
 - 5. Buy-bust operations
 - 6. Preplanned non-warrant investigation (i.e. knock and talk)
 - 7. Controlled delivery
 - 8. Covert operations
 - 9. Surveillance operations
 - 10. Any other event as deemed necessary or beneficial by the primary case agent or a supervisor.
- D. Alcohol and tobacco compliance checks are exempt from the requirements of this policy.
- E. Incidents involving exigent circumstances, where immediate law enforcement action is imperative, shall not require deconfliction.

IV. Procedure: Authorized users and administrators

- A. The Criminal Investigations Division Commander or designee shall be the administrator of all deconfliction systems utilized by the Department.
- B. All sworn personnel assigned to the Criminal Investigation Division as well as the administrative personnel utilized for crime analysis shall be authorized to enter events into the deconfliction systems and shall maintain active accounts to enter said information.

- C. Detectives assigned to the Mid Iowa Narcotics Enforcement Drug Task Force (MINE) may also utilize criminal analysts assigned to the task force to enter events into the deconfliction system.
- D. Prior to use, all personnel authorized to enter events into either deconfliction system shall receive training on the proper use of the system and activate their own account and secure access.

V. Procedure: Processing conflicts

- A. Sufficient case details to alert the users and provide appropriate conflict information shall be provided; however, additional details provided on the event or target will allow the systems to work at its full capacity. Supplying information beyond what is required by the systems for entry shall be at the discretion of the case officer or their supervisor.
- B. When either RISSafe or SAFETNet discovers a conflict, the submitting employee shall immediately be notified and informed of the conflict. Employees shall not be considered notified until at least one submitter has been personally notified of the conflict. Voicemail or messages left with an individual will not be considered notification. Upon receiving a voicemail, the primary or secondary submitting person shall contact the deconfliction center to officially acknowledge the notification.
- C. When a conflict exists, the primary case agent or their supervisor shall be required to contact the other agency prior to any further operations. Information regarding a conflict shall only be distributed to those employees and supervisor involved in the event.

Chapter 5: Law Enforcement Operations
Section 46: Critical Incidents, Special Operations, and Homeland Security
Subsection 2: Special Operations



Policy/Procedure #: 9
Title: Hostage/Barricaded Situations
CALEA Reference#:

I. Policy:

In a hostage/barricaded person situation, it shall be the policy of the Urbandale Police Department to conduct a coordinated response to enhance the prospects of a peaceful resolution. Involved officers must recognize they do not control the suspect; they do control their own actions and shall focus their initial effort on avoiding unnecessary suspect confrontation, absent a compelling reason to do otherwise. This coordinated response shall include containment, negotiations, tactical responses, and in hostage situations, every reasonable effort to obtain the safe release of the hostages.

II. Procedure: General

- A.** A hostage is a victim, held against his/her will by the threat of, or actual use of force. No distinction shall be made as to how or why the victim was taken hostage.
- B.** A barricaded person is any individual in a strong position who is reasonably believed to be a threat to commit serious physical injury or death to themselves, officers, or others in the community.
- C.** The safety of involved persons shall be prioritized as follows:
 - 1.** Hostages/Innocent bystanders
 - 2.** Officers
 - 3.** Subject/suspect(s)
- D.** During a hostage situation, the jeopardy to the hostage is continuous and uninterrupted until they are released. Although tensions may rise and fall, it is only an indicator of the temporary safety of the hostage(s). The hostage(s) shall never be considered safe until they are secured by authorities.
- E.** Because the victim is in constant danger while being held hostage, the Department will make every attempt to secure the hostage(s) release at the earliest opportunity. It may be necessary to rescue the hostage(s) at the

- expense of the hostage taker.
- F. If a hostage rescue is necessary, the primary mission shall be to rescue the hostage(s). All other missions (e.g. arrest, securing evidence, etc.) are subordinate.
 - G. Once released and in police custody, an officer shall be assigned to maintain direct control over the hostage(s) until they have been debriefed. At the conclusion of their debriefing, hostage may be released to a responsible party (family member, clergy, social services, support group, etc.) based on the circumstances of the incident. It may be necessary to maintain control of the hostages to prevent interference with the incident (e.g. hostage was a family member).
 - H. Hostage negotiation is the recommended course of action on most incidents. Negotiation as a starting point will produce valuable information should it be necessary to utilize tactical approaches.

III. **Procedure: Responsibilities**

- A. When WestCom Emergency Communications Center (WestCom) becomes aware a hostage/ barricade situation has developed, they will immediately direct a patrol supervisor to respond. The dispatcher shall:
 - 1. Establish priority channel and additional designated channels as needed.
 - 2. Relay all pertinent information to officers concerning safe routes of travel, location of staging area, individual assignments, etc.
 - 3. Implement call out and notification as directed by a supervisor.
- B. Patrol officers confronting hostage/barricaded incidents shall not initiate tactical actions other than those necessary to protect the lives and safety of others as listed in the safety priorities above. Officers shall then:
 - 1. Deploy utilizing a controlled-silent response.
 - 2. Do not assault the suspect(s) unless Rapid and Immediate Deployment (RAID) procedures are warranted. Return fire must be based on the fact that loss of life is imminent; hostage/bystanders must be clear and the armed suspect(s) clearly visible and identifiable.
 - 3. Notify a field supervisor of the incident and request assistance.
 - 4. Contain and isolate the incident scene to as small an area as is safe and practical by establishing inner perimeter containment including disabling vehicles accessible to the subject/suspect. As time and resources permit, outer perimeter containment shall be established to control pedestrian and vehicular traffic into the area.
 - 5. In the event of an in progress violent situation, officers shall take appropriate and immediate action to stop the suspect from any further dangerous behaviors as stated in Chapter 5 Section 46.2.1 (Rapid and Immediate Deployment).
 - 6. Establish a plan to initiate RAID if the situation turns violent.
 - 7. Evacuate injured persons or those in immediate danger as soon as possible. Officers should consider the use of construction equipment or other available vehicles that can defeat the potential threat.
 - 8. Evacuation of affected residents and businesses within sight and range

of the suspect shall be accomplished as soon as practical. Persons should be moved to a point beyond the outer perimeter.

9. Begin initial Intelligence data relay to responding personnel.
 10. Establish communications with the suspects, attempt to persuade them to surrender and maintain communications. Avoid deadlines or demands.
- C.** The ranking officer on scene shall be in command until relieved by a superior. The ranking officer shall:
1. Assume command and brief officers at the scene on the incident via the radio.
 2. Acquire an initial debrief of the incident and update deployment as needed.
 3. In conjunction with WestCom, establish an alternative communication channel or request a clear channel. Ensure all officers at the scene are informed of the designated communications channel.
 4. Establish an initial react team and a plan to implement should the situation turn violent.
 5. Ensure the inner perimeter has been established and include evacuations, traffic control, and crowd control.
 - a. The inner perimeter is the immediate area surrounding the hostage scene which officers can seize and control without endangering their safety.
 - b. The scene must be isolated so physical movement into, from, and around the inner perimeter is controlled.
 - c. The only uncontrolled movement within the inner perimeter should only be the suspect and the victims.
 - d. If possible, the creation of the inner perimeter should be accomplished without suspect knowledge.
 - e. After blocking the hostage-takers escape route to the outside including disabling vehicles accessible to the subject/suspect, officers should contain the situation to a specific room or floor within the building. The smaller the area controlled by the suspect the easier the containment.
 6. Ensure the outer perimeter is established including evacuations, traffic control and crowd control. The establishment of the outer perimeter provides public safety. Pedestrian and vehicular traffic must be kept outside the outer perimeter. The distance of the outer perimeter from the scene is determined by:
 - a. The location of the suspect.
 - b. Type of weapon being used.
 - c. Number of available officers for control purposes.
 - d. Uniformed officers should be used to evacuate persons in the outer perimeter to eliminate problems with identification and lengthy explanations to citizens.
 - e. Evacuation shall be attempted only if it does not expose these persons to unnecessary danger.

7. Based on the conditions at the scene, initiate the incident command system as established Chapter 5 Section 46.1.1(Critical Incidents).
8. Select an initial command post site and identify a safe staging area (considering location, accessibility, and safety) and safe approach route for all responding officers.
9. Ensure WestCom is directing responding personnel to the designated staging area.
10. Develop required police information on the suspect(s) and hostages. Disseminate descriptive data, weapons, location, etc., on the suspect and hostages.
11. Evaluate the situation using the following criteria:
 - a. What criminal act has been committed?
 - b. Are the suspect(s) armed? If yes, with what type of weapon?
 - c. Have the suspect(s) barricaded themselves?
 - d. Have the suspect(s) refused to surrender to police custody?
 - e. Are the suspect(s) a threat to life and safety of citizens, hostage(s) and law enforcement officers?
 - f. Is the situation beyond the capability of patrol personnel?
- D. If the situation warrants, request the activation of SERT and make the appropriate command staff notifications.
- E. If appropriate, ensure Fire and EMS services are available at the staging area.
- F. If appropriate, notify the Department's public information officer and establish a restricted area for media relations beyond the outer perimeter.
- G. Attempt to create an accurate floor plan of the structure.
- H. Continue containment until directed otherwise by the incident commander.

IV. Procedure: Special Considerations

- A. When the hostage is a visiting VIP or a foreign official/official guest the jurisdiction may be shared concurrently by the Federal Bureau of Investigation and the Department. When control has been initiated by the Department, operational command is retained until assumed by the Federal Bureau of Investigations. If a determination is made for concurrent jurisdiction, joint decision making will be undertaken by the incident commander and the senior F.B.I. agent at the scene. Every effort should be made to ensure mutual agreement in the decision making process prior to conducting tactical operations.
- B. If the hostage situation results from the commission of a federal crime (e.g. bank robbery), the jurisdiction shall be concurrently shared. If the initial control of the operation is held or maintained by the Department, it will be retained until such time as another appropriate agency relieves the Department of the incident responsibilities.

Chapter 5: Law Enforcement Operations
Section 46: Critical Incidents, Special Operations and Homeland Security
Subsection 3: Homeland Security



Policy/Procedure #: 1

Title: Terrorism

CALEA Reference#: 46.3.1, 46.3.2, 46.3.3

I. Policy: Terrorism

A policy is established to ensure the exchange of information relating to terrorism with the appropriate task force, law enforcement agency, or other entity with a need and right to know. Distribution of informational materials to encourage citizen reporting shall also be addressed.

II. Procedure: Liaison With Other Agencies

- A.** The Urbandale Police Department is a member of the Iowa Law Enforcement Intelligence Network (LEIN) Region 5 Fusion Center, which in turn is a part of the FBI's Joint Terrorism Task Force (JTTF).
- B.** The Iowa LEIN Region 5 Fusion Center and JTTF serve as liaisons with other organizations for the exchange of terrorism-related information.
- C.** The Chief of Police and the Commander of the Criminal Investigations Division shall serve as the Department's representatives on the JTTF.

III. Procedure: Reporting Terrorism or Terrorism Intelligence Information

- A.** Officers who make contact with a subject who is suspected of terrorism-related activities will contact their immediate supervisor before releasing the individual.
- B.** The immediate supervisor will determine if an investigator, the department's JTTF liaison, and/or appropriate federal authorities should be notified and respond to the scene.
- C.** All subjects detained for terrorism-related activities will be fingerprinted and photographed in compliance with applicable federal, state and local statutes.
- D.** A thorough vehicle search and inventory is desirable on any vehicle suspected of being involved in terrorism-related activity. The Department policies regarding vehicle search and seizure apply and if necessary,

consent or a search warrant will be obtained. Any search or inspection will include photographing and forensic processing as appropriate under the circumstances.

- E. Any officer receiving intelligence/information concerning possible terrorism-related activities will immediately notify their supervisor and complete an incident report. The supervisor will determine the validity of the information and the appropriate response from the Department. This may include notification of the Department's JTTF liaison who will in turn notify other local law enforcement agencies, or the appropriate state and federal agencies as necessary.
- F. In cases where the JTTF liaison is not immediately available or the information is extremely critical and time-sensitive, a command officer can directly forward the information to the FBI.
- G. If the information was developed from a crime that occurred within the jurisdiction of the Urbandale Police Department, the crime will be documented on a case investigation report (CIR). The case will be assigned to the Criminal Investigations Division for follow-up.

IV. Procedure: Relaying Terrorist Intelligence Information To Department Personnel

- A. After receiving terrorism-related information, the JTTF liaison shall determine if the information may be forwarded to department personnel with a need and right to know. Reporting information to department personnel may be in the form of a bulletin, command staff memorandum, telephone notification, roll-call briefings or other available means depending on the nature of the information and type of threat.
- B. General intelligence related to terrorist activities produced for law enforcement by the Region 5 Fusion Center, FBI, the Department of Homeland Security and others may be distributed to sworn officers by the department's JTTF liaison or designee. This information will be treated as confidential unless otherwise stated.

V. Procedure: Terrorism Awareness Information

- A. As part of the community outreach programs provided by the Urbandale Police Department, information on how to report suspicious activity related to terrorist activities shall be presented.
- B. Through the Support Services Division, the Department shall provide the public with updated public information about terrorism.

Chapter 5: Law Enforcement Operations
Section 46: Critical Incidents, Special Operations and Homeland
Security
Subsection 3: Homeland Security



Policy/Procedure #: 2
Title: Hazardous Materials
CALEA Reference#: 46.3.2

I. Policy: Hazardous Materials

A policy is established to ensure officers responding to the scene of a hazardous materials incident have the basic knowledge necessary to protect themselves and others within the community.

II. Procedure: Training

- A.** Initial awareness training for officers in hazardous materials recognition and response shall be provided by the Iowa Law Enforcement Academy or other state accredited training academy as part of the officer's State of Iowa law enforcement certification.
- B.** Officers shall receive in-service refresher training on hazardous materials recognition and response at a minimum of once every 4 years.

Chapter 5: Law Enforcement Operations
Section 46: Critical Incidents, Special Operations, and Homeland Security
Subsection 3: Homeland Security



Policy/Procedure #: 5
Title: Bomb Threats
CALEA Reference#: N/A

I. Policy: Bomb Threats

A policy is established to direct the Department's efforts when responding to suspicious devices, bombs, and bomb threats. The policy shall address response, decision to evacuate, searching, and disposal.

II. Procedure: Response

- A.** Personnel receiving information of a suspicious device, bomb, or bomb threat shall immediately notify communications. All threats will be treated in a serious manner and never assumed to be false.
- B.** Chain of command shall be immediately notified of any officer confirmed suspicious package or bomb/bomb threat.
- C.** Unless there is some compelling reason for their use, units responding to the scene shall not activate their lights or siren. Based on the information received, personnel may not want to respond directly to the location in question until the scene has been assessed.
- D.** If there is a possibility of an electronic detonating device, the patrol car radios, portables, and cell phones shall not be used in the immediate area.
- E.** When necessary, responding officers shall implement the incident command system as established in Chapter 5 Section 46.1.1 of the Operations Manual including the activation of Fire Department, EMS, and/or the Criminal Investigation Division to assist.
- F.** Under most circumstances, the decision to evacuate and physically search a property following a bomb threat shall be the responsibility of the person in charge of the property. If the following conditions exist, the Department will determine evacuation and searching parameters:
 - 1.** A suspicious device or bomb has been located.
 - 2.** Based on the totality of the circumstances, the threat seems credible.

- G. If the decision to evacuate is made, determine if the facility has an evacuation plan in place and assist in implementation. If no plan exists, command personnel in charge of the scene shall determine the most efficient and effective means to evacuate.
- H. If the decision is made to assist with a search of the property, the following procedures shall be used:
 - 1. Assemble personnel who will be participating in the search for instructions.
 - 2. Obtain a floor plan of the building if possible.
 - 3. Divide personnel into teams and assign specific areas to be searched.
 - 4. Brief teams on what to look for and how to report if anything is found.
 - 5. A person familiar with the area will be helpful in identifying those objects that belong and those that do not. When possible, have someone familiar with the area accompany each team or be available at a designated location. Note: The decision to utilize civilians shall be based on the credibility of the threat. The danger shall be explained to all civilians prior to their assistance and shall be strictly voluntary.
 - 6. Critical areas shall be searched first. Areas outside the building shall not be neglected.
 - 7. The number of personnel concentrated in one area shall be kept to a minimum.
 - 8. Refrain from utilizing light switches.
 - 9. Search personnel shall be thorough and patient.
 - 10. A log of areas searched shall be maintained to ensure the entire building and grounds have been cleared.
 - 11. The finding of a device shall be indicated by a prearranged signal.Note: Radio communications at scene shall be avoided.

III. Procedure: Location of a suspicious device or bomb

- A. If not already in effect, the commanding officer on the scene shall immediately activate the incident command system.
- B. The building and/or immediate area shall be evacuated immediately. A secure perimeter shall be established. The size of the evacuation area and secure perimeter shall be determined by the following:
 - 1. The size of the device and the projected blast radius.
 - 2. The advice of disposal experts.
 - 3. Other factors such as types of structures and populations masses nearby (e.g. schools, retail locations, residential, etc.).
- C. Fire and EMS personnel shall be placed on standby for a response.
- D. Bomb disposal personnel from the Department of Public Safety Bomb Squad shall be requested to respond. Specialized response personnel will be requesting additional information to include:
 - 1. Location of the device
 - 2. Directions to the scene/command post

- 3. Evacuation distances
- 4. Description of the device including the size
- 5. If known, the projected detonation time.
- E. At no time shall the device be handled, moved, or manipulated in any manner except by trained personnel.
- F. If one explosive device is found, a search for additional devices shall be conducted when safe to do so.

Chapter 6: Operations Support
Section 53: Inspectional Services
Subsection 1: Line Inspections



Policy/Procedure #: 1
Title: Line Inspections
CALEA Reference#: 53.1.1

I. Policy: Line Inspections

A policy is established to direct line inspections. The inspection process is a mechanism for evaluating the quality of the police operations. Line inspections provide a means of assessing the Department's effectiveness, efficiency and ability to meet its commitments. It also provides a basis for adjusting existing policy and procedure to meet continually changing needs. It shall be the policy of the Urbandale Police Department to utilize a system of line inspections as a means of ensuring compliance with its goals, policies, standards and regulations. The policy shall ensure proper documentation of findings, recommendations and corrective action.

II. Procedure: General

- A.** Line inspections shall be conducted by supervisory personnel in control of employees, facilities, procedures, or other elements. Line inspections may be carried out by any supervisor within the chain of command. Supervisory personnel shall also be responsible for ensuring any substandard conditions revealed in the inspection are corrected.
- B.** All organizational components, functions, facilities, equipment, property, activities, and personnel are subject to line inspections.
- C.** All personnel are subject to visual inspection to ensure their physical appearance complies with uniform and grooming standards.
- D.** Buildings, facilities, equipment, vehicles, supplies, etc. shall be examined to ensure they are in good condition and adequately maintained.
- E.** Direct and indirect observation of employee activity shall be utilized to ensure compliance with departmental procedures.

III. Procedure: Supervisory Responsibility

- A.** All supervisors are responsible for conducting inspections of personnel, equipment, property, and activity that fall within the scope of their immediate command or control.

- B.** When conducting line inspections, supervisors who encounter an infraction shall initiate corrective or disciplinary action. Serious infractions shall be documented on a departmental memorandum and forward up the chain of command. Included in the memorandum shall be the date, a description of the infraction and a statement of the corrective action taken or needed.
- C.** Supervisors who take or recommend corrective measures shall be responsible for conducting follow-up checks to ensure the infraction has been satisfactorily resolved.

IV. Procedure: Inspections

- A.** Informal line inspections of personnel, equipment, and activities shall be conducted on a continuous basis.
- B.** Supervisors are tasked with the duty to ensure their personnel are wearing proper uniforms and are properly groomed at roll call and at all times while on-duty. This is a daily responsibility and will continue in addition to the following:
 - 1.** Once a month, the sergeant will have an informal inspection of their personnel to ensure the grooming and uniforms of their personnel are up to the standards of the Department.
 - 2.** The sergeant will also inspect each officer's firearm and other personal equipment and ensure it is functional and clean.
 - 3.** An inspection report will be completed for each officer and placed into a file. The sergeant shall maintain the file for each officer under their supervision.
 - 4.** Sergeants may conduct random informal inspections on other days.
 - 5.** On occasion, the division commander may conduct a formal in-ranks inspection of the officers to ensure the departmental standards are being maintained.
- C.** Any department equipment, property or vehicles that during inspection are found to be in need of repair, replacement, or maintenance shall be documented on a repair/service request form and submitted to the Support Services Division. The Support Services Division shall arrange for the needed repair, replacement, or maintenance and document the resolution on the repair/service request form. When the inspection reveals a cleanliness issue that can and should be resolved by agency personnel. Support services division shall notify the appropriate division for resolution.
- D.** Vehicles shall be inspected by a supervisor of the division to which they are assigned. Vehicles assigned for daily patrol use shall be inspected every third month while other department vehicles shall be inspected annually. Cleanliness issues shall be addressed to the specific employee to whom the vehicle is assigned. When the vehicle is operated by multiple

personnel, a supervisor for the division responsible for the vehicle shall assign an employee to address cleanliness issues.

- E.** A formal facility inspection shall be completed on a monthly basis by the command staff. Any deficiencies or conditions of noncompliance shall be assigned to Support Services Division for resolution unless the problem is directly related to another division.
- F.** Formal line inspections of departmental equipment and property shall be conducted by the Support Services Division as needed or at the request of the Chief of Police. This inspection shall not include the facility, vehicles, or items listed in the personnel inspection report.
- G.** Formal line inspections shall require a written report by the inspecting supervisor. The inventory software program can be utilized to meet the reporting requirements. Additional reporting of items not listed in the inventory software program shall be listed on the facility/general item inspection report. The inspection report shall include the following:
 - 1.** The object being inspected.
 - 2.** The current status or condition.
 - 3.** Any deficiencies or conditions of non-compliance.
 - 4.** Corrective actions taken or recommendations for correction or improvements.

Chapter 6: Operational Support
Section 53: Inspectional Services
Subsection 2: Staff Inspections



Policy/Procedure #: 1
Title: Staff Inspections
CALEA Reference#: 53.2.1

I. Policy: Staff Inspections

A policy is established to guide command staff on staff inspections. Staff inspections are utilized to determine if policies, procedures, and regulations are being carried out as designed. Staff inspections will help determine if the desired goals of the Department are being obtained and if personnel and resources are being utilized to the fullest extent possible.

II. Procedure: Staff Inspections

- A.** Staff inspections of all divisions shall be conducted by the commander of the Support Services Division or designee. If the need exists, the Chief of Police may order a staff inspection of the Support Services Division by a commander outside of the division.
- B.** Staff inspections of each division shall occur every four years. Staff inspections should not occur within six (6) months of a CALEA assessment.
- C.** At the conclusion of a staff inspection, a written report shall be submitted to the Chief of Police detailing the findings. The written report shall detail any deficiencies noted during the inspection and recommendations to correct said deficiencies. The report shall also note positive aspects noted during the inspection.
- D.** If any deficiencies are noted in the report that were not immediately correctable, a follow up report detailing the measures taken to correct the deficiencies shall be submitted to the Chief of Police by the division commander responsible. A copy of the report shall be forwarded to the author of the original staff inspection report.
- E.** Staff Inspections shall be conducted in the following manner:
 - 1.** A thirty day notice should be given to the division to be inspected.

2. Once started, a staff inspection of a division shall be completed within thirty (30) days. Extensions to complete the inspection may be granted by the Chief of Police.
3. The division being inspected may assign a liaison to assist the inspector with gathering needed information. This liaison shall be someone that is knowledgeable about the division but shall not be the division commander.
4. Interviews may be held with various personnel from the division as part of the inspection process.
5. The inspector's focus should include but not be limited to the following:
 - a. Are the policies, procedures, rules and regulations being carried out as prescribed?
 - b. Is there a need for additional or a revision of current policies, procedures, rules and regulations?
 - c. Does the division have adequate resources to obtain its goals?
 - d. Are resources being utilized to the fullest extent possible?
 - e. Are there deficiencies in integrity, training, morale, or supervision?
 - f. Are personnel adhering to line inspection requirements?
- F. The commander of the division being inspected shall not attempt to influence the inspector or change normal operations prior to the inspection in an attempt to influence the outcome of the inspection report.

Chapter 6: Operations Support
Section 54: Public Information
Subsection 1: Public Information



Policy/Procedure #: 1

Title: Public Information and Social Media Use

CALEA Reference#: 54.1.1, 54.1.2, 54.1.3, 54.1.4

I. POLICY: Public Information

The Urbandale Police Department shall be committed to the release of public information and the use of social media to maintain a well-informed community. Liaisons shall be established with area media personnel to facilitate this activity. The department shall designate personnel to facilitate the dissemination of information and formal press releases.

The Department endorses the use of social media to enhance communication, collaboration, and information exchange with citizens and increase effectiveness of investigations. This policy establishes the Department's position on the utility and management of official department social media accounts and provides guidance on its management, administration and oversight.

The Department also recognizes the role social media plays in the personal lives of some department personnel. The personal use of social media can have a bearing on departmental personnel in their official capacity. Department personnel must be credible, unbiased, and impartial to effectively perform their duties for the Urbandale Police Department. Personnel are cautioned that improper social media use can have a negative impact on both their credibility and the Department's reputation.

This policy is not meant to address a particular form of social media, but social media in general, as advances in technology will occur and new tools will emerge.

II. PROCEDURE: Release of Information

- A.** The Urbandale Police Department shall establish personnel as public information officers. Public information officers shall report to the Support Services Division chain of command. Public information officers shall be responsible for releasing information to the public or the media in the form of official press releases. All official press releases will require a secondary review for editing of content, formatting, and a properly affixed disclaimer notices. The Support Services Division Commander or designee shall approve all media releases by the public information officers. The document will be forwarded to the Chief of Police or designee for final approval before release.
- B.** In addition to releasing information to the public or the media, the public information officer shall be responsible for the following:

 - 1. Coordinating and authorizing the release of information about victims, witnesses and suspects.
 - 2. Assisting in crisis situations within the agency.
 - 3. Maintaining an accurate contact list for all area media organizations.
 - 4. Arranging for and assisting at media conferences.
- C.** Personnel assigned as a public information officer for the Department shall receive appropriate training for the position. The training may include departmental training from experienced public Information officers and/or training classes offered by outside agencies/organizations.
- D.** When multiple agencies are involved in an incident in which a media release is needed, a joint release is preferred to each agency releasing their own information. This will eliminate confusion, differing accounts of the events, and be more efficient and effective. The following procedures shall be utilized by the Department for releasing information when other public service agencies are involved in a mutual effort:

 - 1. The public information officer or a supervisor shall make contact with the public information officer or other official from the involved agencies to coordinate a joint information release. A designation as whose public information officer or supervisor will be handling the actual release shall be established and agreed upon by all involved agencies.
 - 2. In cases where the Urbandale public information officer or supervisor is not handling the release, the public information officer or supervisor shall act as the liaison with the other agencies designee(s) and ensure the commander of the division involved in the incident and the Chief of Police are notified of the content and the expected date and time of any joint release as well as approval from the Chief of Police to include the Urbandale Police Department.
 - 3. In cases where the Urbandale public information officer or a supervisor is tasked with providing the joint release to the media, the internal approval process utilized for media releases shall be employed. In addition, the public information officer or supervisor shall receive approval from all other agencies involved prior to the release.

4. Media releases from multi-jurisdictional task force operations shall be handled by task force supervisory personnel or designees. The Urbandale supervisor of personnel assigned to the task force shall notify the division commander and the Chief of Police when the media release directly involves an Urbandale officer or the event occurs within the City of Urbandale.
 5. Nothing in this policy shall preclude the Department from issuing its own media release.
- E. If the information released to the public or the media involves the release of official police documents or statistical data, the Support Services Division commander or designee shall be notified.
 - F. The Criminal Investigation Division Commander or designee shall be consulted prior to releasing any information pertinent to an active investigation. Personnel shall not divulge evidence or confidential matters related to an active investigation. Information which might hamper an investigation, prevent the arrest of a wanted person, or interfere with the apprehension or interrogation of a suspect shall not be released.
 - G. The Chief of Police or a division commander may release information directly to the public or the media without the use of the public information officer.
 - H. Release of information or refusal to release information to the media shall be conveyed to the Chief of Police at the earliest convenience. Unless the incident is unusual, "police blotter" information released to the media does not require notification to the Chief of Police.
 - I. When the media responds to the scene of an incident, a supervisor may request the public information officer to respond. If able to respond to the scene, the public information officer shall handle all media relations. Release of information at the scene requires the same permission and review as stated above.
 - J. At the scene of an incident, it shall be the duty of the supervisor or the public information officer to establish physical boundaries with the media. The boundaries shall ensure unimpeded response to the incident by emergency personnel as well as accessibility of media to cover the event. At no time shall media access expose anyone to additional risks. The arrival and handling of the media at an incident shall be documented by the officers involved. This shall include:
 1. The media agency(s) responding.
 2. Creation or review of media staging area (i.e. did they need to be moved or was initial set up sufficient). When practical, crime scene tape shall be utilized to designate the media staging area.
 3. A photograph of the media staging area may be included as an attachment to the case.
 4. Any interaction, to include statements given.
 - K. When the public information officer is unable to respond to the scene, the supervisor on scene may issue a brief media release confirming basic news information such as the existence of a crime or incident, to include

location; however, all additional information will be referred to the public information officer or division commander. On all major crimes or serious incidents, any information beyond the confirmation of the crime and location will be released by the public information officer, division commander, or the Chief of Police.

- L.** Authorized news media representatives shall be permitted to take pictures of incidents occurring on public property or highways so long as they do not delay police investigation or the efforts of police personnel to administer to injured persons.
- M.** The Department shall extend full cooperation to bona fide representatives of the media consistent with this policy. Department personnel shall be fair and impartial and show no favoritism for one media organization over another. The Department shall furnish to the media information of news value relating to the cases and incidents that come to police attention except in the following circumstances:
 - 1.** The information is restricted under the code of Iowa, chapter 692 or chapter 22.
 - 2.** The information is restricted under Iowa rules of professional conduct 32:3.6 and 32:3.8.
- N.** Any disagreement or misunderstanding between department personnel and the media concerning release of information that cannot be resolved at the division level shall be referred to the Chief of Police.
- O.** The Department shall involve the media in the development of or changes in policies and procedures relating to the public information function. By allowing media representatives to participate in the process of developing policies and procedures relating to the public information function, agencies can receive input that may lead to more effective working relationships between department and media personnel.
- P.** Any written communication which includes information a defendant will be or has been charged with a crime must also include a statement explaining a criminal charge is merely an accusation and the defendant is presumed innocent until and unless proven guilty.
- Q.** In addition to the restrictions stated above, the following restrictions shall apply:
 - 1.** Statements of policy, administration, and disciplinary action shall be released only by the Chief of Police or designee.
 - 2.** Confidential sources of information or names of informants shall be strictly guarded.
 - 3.** Personal observations about character shall not be released.
 - 4.** Information on procedures such as ballistic tests, laboratory tests, or other tests shall not be released.
 - 5.** Identity of any prospective witnesses shall not be released.
- R.** All official media releases shall be documented for future reference. The information shall be retained by the Support Services Division and contain the following:
 - 1.** A copy of the media release and any accompanied documents.

2. Identification of who made the release.
3. Identification of who authorized the release.
4. A list of all persons or organization that received the release information.

III. Procedure: Departmental Sponsored Social Media

A. Definitions:

1. Blog: A self-published diary or commentary on a particular topic that may allow visitors to post responses, reactions, or comments. The term is short for "Web log."
2. Page: The specific portion of a social media website where content is displayed, and managed by an individual or individuals with administrator rights.
3. Post: Content an individual shares on a social media site or the act of publishing content on a site.
4. Profile: Information a user provides about himself or herself on a social networking site.
5. Social Media: A category of Internet-based resources that integrate user-generated content and user participation. This includes, but is not limited to, social networking sites (Facebook, MySpace), microblogging sites (Twitter, Nixle), photo- and videosharing sites (Flickr, YouTube), wikis (Wikipedia), blogs, and news sites (Digg, Reddit).
6. Social Networks: Online platforms where users can create profiles, share information, and socialize with others using a range of technologies.
7. Web 2.0: The second generation of the World Wide Web focused on shareable, user-generated content, rather than static web pages. This term may be used interchangeably with social media.
8. Wiki: Web page(s) that can be edited collaboratively.

B. The Chief of Police shall approve the creation of all official department social media accounts.

C. Operation of department social media will be conducted by Support Services Division staff. Support Services Division staff, investigators, patrol sergeants, and command staff are authorized to use departmental social media. Support Services Staff will maintain and control passwords to social media sites. Those operating social media sites for the Department shall conduct themselves at all times as representatives of the Department and adhere to all department policies, rules, and regulations.

D. Requests to post information over departmental social media by employees who are not authorized to post shall be made through the employee's chain of command.

E. Social media postings after hours shall be completed on departmental issued cell phones or electronic devices. Any posts that occur during off duty time shall be approved by a Support Services Division supervisor.

IV. Procedure: Guidelines for Departmental Social Media

A. Support Services Division supervisors shall be responsible for monitoring and approving all posts to department social media sites. Support services

supervisors may designate a member of the Department to make general posts to the department social media accounts that are minor in nature without seeking additional approval. Examples of minor posts include safety messaging or upcoming departmental events. The Investigation Division shall have the authority to post requests to identify suspects and witnesses as needed to further their investigations.

- B.** In general, the following guidelines shall be followed when posting information on department social media sites:
 - 1. Where possible, the page(s) should link to the department's official website. Social media pages shall clearly indicate they are maintained by the Department and shall have department contact information prominently displayed.
 - 2. Social media content shall adhere to applicable laws, regulations, and policies, including all information technology and records management policies.
 - 3. Content is subject to open government laws. Relevant records retention schedules apply to social media content. Content must be managed, stored, and retrieved to comply with open government laws, records retention laws, and e-discovery laws and policies.
 - 4. If a visitor to an official department social media account posts comments that are off-topic, threatening, inappropriate, contain obscenities, or personal attacks they may be banned or blocked from visiting and posting to the social media account by a supervisor. Any unwanted posts or comments shall be saved as evidence to support the ban or block.
 - 5. Pages shall clearly indicate posted comments will be monitored and the department reserves the right to remove any posting.
 - 6. Social media pages shall state the opinions expressed by visitors to the page(s) do not reflect the opinions of the department.
- C.** Departmental social media accounts and content shall adhere to applicable laws, regulations, and policies including records management and the Freedom of Information Act.

V. Procedure: Uses of Departmental Social Media

- A.** In general, the following guidelines should be followed when posting information on departmental social media websites:
 - 1. Social media can be used to make time-sensitive notifications related to:
 - a. Road closures
 - b. Special events
 - c. Weather emergencies
 - d. Missing or endangered persons
 - 2. Social media is a valuable investigative tool when seeking evidence or information about:
 - a. Missing persons
 - b. Wanted persons
 - c. Gang participation

- d. Crimes perpetrated online and photos or videos of a crime posted by a participant or observers.
- 3. Social Media can be used for community outreach and engagement by:
 - a. Providing crime prevention tips
 - b. Offering online-reporting opportunities
 - c. Sharing crime maps and data
 - d. Soliciting tips about unsolved crimes
- B. Social Media can be used by patrol supervisors for real time updates. If appropriate, patrol supervisors can access social media sites, such as twitter, to notify the commuting public of potential hazardous situations. Major incidents shall adhere to the requirements of this policy.
- C. Patrol supervisors will be provided instruction by Support Services Division personnel on how to access departmental social media sites for these purposes.

VI. Procedure: Use of Covert Social Media Sites for Investigation Operations

- A. Only the Chief of Police or Criminal Investigation Division Commander shall approve the use of any covert or undercover social media site or postings to other social media sites for undercover investigative operations. A supervisor shall be assigned to monitor the operation of the investigation.
- B. When appropriate, the prosecuting attorney with jurisdiction shall be consulted to ensure all legal requirements have been met for admissibility of any evidence obtained in operating any covert or investigative social media site or posting to other social media sites for purposes of a covert or undercover investigation.

VII. Procedure: Personal Social Media Accounts

- A. Nothing in this policy shall prohibit employees from utilizing social media in their personal lives when not functioning as an employee of the Urbandale Police Department.
- B. Employees shall not publish any statements, speeches, appearances, endorsements, or materials that would reasonably be considered to represent the views or positions of the Urbandale Police Department without expressed authorization of the Chief of Police.
- C. Photographs or other depictions of department uniforms, badges, patches, logo, and marked units shall not be used in employee personal social media accounts unless approved by the Chief of Police. The employee seeking approval to use references to the department on personal web pages or sites shall:
 - 1. Submit a request for approval to the Chief of Police via the Chain-of-Command.
 - 2. Describe the proposed reference to the Agency and purpose.
 - 3. Provide a list and media to be used on the web page.
- D. Department employees shall not post anything that includes obscene or sexually explicit language, images, or acts or statements that ridicule,

malign, disparage, or otherwise express bias against any race, religion, sexual orientation or protected classes of individuals that may provide grounds for undermining the Department or impeaching their testimony in criminal or civil proceedings.

- E. Employees shall not post acts showing participation in illegal activity.
- F. Supervisors within the Department may conduct investigations into the postings of employees for purposes of protecting the integrity and reputation of the Department, protecting the integrity of investigations, and ensuring privacy and security of departmental records and information. Any information created, transmitted, downloaded, exchanged, or discussed in a public online forum may be accessed by the Department at any time without prior notice.
- G. Department personnel shall not post information gained because of their official authority or access. Examples include but are not limited to the following:
 - 1. Photos, videos, or other depictions of the inside any building or facility/vehicle owned or in the control of the City of Urbandale.
 - 2. Photos, videos or other depictions of crime scenes or accidents scenes captured while on duty.
 - 3. Photos, videos or other depictions of departmental training, activities, work related assignments, or any activity occurring while functioning in the capacity as an employee of the Urbandale Police Department.
 - 4. Descriptions, photos/video of any activity/events witnessed while functioning in the capacity as an employee of the Urbandale Police Department.
 - 5. Photograph, name or address of an officer who works an undercover assignment.
 - 6. Personal information or address of a fellow employee.
- H. In addition to this policy, all employees are subject to the provisions of the social media policy of the City of Urbandale as established in the City Handbook.
- I. Any employee becoming aware of or having knowledge of a posting or of any website or web page in violation of the provision of this policy or the City's social media policy shall notify their supervisor immediately.

VIII. Procedure: Personal information

- A. To protect the privacy of our employees and to prevent employees and their families from harassment, no personal cell phone numbers, home phone numbers, or home address will be shared with the public without the consent of the employee.
- B. Subjects requesting an employee's personal phone number shall be directed to leave a message for the employee and it will be the employee's responsibility to contact the subject and provide any needed information as deemed necessary.
- C. Exceptions to providing an employee's personal phone number(s) shall be made in the following cases for official business needs:

1. An employee of the Urbandale Police Department, City of Urbandale Human Resources, or other City of Urbandale official.
2. WestCom.
3. Another Police Agency or the appropriate county or city attorney.

IX. Procedure: Department Issued cell phones

- A.** Cell phones shall be issued to select department personnel when it has been determined such access will significantly increase the quality, efficiency, and effectiveness of services to the public. The main purpose is to ensure key personnel can be reached by department personnel and/or the communication center when the need arises.
- B.** The Chief of Police shall determine which department members shall be issued a cell phone. Issuance of a department cell phone shall be recorded with the Support Services Division as part of the employee's department issued property. The Office of the Chief of Police shall be responsible for maintaining all cell phone records, contracts, etc.
- C.** It is recommended all personnel issued department cell phones carry them at all times. If an employee is issued a department issued cell phone and is "on call", it is mandatory the department issued cell phones be carried during this time frame (e.g. investigations follow up, MINE Task Force follow up, etc.)
- D.** It is recommended department issued cell phones be used for departmental purposes only; however, personal use is permitted and should be held to a minimum. Any cost incurred for personal usage shall be the responsibility of the employee. Any cost for downloads and/or add-on's to the phone other than for departmental purposes shall be at the employee's expense.
- E.** The Department is a public entity and as such is subject to disclosure of public records. This may include any and all records produced by a department issued cellular phone to include phone records, text messages, emails, etc.
- F.** As most cell phones are capable of internet and email access, the city's internet and email use policy shall apply to use of department issued cell phones.
- G.** Periodic audits of departmental issued cell phone usage may be conducted at the discretion of the Chief of Police.
- H.** An employee's city issued cell phone number shall not be given to the public except at the discretion of the employee or the Chief of Police.
- I.** Except in emergency situations, use of a department issued cell phone by someone other than a departmental employee is prohibited.

Chapter 6: Operations Support
Section 55: Victim/Witness Assistance
Subsection 1: Administration



Policy/Procedure #: 1

Title: Victim/Witness Assistance

CALEA Reference#: 55.1.1, 55.1.2, 55.2.1, 55.2.2, 55.2.3, 55.2.4, 55.2.5

I. Policy: Victim/Witness Assistance

Law enforcement is often the first to arrive on the scene of a crime and is the initial source of protection for the victim or witness. All Department employees shall treat victims and witnesses with fairness, compassion, and dignity. The treatment of the victim or witness often determines the amount of cooperation they will offer to assist in the prosecution of the case. The Urbandale Police Department is committed to offering a victim/witness assistance program aimed at protecting rights and helping victims and witnesses navigate the criminal justice system.

II. Procedure: Victim/Witness Coordinator

- A.** Victims are provided numerous protections under the law as stated in Iowa Code Chapter 915. The Department shall ensure victims and witnesses rights are being met through adherence to the following procedures.
- B.** Support Services Division Commander shall designate a specific administrative staff person as the Department's Victim/Witness Coordinator. The Victim/Witness Coordinator shall administer and coordinate the Department's victim/witness assistance activities as well as maintain a liaison with other criminal justice agencies and organizations concerned with victim/witness needs and rights.
- C.** The purpose for maintaining a liaison with outside sources of victim/witness assistance is twofold:
 - 1.** To ensure the Department's referrals of victims/witnesses to outside sources are based on accurate and up-to-date knowledge of the services offered by those sources.
 - 2.** To maintain an ongoing channel of communication to best determine how the Department and outside sources can more effectively work together in order to better serve victims/witnesses.
- D.** The victim/witness coordinator shall complete a review of victim/witness assistance needs and available services within Polk and Dallas Counties at

least once every two years or obtains access to a current review. The review may include the following elements:

1. The extent and major types of victimization within the primary service area.
 2. An inventory of the information and service needs of victims/witnesses in general (including homicide or suicide survivors) and special victims, such as those victimized by domestic violence, abuse and neglect (especially children and the elderly), sexual crimes and drunken drivers.
 3. Victim assistance and related community services available within the service area.
 4. Identification of unfulfilled needs and if any of those needs are appropriate for the Department to provide.
- E. On the basis of the above review of the victim/witness assistance services available and available resources, the Department shall develop policies and procedures that meet the needs of victims and witnesses.
- F. The victim/witness coordinator for the Department shall provide the following services:
1. If a crime is classified as a serious misdemeanor or above and has a victim or a witness, ensure the appropriate referrals have been made by the reporting/responding and/or investigating officers. If the victim or witness has not received the proper referrals, it shall be the responsibility of the victim/witness coordinator to contact the victim or witness and make the referrals.
 2. Act as the liaison between the victim/witness and the Department by providing answers to questions and referrals to the proper personnel for follow up information on their case.
 3. Act as the liaison between the victim/witness and other criminal justice agencies and social service agencies by providing needed information, referrals and contact information.
 4. When needed, assisting the victim in documenting losses.
 5. Liaison with the Support Services Division to provide the victim (or their representative) with police reports concerning incident reports or traffic crashes as permitted by law.
 6. Ensure Westcom emergency communications center has an updated contact list for all referral agencies in our service area.

III. Procedure: Officers Initial Response to Victims/Witnesses

- A. All members of the Department shall cooperate with prosecuting attorneys, other law enforcement agencies, local service agencies and the courts to afford victims/witnesses the rights and services provided by law. Direct support to victims and witnesses should include the following:
1. When practical, advise the victims and witnesses if an arrest has been made and how the case will proceed. If unable to make this notification,

the victim/witness coordinator shall be informed and he/she shall make the notification at the earliest convenience.

2. If applicable, provide the victim/witness with a case number and subsequent steps that will be taken in the case.
 3. In cases of sexual abuse or domestic violence, the investigating officer will advise the person of the appropriate referral agencies. The officer shall ensure notification is made to the proper agency.
 4. Provide the victims and witnesses with a printed material containing the contact information for the appropriate agency/organization.
 5. Ensure the "Notification of Victim Rights" form is provided for all victims of domestic abuse and answer any questions the person may have.
 6. Ensure the "Notification of Rights for Victims of Sexual Abuse" form is provided to all victims of sexual abuse and answer any questions the person may have.
 7. When needed, liaison with referral agencies in providing immediate care and assistance to the victim/witness.
 8. Advise the victim or witness to contact the Department if they are threatened or intimidated by the suspect or anyone associated with the suspect. If this is an imminent danger, the victim or witness shall be directed to call 911. All other reports of threats shall be directed to the detective handling the case if known or the victim/witness coordinator for the Department.
 9. Providing information on how to register as a victim with the appropriate county attorney's office.
 10. Providing information on how to obtain emergency crisis intervention services.
 11. Providing reasonable protection from immediate harm or threats of harm arising from cooperation with law enforcement.
 12. Upon request, provide a victim of a crime with contact information so they may obtain information relating to the release of the suspect/defendant.
 13. Provide the victim with contact information for the officer. Contact information should also be provided for the Investigation Division and the victim/witness coordinator to ensure they can contact the proper personnel in the department reference their case.
 14. Document the services or referrals provided to a victim or witness to include if a victim is requesting to register with the appropriate county attorney's office.
- B. When officers are the victim of a crime and receive a "Victim Verification" form, they shall complete the form as soon as practical. The form shall be forwarded to the victim/witness coordinator for mailing.

IV. Procedure: Follow-up Response to Victims/Witnesses

- A. If the impact of a crime has been unusually severe, the investigator assigned to the case shall contact the victims and witnesses within ten (10) days of the initial report to ensure victim/witness assistance is occurring. If an investigator is not assigned to the case, the victim/witness coordinator shall make contact with the victim/witness.
 - B. When making initial contact with a victim/witness in a case, an investigator shall explain the procedures involved in the prosecution of the case and what role the victim/witness will play in those procedures. If an investigator is not assigned, the victim/witness coordinator may make the notification based on the severity of the crime and the impact on the victim/witness.
 - C. To lessen the burden on victims/witnesses, any need for victims/witnesses to participate in viewing lineups, interviewing or other required appearances should be scheduled at the victims/witnesses convenience. Transportation needs should be met when feasible to help alleviate the burden on victims/witnesses.
 - D. When permitted by law and when doing so will not have an adverse effect on the investigation or prosecution of a case, assigned investigators shall assist victims/witnesses with the return of their property taken as evidence. This does not include contraband, weapons used in the course of a crime or disputed property. The victim/witness coordinator may assist as a liaison between the victim/witness and the property/evidence custodian.
 - E. Iowa Code 915.20 establishes a victim's right to request and have a victim counselor or advocate present at any legal or evidentiary medical proceeding related to the offense. If requested, the victim/witness coordinator shall ensure the victim/witness has access to an advocate as provided by Iowa Code 915.20.
 - F. The investigator assigned to a case shall ensure copies of the incident report and any supplemental reports are forwarded to the appropriate prosecuting attorney's office, if required.
- V. Procedure: Availability of Information**
- A. Efforts shall be taken to inform the public and media about the Department's victim/witness assistance services. Such information may be disseminated by one or more of the following: media releases, brochures, pamphlets, newsletters, prominent posting, personal contact, web sites, the community resource officer, and annual reports. The victim/witness coordinator shall facilitate the creation of the information to be distributed.
 - B. The Department shall maintain victim and witness assistance and referral information on a 24-hour basis through its dispatching service and through personal response by police officers.
 - 1. The police dispatcher shall make a determination, based upon the scope of the emergency phone call, if the victim or witness needs direct

emergency medical service (E.M.S.) and/or physical police response or referral. If either the E.M.S. or police are needed, the dispatcher will promptly dispatch appropriate personnel. In cases of a referral, referral lists are maintained in the dispatch center and agency contact phone numbers shall be kept updated.

2. If physical police response is necessary, the responding officer shall determine whether overt police actions such as written reports, notifications, arrests or transportation are required or if the need exists for other types of assistance or intervention (e.g. contact with Polk County Victim Services, Rape Crisis Center, Polk County Family Violence Center, Domestic Abuse Services or the Mobile Crisis Unit).

VI. Procedure: Training

- A. When hired, all personnel shall be trained in the existing Department and community Victim/Witness assistance programs.
- B. When possible, the victim/witness coordinator shall receive additional training and attend seminars and conferences hosted by area referral agencies as a means to network and become familiar with services available.
- C. The victim/witness coordinator shall be responsible for training Department personnel on the services available. The victim/witness coordinator shall liaison with the training coordinator in the Support Services Division to provide continuing education in the victim/witness assistance field.

VII. Procedure: Victim and Witness Protection

- A. If the Department becomes aware of danger to a victim/witness, the Department shall promptly attempt to contact and alert the victim/witness.
- B. The Department shall provide appropriate assistance to victims/witnesses who have been threatened or who, in the judgment of an officer, express credible reasons for fearing intimidation or further victimization. The following shall be used to determine the level of response from the Department when a victim or a witness has been threatened:
 1. Based upon the nature of the threat and the ability to commit the act, an officer shall offer appropriate assistance and protection commensurate with the danger faced by the victim/witness.
 2. Appropriate assistance and protection shall range from counseling the victim on temporarily moving to a location that is unknown to the suspect, assisting the victim in finding a protective environment such as a shelter, or providing extra patrol checks. Area service agencies, county, state, or federal attorney's offices may be contacted for assistance when protection of a victim or witness is needed.

VIII. Procedure: Registered Victims

- A. Victims of crimes who suffer any type of loss or physical injury as a result of a crime, other than a simple misdemeanor, must be notified of their right

to register with the appropriate county attorney's office. Victims who choose to register will be kept updated as to the status of the suspect/defendant through the criminal justice system. The following procedure shall be followed:

1. The officer who has contact with the victim of a reported crime that is classified as a serious misdemeanor or above, will advise the victim he/she has a right to register with the county attorney. The officer shall give the victim a victim's rights notification form and a "Crime Victim Rights in Iowa" pamphlet provided by the Iowa Attorney General's Office.
 2. If the victim wishes to register, the officer shall have the victim complete the victim request for registration form. The victim request for registration form can be collected by the officer while taking the report, submitted by the victim directly to the appropriate county attorney's office, or it may be submitted later by the victim to the victim/witness coordinator. Any victim request for registration forms collected by the officers shall be forwarded to the victim/witness coordinator for referral to the appropriate county attorney's office.
 3. The victim may also register by contacting the appropriate county attorney's office from the information provided in the victim's rights notification form. Victims are not required to use the victim request for registration form in order to register as a victim.
- B.** The Department shall maintain the confidentiality of related records and files to the extent consistent with state and other applicable laws.

Chapter 6: Operations Support
Section 55: Victim/Witness Assistance
Subsection 2: Operations



Policy/Procedure #:6
Title: Emergency Notifications
CALEA Reference#: 55.2.6

I. Policy: Emergency Notifications

A policy is established to provide officers with guidelines for notifying family members regarding emergencies to include death or serious life threatening injury/illness. Emergency notifications including death or serious injury/illness of a family member is a difficult task even for experienced officers. Without guidance, inappropriate methods, comments, or remarks may unnecessarily exacerbate the mental distress of the persons notified. As a result, the Department shall require all officers become familiar with concepts and procedures set forth in this policy to provide the persons notified with sufficient useful information and support in a manner consistent with professionally accepted crisis intervention techniques.

II. Procedure: Preparation for Notification

- A.** It is imperative accurate useful information be gathered for the person notified. Officers shall use the death or serious injury-illness notification form to capture needed information. This form will contain all needed contact information for the Department and any other agency involved in the incident.
- B.** All information shall be verified by the officer assigned to complete the notification. When practical, a supervisor shall review the information prior to delivery. Verification of information, including completion of the death or serious injury-illness notification form, by talking directly to the party requesting the notification is essential. Teletype information should not be relied upon as the sole source of information unless absolutely necessary.
- C.** Unless an exception is granted by a supervisor, an emergency notification team shall be assembled to deliver a message of death or serious injury/illness. The following procedures shall be used:

1. Determine who will constitute the notification team and where they will meet. The station is the preferred place to gather and prepare for the notification.
2. When the notification involves a death, one of the Urbandale police chaplains shall be part of the notification team. If the notification involves a serious injury, illness, or other emergency a supervisor shall determine if a chaplain is needed.
3. Prior to notification, the notification team will review the information so they all know the circumstance and the parties involved. The accuracy and completeness of the information will be verified at this time. The notification team shall familiarize themselves with essential details concerning the deceased, to include, full name, age, race, address as well as details of the death/incident, location of the victim, personal effects, and other pertinent information.
4. Determine who share the information with the family. Often the chaplain will have more experience in delivering this type of message and may be relied upon to make the initial notification. The chaplain shall then refer the family member(s) to the officer for the facts of the incident.
5. When dealing with an emergency notification, the notification team shall identify the family of the victim for purposes of notification. Particular efforts shall be made to locate the closest family member starting with a spouse and followed by adult children, parents, brothers, sisters and then minor children. Family dynamics such as estrangement and divorce may be considered when locating the closest family member.
 - a. Only where substantial delays would be required to make contact with family listed above should the order of notification be altered.
 - b. Officers shall contact a supervisor for guidance when in doubt concerning whom to notify or delays in notification.
6. Time is of the essence when making a notification. Delays in the notification process shall not be made unless information is not sufficient to make a proper notification or an emergency situation exists. Any unusual delay in notification shall be approved by a supervisor.

III. Procedure: Notification

- A. All emergency notifications that are the responsibility of the Department shall be delivered in person unless the exigency demands telephonic notification.
- B. Whenever possible, officers shall avoid using the name of the victim over the radio prior to notification.
- C. Officers shall be provided adequate time to spend with the person notified to provide the assistance authorized by this policy. The notification team

should regroup at the station following a notification in order to debrief and decompress.

D. Officers and chaplains shall follow the following procedure when making a death notification:

1. Go to the residence or place of employment of the person to be notified. Check the accuracy of the location to ensure you are at the correct address.
2. Identify yourselves and ask to be admitted to the residence. If this is a place of employment, ask for a room where you can have privacy. Request to speak to the person to whom notification is to be made. If the slightest doubt exists, ensure you have the correct person by verifying the relationship of the survivor to the deceased. Every reasonable effort shall be made to make the death notification in the privacy of the survivor's home or in another location away from public scrutiny.
3. Prior to making notification, the officer or the chaplain shall, when possible, bring members of the family together who may be in the house or otherwise on hand. If possible, have family members seated for the notification to avoid any injuries. In calm, direct, adequate but not lurid detail, explain what has happened (e.g. "There was an accident at _____, and _____ was involved. His injuries were so severe he was killed). If we say, "He did not survive", they may not grasp what we are trying to say in the emotion of the moment. Team members shall not to use police terms or jargon when making the notification. Team members shall refer to the deceased using his/her first name or terms reflecting the deceased's relationship to the survivor (i.e. son, daughter, etc.).
4. Wait for the information to sink in and then be ready to answer as many questions as possible. Most will inquire for more details on exactly what happened, where it occurred, if they can go to the scene, where their family member is now, where the car has been taken, etc.
5. In many incidents it will be necessary to say we are not sure exactly how the incident occurred. A full investigation is ongoing and we will let them know as soon as possible.
6. Tell them "John is at the Medical Examiner's office in Ankeny," not "The body is at the Medical Examiner's office." Let them know the medical examiner will do a full examination to determine the cause of death and they may obtain a copy of the report, if they wish.
7. The chaplain should then ask if they have a clergy person he/she may contact (a list of all Urbandale clergy is included with the death/serious injury/illness notification information form), if there are family and friends we can call for them, or if there are neighbors they would like

us to contact. Our goal is to serve the family and give them support in this very difficult time.

- 8.** After adequate time has passed, the chaplain may inquire about what funeral home they may prefer. This is a delicate topic, but we need to know their wishes once the medical examiner has finished their job (the death/serious injury/illness notification information form includes the names and phone numbers of area funeral homes). If the family asks for recommendations, the chaplain may assist.
 - 9.** Stay with the family until you are confident they are emotionally stable and they have some type of support system with them. Under normal circumstances, no family member should be left alone. Family, friends, co-workers, neighbors, clergy, crisis counselors or other community social service agencies should relieve the notification team (If a family member leaves the room, keep track of them. In this emotional time, we do not want anyone to harm themselves in their immediate grief.). In gauging the need for assistance, officers shall also consider the following:
 - a.** The emotional reaction and physical condition of the survivor.
 - b.** The availability of other adults in the home.
 - c.** Responsibility for infants or small children.
 - d.** Home environment (e.g. evidence of excessive alcohol or drug use, lack of means of financial support, shortage of food, problems with shelter, etc.).
 - e.** Availability of a support system (e.g. including friends, family, close friends, access to clergy, means of transportation, etc).
 - 10.** Personal effects of the deceased shall not be delivered to survivors at the time of death notification.
 - 11.** Any of the notification team may attend the visitation and/or the funeral to give continued support to the family on behalf of the Department.
 - 12.** A similar procedure shall be used for other types of emergency notifications.
- E.** When there is concern for the well-being of the person notified, officers or the assisting chaplain should have follow-up contact with the person or other family members. This follow up contact shall be documented in the case file.
- F.** Transportation related to the notification may be provided by the Department based on the availability of family or friends and if the officer feels the person is in no condition to drive.
- G.** Notification team members shall be prepared for unexpected responses from persons notified of an emergency to include hysteria and possible verbal or physical attack.
- H.** Notification team members shall remain alert to the possible need for medical assistance. When officers are aware of serious medical

conditions in advance of notification, they shall place a local medical response unit on alert.

- I. Contact information for the notification team as well as any other involved agencies shall be left with the person notified through use of the family member/person notified information portion of the death and serious injury-illness notification form.
 - J. Contact information for the victim/witness coordinator for the Department shall also be left with the person notified. When able, the victim/witness coordinator may assist the person by acting as a liaison with social service agencies.
 - K. All notifications shall be documented on a CIR for future reference.
- IV. Requesting Notification From Another Agency**
- A. When another agency must be contacted to notify a person of an emergency for the Department officers shall:
 - 1. Speak to the agency directly and preferably to the personnel from the other agency that will make the notification. This will decrease the chance for miscommunications or errors being made in the notification.
 - 2. Request the notification be made in person.
 - 3. Request immediate verification when notification has been accomplished.
 - 4. Furnish as much information as possible based on the incident being mindful of the confidentiality of certain investigations.
 - 5. Whenever possible, officers shall gather available information concerning the person to be notified that may aid in the notification. This includes, but is not limited to, whether the person is elderly, disabled, visually or hearing impaired, have medical problems or may not speak English. If possible, obtain the names of the person's closest relative, friend, family doctor and clergy.
 - B. Officers shall document the request for another agency to complete a notification on a CIR for future reference.

Chapter 7: Traffic Operations
Section 61: Traffic
Subsection 1: Traffic Enforcement



Policy/Procedure #: 1

Title: Traffic Enforcement

CALEA Reference#: 61.1.1, 61.1.2, 61.1.4, 61.1.5, 61.1.6, 61.1.8, 61.1.11, 61.1.12

I. Policy: Traffic Enforcement

Appropriate enforcement of traffic laws is important to ensure motorists and pedestrians enjoy a safe environment within the City of Urbandale. Reasonable judgment by the officer with a focus on impartiality, consideration of the circumstances, and conditions at the time of the violation will ensure appropriate action and gain the public confidence in traffic enforcement leading to voluntary compliance. This policy shall serve as a general guideline for officers and shall not infringe upon officer discretion regarding traffic enforcement.

II. Procedure: Selective Traffic Enforcement

- A.** The goal of selective traffic enforcement is to reduce traffic accidents. This may be achieved through the application of techniques such as geographic/temporal assignment of personnel and equipment and the establishment of preventive patrols to deal with specific categories of unlawful driving behavior. The techniques used shall be based on accident data, enforcement activity records, traffic volume, and traffic conditions. The objective is to direct appropriate enforcement efforts toward violations, not only in proportion to the frequency of their occurrence in accident situations but also in terms of traffic-related needs identified in the community.
- B.** Traffic accident data and traffic enforcement activities shall be compiled by the Support Services Division for presentation at staff meetings. The data shall be reviewed by all staff member with particular emphasis by patrol supervisors.
- C.** A comparison of collision data and enforcement activities shall also be presented by the Support Services Division at staff meetings. The comparison shall include but not be limited to:

1. Top accident locations. Top accident location information shall also include type of accidents and causal factors, if known.
 2. Overall enforcement activity at top locations.
 3. Selective traffic enforcement activities at top locations (radar or special assignment setups).
- D.** After a comparison of the data, supervisory personnel shall evaluate the data and determine if an action plan shall be implemented to address the situation. Any action plan implemented shall be documented in the staff meeting minutes. The action plan may include but not be limited to the following:
1. Increased radar or special assignment setups utilizing selective enforcement techniques and procedures.
 2. Contact with public works and/or engineering to increase signage, adjust traffic lights, etc.
 3. Use of radar speed signs.
 4. Observation of the area to determine causal factors (e.g. traffic light issues, construction, etc.).
- E.** Patrol supervisory personnel shall be responsible for the implementation of selective enforcement techniques and procedures as required by action plans or for general traffic enforcement. These techniques and procedures shall include but not be limited to the following:
1. Conducting visible traffic patrols to include:
 - a. Line: Moving patrol observation on a specified route between two points, usually on city streets or a section of the highway.
 - b. Area: Moving patrol or stationary observation in an area or beat that includes a number of streets, roads, or sections of highway.
 - c. Directed: Enforcement of a specific violation identified as a primary cause of accidents or source of complaint in a specific area.
 2. Conducting stationary traffic observation at a specific location that has frequent accidents or traffic flow problems to detect violations and deter possible violators to include:
 - a. Covert traffic observation: Stationary observation in which the observer is not visible to persons using ordinary powers of observation from the roadway or observation in which the officer is in full view but so located as to require effort on the part of motorists to discover the officer.
 - b. Overt traffic observation: Stationary observation in which the officer tries to attract attention by keeping in full view of motorists.
 3. The use of unmarked (no police markings), semi-marked (no top light bar), or other specialty vehicles.
 4. Traffic safety check points may be used in accordance with Iowa Code 321K.1.
- F.** Deployment of traffic enforcement personnel or equipment to address specific action plans or complaint areas shall be the responsibility of the patrol supervisors. Any personnel assigned to address a specific action

plan or complaint area shall document their assignment by utilizing the radar or special assignment designation in the computer aided dispatch (CAD) and/or by utilizing the traffic enforcement log form. When deploying traffic enforcement personnel, the supervisor shall consider the following:

1. Manpower
 2. Trip load
 3. Weather conditions
 4. Any other factors that affect the ability to perform self-initiated activity.
- G. The Patrol Division Commander shall complete an annual review of selective traffic enforcement activities and submit to the Chief of Police for review.

III. Procedure: Enforcement Action and Special Processing Requirements

- A. When a person is stopped for a traffic violation one of the following action shall be taken:
1. The person may be issued written or verbal warning. Verbal warnings for violations shall only be given after receiving permission from the on-duty supervisor. The supervisor granting permission shall draft a memorandum to the Patrol Division Commander stating the reason for issuing a verbal warning in lieu of a written warning or citation. The memorandum must include the race/ethnic origin of the driver issued the verbal warning. The race/ethnic origin of the driver must also be recorded in the computer aided dispatch record.
 2. The person may be issued a traffic citation. Traffic citations shall be utilized when an officer is charging a person with a traffic violation constituting a simple misdemeanor. Unless the person is taken into physical custody, a temporary detention for the purpose of issuing a traffic citation shall not be considered an arrest.
 - a. A court date for simple misdemeanor traffic citations shall be set for approximately thirty (30) days from the issuance of the citation at the time of day established by the court with jurisdiction.
 - b. The person is required to sign the traffic citation in the appropriate location. If the person refuses to sign the citation, they may be arrested (see below).
 - c. Completed traffic citations shall be submitted at the end of the officer's shift to their supervisor for review and submission into department records.
 - d. Citations are required to have a verifying signature from another sworn officer prior to submission to records.
 3. The person may be arrested and required to post bond. Arrest shall occur in the following circumstances:
 - a. The person refuses to sign the citation indicating they will not pay the fine or appear on the designated court date.
 - b. The person is willing to sign the citations but has made it clear to the officer they do not intend on paying the fine or appear on the court date indicated on the citation.

- c. The violation is a serious misdemeanor or above requiring the person to be fingerprinted and photographed.
 - d. The officer has legitimate articulable reason to believe the person will not appear in court. This shall not be based on residency alone.
- B. Violators residing outside the State of Iowa shall be handled in the same manner as those residing within the state; however, if the violation is severe enough to require arrest, the violator shall be required to post bond or held for initial court appearance.
- C. Traffic violations by juveniles shall be handled in the same manner as adults. If the violation is a serious misdemeanor or above, the juvenile shall be fingerprinted and photographed. See Chapter 5 Section 44.1.1 (Juveniles) of the Operation Manual to determine when a juvenile may be handcuffed and to determine what juvenile cases shall be referred to juvenile court. After the booking process, the juvenile shall be released to a parent or appropriate guardian or transported to the juvenile intake facility based on the charges and circumstances of the case. It will be extremely rare that a traffic violation will result in a juvenile being held at the juvenile intake facility.
- D. Violations by legislators shall be handled as follows:
 - 1. Members of the United States Congress shall, in all cases, except treason, felony, and breach of peace, shall be immune from arrest during attendance at the session of their respective houses, and in going to and returning from same; and except for any speech or debate in either house, they shall not be questioned in any other place. Members of Congress may not be detained for the issuance of a citation while they are in transit to or from the Congress of the United States. If a member of Congress is stopped, they shall be identified and immediately released. If circumstances warrant, an officer may prepare a citation and make arrangements to have it served when the member of Congress is not in transit to or from Congress, or on other official business.
 - 2. State Legislators, under Article III, Section 11, Constitution of the State of Iowa, are immune from arrest except for treason, felony or breach of peace, and shall be privileged from arrest during the session of the General Assembly, and in going to and returning from same.
- E. Electors, under Article II, Section 2, Constitution of the State of Iowa, are immune from arrest on days of election, during their attendance at such election and going to and from, except for cases of treason, felony and breaches of peace.
- F. Violations by member of the military shall be handled as follow:
 - 1. Members of the United States Armed Forces, the Reserves or the National Guard, if on active duty orders, shall be treated as residents of the State of Iowa if they are assigned to a military installation within the state.

2. Under Chapter 29A.41 of the Iowa Code, a member of the national guard shall not be arrested, or served with a summons, order, warrant or other civil process after having been ordered to any duty, or while going to, attending, or returning from, any place to which the officer or enlisted person is required to go for military duty. This section does not prevent the officer's or enlisted person's arrest by order of a military officer or for a felony or breach of the peace committed while not in the actual performance of the officer's or enlisted person's duty. The articles of equipment personally owned by such members are exempt from seizure or sale for debt. Every member of the National Guard who has faithfully served the full term of the member's commission, warrant or enlistment is entitled, upon application, to an honorable discharge, exempting the member from military duty except in time of war or public danger.
3. Officers shall note state driver's licenses of military personnel do not expire until six (6) months after the separation from duty.
4. Per Iowa Code chapter 321.176, any person while operating a military motor vehicle in the service of the armed forces of the United States are exempt from driver's licensing requirements.
5. Per Iowa Code 321.176A, the following persons are exempt from commercial driver's license requirements when operating commercial motor vehicles for military purposes:
 - a. Active duty military personnel.
 - b. Members of the military reserves.
 - c. Members of the National Guard on active duty, including personnel on full-time National Guard duty, personnel on part-time National Guard training, and National Guard military technicians.
 - d. Active duty United States Coast Guard personnel.
- G. The United States Department of State issues identification documents to foreign government personnel who are entitled to immunity. Samples of the ID's are provided on the United States Department of State website. Because there are different degrees of immunity, officers shall read carefully identification cards presented to them. Questions regarding an individual's status or immunity shall be directed to the State Department's 24/7 diplomatic security command center at (866) 217-2089. For United Nations members, officers shall call 212-415-4444
- H. When a person is charged with a traffic violation, the officer shall provide the following information:
 1. A full explanation of the violation(s).
 2. Court appearance date and whether appearance is optional (may be mailed in) or mandatory.
 3. If the appearance date is optional, an explanation of the court date, where to appear, or how to plead guilty and pay the fine.
- I. Uniform enforcement of traffic violations will encourage compliance and reduce complaints. Although every situation is different and subject to applied officer discretion, the following guidelines are established:

1. Officers shall take appropriate action to remove impaired drivers from the road and enforce laws pertaining to operating a motor vehicle under the influence of alcohol and drugs.
2. Persons who have their privilege to drive suspended are normally cited at the scene while drivers that are revoked or barred (serious misdemeanor and above) shall be arrested and booked.
3. Officers shall take appropriate enforcement action for violations that involve moving violations. Officers shall exercise discretion when deciding if a warning or citation is appropriate. Consideration shall be given to weather conditions, traffic volume, pedestrian traffic, time of day, location and offense encountered.
4. When a vehicle is found being operated in violation of non-moving violations such as equipment or lighting not functioning properly, the operator may not be aware. A warning may be all that is necessary to bring the motorist into compliance. In instances where a motorist is aware of the non-moving violation and has failed to act in a timely manner to correct the issue or the violation is likely to result in an accident, stricter enforcement may be warranted.
5. Commercial motor vehicle drivers shall be treated the same as the general motoring public. The Iowa DOT commercial motor vehicle enforcement officers may be contacted for assistance when dealing with commercial motor vehicles.
6. When multiple violations occur, the circumstances and seriousness of the violations shall guide the officer in deciding the appropriate enforcement action.
7. When newly enacted laws or regulations are passed and become applicable to the motoring public, the enforcement guidelines prescribed in the text of each new law shall be followed. Often the law will allow an interim period in which violators are simply given notice of the new law. When the law goes into effect without an interim period, officers shall utilize their discretion in deciding to issue a citation or a warning.
8. Under normal circumstances, Department procedure shall be to issue a citation to a driver that has caused an accident due to a violation. Officers not issuing citations to violators involved in accidents may be required to articulate why they exercised discretion.
9. Officers shall use discretion and take appropriate enforcement action for violations committed by pedestrians and bicycles. Consideration shall be given to the age of the violator and seriousness of the violation.
10. When a driver is suspected of incompetency, physical or mental disability, disease, or other conditions that may prevent the person from exercising reasonable and ordinary care when operating motor vehicle, the officer shall make a referral to the Iowa Department of Transportation for driver's license reexamination. Copy of the referral sheet shall be included with the case reports. If no case report has

been generated, notation of the referral shall be added to the computer aided dispatch (CAD) entry.

IV. Procedure: Speed Measuring Devices

- A.** The Department provides vehicle mounted and hand held speed measuring devices that utilize radar or lidar technology. The radar/lidar devices shall be National Highway Traffic Safety Administration (NHTSA) and/or International Association of Chiefs of Police, (IACP) approved.
- B.** All officers authorized to operate radar/lidar units shall be trained in their proper use during the field training program.
- C.** Radar/lidar units shall be operated in accordance to the manufacturer's operation manual and the officer's training. Officers are required to perform the following actions when utilizing a radar/lidar:
 - 1.** Internal and external tests shall be performed at the beginning and the end of each officer's shift in which the unit will be utilized. Testing shall follow the manufacture recommendations.
 - 2.** When a citation is issued for speeding based on the use of a radar/lidar unit, documentation of the radar/lidar unit number and testing shall be included in the notes section for each citation.
- D.** Maintenance records for each radar/lidar unit shall be maintained by the Support Services Division. The records shall document all maintenance and calibration certifications for the unit.
- E.** Officers shall treat the radar/lidar units with care as they are a precision device. Hand held units shall be stored in their protective case with the proper tuning forks and other equipment specific to the unit. If a radar/lidar unit is not functioning properly, a repair notice shall be forwarded to the support services division and the unit shall be immediately removed from service until it can be repaired.
- F.** Officers shall be allowed to pace motorists suspected of speeding when unable to capture their speed in any other way. Pacing shall only be allowed when utilizing a radar unit to confirm the pace speed. Officer shall be trained how to pace during the field training program.

V. Parking Enforcement

- A.** The Patrol Division shall enforce parking ordinances and laws to maintain the safe and efficient movement of traffic. Patrol officers shall be responsible for the enforcement of parking regulations on city streets, alleys, and lots as regulated by city code and state law.
- B.** Unless directed by a supervisor, officers shall use discretion in deciding the manner in which to enforce parking violations. The options shall include:
 - 1.** Verbal warning.
 - 2.** Written warning.
 - 3.** Citation.
 - 4.** Impoundment. Officer shall obtain supervisor approval to impound a vehicle for a parking violation. Factors to consider when requesting an impoundment shall include:

- a. Officers are unable to locate or identify the owner of the vehicle (e.g. no registration plates or out of area owner).
 - b. The vehicle/owner is a repeat offender for the parking violation.
 - c. The vehicle is a safety/traffic hazard.
 - d. In case of snow ordinance violations, the vehicle has not been moved for 48 hours since the latest snow event has ended.
 - e. The Department has received a citizen complaint on the violation.
- C. In response to complaints of vehicles being parked over the allowed amount of time, as stated in the city ordinance, an officer shall respond and mark the tire(s) on the vehicle. Once marked, the officer shall notify communications to log the date and time along with the vehicle description. This action will facilitate a verifiable record enabling enforcement action to take place. It shall be the officer's duty to check the vehicle after the allotted time has passed to verify a violation. If the officer will not be on duty, it is their responsibility to pass the information on to the supervisor of the shift that will be working when the allotted time has passed. The supervisor shall be responsible for assigning an officer to follow up on the parking complaint.

VI. Speed Signs

- A. The Patrol Division shall utilize speed signs as a means to control traffic in certain areas of the city. The signs are designed to capture the speeds of passing vehicles and display the speed to the driver. The speed signs act as a reminder to drivers to operate at an appropriate speed.
- B. Data captured by the speed signs shall be reviewed by patrol supervisory personnel. The data will assist the Department in determining the need for additional enforcement in a particular area.
- C. The speed signs may be deployed in various areas throughout the city as determined by the Chief of Police, Patrol Commander or designee.

Chapter 7: Traffic Operations
Section 61: Traffic
Subsection 1: Traffic Enforcement



Policy/Procedure #: 7
Title: Traffic Stops
CALEA Reference#: 61.1.7

I. Policy: Traffic Stops

Although enforcing traffic laws is one of the more basic functions law enforcement performs, all too frequently officers are injured or killed in the process. Therefore, the department shall develop procedures to ensure officers respond to traffic stops in a safe, effective, and uniform manner.

II. Procedure: Traffic Stops

- A.** Officers shall receive initial and ongoing training in conducting traffic stops. Training shall emphasize the rights of all persons to be treated equally and to be free from unreasonable searches and seizures. In developing training programs, the department shall stress the following aspects of traffic stops:
 - 1. Officer safety.
 - 2. Courtesy and interpersonal communication skills.
 - 3. Documentation.
 - 4. Cultural awareness/language barriers.
 - 5. Search and seizure laws and other related constitutional issues.
- B.** Traffic enforcement activities shall receive consistent, ongoing supervisory attention to ensure officers are placing sufficient emphasis on the need for proactive traffic enforcement and conducting traffic stops in a courteous and constitutional manner. Supervisors shall be particularly alert to any indication of discriminatory treatment of any segment of society by officers.
- C.** There is no such thing as a routine stop. All stops have the potential to escalate into a high risk situation. Too many officers have been injured or killed from an unanticipated assault to regard any stop as routine. Officer safety must be the paramount consideration in all stops but must not override the use of courtesy and helpfulness when appropriate. The risks involved in stops include not only hazards from the person(s) being

stopped but also from other persons at or near the location of the stop and the risk of being struck by other vehicles.

- D.** After a violation has been identified, the actual stop should be attempted in a location that will afford the officer the greatest safety available with consideration being given to the availability of lane usage, shoulders, traffic flow, lighting, etc. If the violator stops in an unsafe area, the officer should use the public address system to instruct the violator to move to a safer location. The traffic stop shall occur as soon as possible after the commission of the violation.
- E.** Communications shall be advised of all traffic stops by giving the location and the license plate number. If no license plate number is available, a description of the vehicle shall be provided. The officer may also choose to give additional information, depending upon the circumstances such as a more detailed description of the vehicle and the operator, the number of occupants, furtive movements, etc.
- F.** When necessary, the officer shall utilize appropriate auditory and visual equipment on the police vehicle to announce the intention to stop the violator. Once the violator has stopped in a safe location, the officer's patrol vehicle shall be positioned offset from the violator's vehicle to allow protection from traffic. The officer's patrol vehicle shall be far enough back from the violator's vehicle to allow the officer to react and protect themselves should the situation change. When a motorist refuses to stop for an officer, the procedures detailed in Chapter 5 Section 41.2.2 (Vehicle Pursuits) of the Operations Manual shall be followed.
- G.** The officer shall approach the violator's vehicle with caution, watching for suspicious or sudden movement in the vehicle. Officer may approach the violator's vehicle from either side based on factors such as stop location, amount of traffic in the area, violator's action, etc. If two (2) officers are approaching a violator's vehicle, one (1) shall be on either side of the violator's vehicle.
- H.** On the approach to the violator's vehicle, the officer shall look at the interior of the vehicle through the rear window. The officer shall examine the trunk lid to ensure it is latched then look into the back seat for firearms, hidden passengers, or other threats. The officer shall stay close to the violator's vehicle. This may give the officer a tactical advantage if there is an assault attempt.
- I.** When making contact with the violator, the officer shall be positioned slightly behind the driver's front door, unless other tactics are warranted.
- J.** There may be occasions where the risks of the motor vehicle stop will be unknown to the officer. It is difficult to describe the factors involved in determining this level but considerations shall be given to the following:

 - 1. Reason for the stop.
 - 2. Number of occupants in the vehicle.
 - 3. Time of day.
 - 4. Any information the officer may possess that would require extra awareness on the part of the officer.

5. The following shall be considered by the officer when conducting such stops:
 - a. Wait to approach the vehicle until a second unit arrives. This is the most important tactic when the risk is unknown.
 - b. Approach from the right side of the vehicle.
 - c. Request the driver/occupants exit the vehicle.
 - d. Conduct a high risk stop as described in this policy.

III. Procedure: High Risk Stops

- A. When a vehicle contains a threat to officer safety, the stopping officer shall not make the stop without having backup unless exigency exists. The supervising officer shall be notified immediately by the officer or communications when there is a high risk stop situation.
- B. The officer shall advise communications of the exact location and direction of travel of the violator's vehicle, what the situation is, where the officer wants the backup police unit deployed and how many other units are needed. It is recommended the stopping officer be no closer than 50' while trailing the vehicle to allow proper reaction time.
- C. The stop location shall be an area with adequate lighting, nearby cover, and a minimum amount of pedestrian and vehicular traffic. If the violator stops where the officer does not want the car to be stopped, the officer shall use the public address system to direct the violator to move the vehicle to a proper location for the stop. Failure to comply with directions shall heighten the risk of the stop.
- D. Based on the threat, the officer shall position their vehicle at a distance that allows adequate reaction time and protection. Based on the distance from the violator, the officer shall consider the use of the patrol shotgun or rifle. When the first vehicle is positioned as stated above, the second officer shall park their vehicle to the left of the first unit and parallel or slightly angling the front of the vehicle to the front of the first officer's vehicle. Enough distance shall be left between the two vehicles to allow the doors to open and be used as cover. Based on the location of the first vehicle the subsequent responding officers may have to improvise with the location of their vehicle to ensure a safe response.
- E. When the primary police unit is a two-person unit, it is the passenger officer who shall utilize control of the shotgun or rifle as appropriate.
- F. Unless the situation dictates otherwise, the driver of the primary police unit shall give all commands to the occupants of the vehicle. During night time stops, the auxiliary lights on the police unit shall be shown into the rear window or outside mirrors of the violator's vehicle.
- G. The driver shall be ordered to shut off the vehicle and place the keys on the vehicles roof. All occupants shall be ordered to raise their hands above their heads while still seated in the vehicle to allow the officers to observe their movements. When appropriate, all occupants of the vehicle shall be ordered to exit through the driver's door or driver's side of the vehicle. When possible, the secondary or backup police unit shall

utilize the spotlight to fully illuminate the person and impair their vision towards the officers.

- H. Once out of the vehicle, the occupants shall be ordered to raise their hands over their head as high as possible and turn completely around 360 degrees. This action will provide the officers an opportunity to view the person for weapons. If heavy or baggy clothing is obstructing the officer's view, particularly of the waist band, the person may be advised to lift or move the clothing with their left hand (as the majority of persons are right handed). If a weapon is visible, instruct the violator any movement other than those instructed shall be considered aggressive. Do not have the violator remove the weapon as this will put the weapon in the violators hand or on the ground where other occupants may gain access.
- I. The officer shall order the occupant to lace their fingers behind their head, face away from the officer and walk backwards toward the police unit. When appropriate based on the circumstances, the occupant shall be directed to the open doors between the two police units. This will allow the officers to handcuff the occupant while maintaining a safe distance and the ability to use the vehicle's door as a protective barrier/cover between the officer and the occupant(s).
- J. After cuffing, the occupant shall be escorted to the rear of the police vehicles to be thoroughly search for weapons and briefly questioned about other occupants in the vehicle and the existence of any weapons. Once searched and questioned, the occupant shall be secured in the back of the police vehicle as other occupants are removed and/or the vehicle is approached and cleared.
- K. New officers shall receive instruction and conduct practical exercises on high risk stops during their field training program. Supervisors shall ensure high risk stops are practiced periodically with their personnel so all officers are aware of their responsibility.

IV. Procedure: Violator Contact

- A. Traffic enforcement is one of the many tasks performed by police officers, but for the violator it may be an emotionally traumatic experience. Traffic stops are an opportunity for the department to make a favorable or an unfavorable impression on a citizen, depending on how the officer handles the situation. Officers shall have the following objectives in mind for every traffic stop:
 - 1. Prevention of traffic accidents and hazardous conditions.
 - 2. Taking immediate action to interrupt an ongoing violation of the law.
 - 3. Having an effect on other traffic. The sight of a police car with a violator stopped reminds the public the police are enforcing traffic law.
 - 4. Detecting evidence of a more serious violation by utilizing proper observation skills and conversational tactics.
 - 5. Having a positive effect on the motorist's future driving behavior.
- B. Officers shall strive to maintain a proper balance between sufficient command presence to maintain control of the stop and a friendly attitude. The key is projecting a courteous, non-confrontational attitude,

being assertive without being overly aggressive; suspicious without telegraphing suspicion. Officers shall strive to make each contact educational and to leave the violator with the impression the officer has performed a necessary task in a professional courteous manner.

- C. Over a period of time, officers shall develop their own approach to the violators that best fit their personalities and the goals of the department. The following method, used consistently, should minimize officer/violator conflict, and enable court testimony to be given with confidence:
1. The officer shall present a professional image in dress, grooming, language, bearing, and emotional stability.
 2. The officer shall greet the violator in a courteous manner and give the reason why the person is being stopped or detained. Describe the actions of the vehicle rather than personalizing the action to the driver. This will reduce tension. Never lecture the driver on their conduct or say anything demeaning.
 3. Invite the driver to offer a reasonable excuse. "Was there some reason why you were speeding?" This approach allows the violator to provide an explanation and reduces tension. Their reason may serve as a reason to use officer discretion or may be used as evidence in a court proceeding.
 4. After explaining the reason for the stop, politely ask for identification and any other documents. When accepting the papers, have the violator reach outside the car, do not reach inside the vehicle. Take the papers with the non-gun hand.
 5. If the driver has no license, attempt to obtain another form of identification. If any suspicions of further infractions of the law develop based on observations, inquire further.
 6. Do not lecture, talk down to, or deliberately embarrass the person you have stopped.
 7. Once satisfied there are no further violations, request the violator remain in the vehicle, and return to your vehicle. When the officer returns to his vehicle to complete the paper work, they shall intermittently glance at the motorist and be alert for any sudden or suspicious movement.
 8. Take an appropriate, documented, enforcement action for every stop. Generally a citation, warning, or arrest.
 9. Avoid situations where a violator, who would otherwise be given a warning, is cited or arrested simply because the officer considered them to be disrespectful.
 10. If there is no reason to hold the violator further, return cautiously to the motorist's vehicle. Return the driver's documents, along with a copy of any written warning or citation, and any public information pamphlets provided by the department.
 11. Advise the violator of the action taken and what if anything they need to do as a result such as signing the citation, appearing in court, etc. Do not attempt to predict the actions of the court.

- 12.** Once cited or warned, and no further reasonable suspicion exists, the violator shall be free to leave. Use an appropriate closing. For example, if the violator was cooperative, thank them for their cooperation. If the violator is upset, give them time to calm down before they resume driving.
 - 13.** Ensure the driver is able to safely re-enter traffic, then clear the stop with communications. Make sure there is a record made of the enforcement action taken.
 - 14.** If a search was conducted and no illegal items or evidence were found, apologize for the inconvenience and be sure the vehicle is returned as closely as possible to the condition in which it was found.
- D.** Any person may file a complaint with the department if they feel they have been stopped or searched illegally, stopped due to profiling, or subjected to improper treatment. No person shall be discouraged, intimidated, or coerced from filing such a complaint or discriminated against because they have filed such a complaint. Complaints shall be addressed according to Chapter 3 Section 26.2.1(Complaint Procedure) of the Operations Manual.
- E.** The deliberate recording of any misleading information relating to a traffic stop or field interview is prohibited and shall be a cause of disciplinary action up to and including termination.

Chapter 7: Traffic Operations
Section 61: Traffic
Subsection 1: Traffic Enforcement



Policy/Procedure #: 9
Title: Operating While Intoxicated
CALEA Reference#: 61.1.9, 61.1.10

- I. Policy: Operating While intoxicated (OWI)**
The Urbandale Police Department is committed to reducing alcohol and drug related offenses by training and equipping the Patrol Division to apprehend and process alcohol and drug impaired drivers.
- II. Procedure: OWI Enforcement**
 - A.** Officers assigned to patrol or directed enforcement duties, shall be alert for driving behavior that may indicate a driver is operating a vehicle under the influence of alcohol or drugs. Upon the course of their duties and each time contact is made with the operator of a motor vehicle, officers shall be cognizant of the signs of operating while intoxicated either by alcohol or drugs.
 - B.** Officer shall be aware observations prompting an investigation into illegal drug possession may lead to an OWI investigation as well.
 - C.** The Department shall participate in the Governor's Traffic Safety Bureau (GTSB) enforcement projects which conducts periodic safety check points with other participating agencies. During these safety checkpoints officers shall look for signs of drivers under the influence of alcohol and drugs.
 - D.** As part of the evaluation reports produced by the Patrol Division on selective traffic enforcement activities, the Patrol Division Commander shall look for trends in OWI that may be addressed by a special enforcement project.
- III. Procedure: Investigation and processing of persons suspected of OWI**
 - A.** The first step in investigating a possible OWI violation is to observe the vehicle being operated by the person suspected of OWI.
 - 1.** Officers shall obtain sufficient evidence of unsafe or erratic driving behavior to establish reasonable suspicion to stop the vehicle. Officers shall not permit unsafe driving to continue for an unreasonable length of time so as to endanger other motorists or pedestrians.

2. Officers may have reasonable suspicion to stop a motor vehicle based on information provided by a witness. This will be a case by case evaluation by the officer. Things to consider when evaluating the witnesses information may include but is not limited to:
 - a. Did the witness leave a name and call back number?
 - b. Did the witness specify why they suspect OWI? Personal observation, erratic driving, smell of alcohol, etc.
 - c. Is the description and location of the driver and/or the vehicle accurate?
 3. Officers may come in contact with drivers that are operating while intoxicated while conducting vehicle stops for traffic violations unrelated to erratic driving or through other investigations.
- B.** Upon contact with a driver, officers shall note the demeanor, actions, and other evidence of intoxication. These observations and evidence may become critical during subsequent prosecution should the driver refuse to cooperate and submit to field sobriety tests or refuse to submit to a chemical test for intoxication. Demeanor, actions, and other evidence that may be signs of intoxication include but are not limited to:
1. Slurred speech or excessively talkative.
 2. The smell of alcoholic beverage and/or drugs on the person or in the vehicle.
 3. Bloodshot, watery eyes
 4. Inability to follow simple instructions
 5. Diminished motor skills and/or focus
 6. Alcohol and/or drugs in the vehicle
 7. Restlessness
 8. Admissions and statements
- C.** Officers shall attempt to perform field sobriety tests on all drivers suspected of OWI. The information gathered during these tests is often the strongest evidence of impaired driving ability. Field sobriety tests shall include but are not limited to:
1. Horizontal gaze nystagmus
 2. Walk and turn
 3. One leg stand
- D.** Officers shall receive training on administering the field sobriety tests listed above during their academy training with verification and additional training as needed in the field training program. When needed, periodic update and refresher training shall be provided.
- E.** When possible, field sobriety testing shall be recorded on the in-car camera system or the jail or holding facility camera system. If no camera system is available in the jail or holding facility, the body worn camera shall be utilized.
- F.** Persons suspected of OWI should be offered a preliminary breath test (PBT). The results of the PBT may assist the officer in determining if the driver is impaired by alcohol. PBT testing devices shall be calibrated monthly by the Support Service Division. Maintenance and calibration

logs shall be kept by the support services division on all PBT devices utilized by the Department.

- G. When a driver refuses to submit to field sobriety tests, is impaired to the point it is unsafe to perform the tests, or has a physical disability, the officer shall determine if probable cause exists to arrest based upon observations of the driver, witness information, and other evidence.
- H. If arrested for OWI, the vehicle being operated by the arrested party may be impounded. Officers shall follow the procedures provided in Chapter 1 Section 1.2.4 (Search and Seizure/Vehicle Impound and Inventory) of the Operations Manual.
- I. Unless circumstances dictate otherwise, the following procedures shall be administered when processing a suspect arrested for OWI:
 - 1. The suspect shall be offered a breath test on the Data Master DMT as part of the implied consent procedure. For implied consent purposes, a chemical test should be offered within two (2) hours of the PBT or arrest. The officer shall read the implied consent advisory form to the suspect using the state of Iowa issued form and complete as much of the form as possible.
 - 2. The suspect shall be fingerprinted and photographed as part of the booking process.
- J. If an officer comes in contact with a driver who is impaired by a substance other than alcohol (e.g., marijuana, methamphetamine, prescription drugs, etc.), the officer may arrest when there is probable cause indicating the driver is impaired. Officers may request a drug recognition expert (DRE) respond to the scene to assist in determining if probable cause exist for impairment. Arrests for suspected drug impairment shall require a DRE to conduct a drug influence evaluation on the driver at the detention facility utilized.
- K. In routine OWI cases, urine shall only be requested after a breath test indicates observed impairment is not due to alcohol.
- L. When required for drug impairment testing or alternate test purposes, a urine specimen may be requested. Officer(s) or matrons of the same sex shall observe the suspect provide the urine specimen.
- M. After processing a suspect for OWI, the arrestee may be held for arraignment at the Polk or Dallas County jail or released to a responsible party after obtaining a signed acceptance of responsibility form. Release to a responsible party shall only occur if the person does not constitute a danger to themselves or others.

IV. **Procedure: Obtaining a search warrant for an OWI investigation**

- A. Officers shall apply for a search warrant for a blood, breath, or urine specimen withdrawal in lieu of invoking implied consent when encountering the following situations:
 - 1. OWI investigations involving serious injury or death.
 - 2. OWI 3rd or subsequent investigations.
 - 3. OWI investigations where prior specimen refusal may indicate future specimen refusal.

4. Other situations where obtaining a specimen by warrant are preferred over invoking implied consent.
- B. Supervisory approval shall be obtained prior to applying for a search warrant in an OWI investigation. The appropriate county attorney may be consulted prior to the application for a search warrant for an OWI specimen withdrawal; however, consultation is only required when the investigation involves serious injury or death.
- C. A blood specimen may be obtained from persons whom a physician certifies is dead, unconscious, or otherwise incapable of providing consent or refusal. The appropriate county attorney's office shall be consulted to determine if a warrant is required.
- D. Blood withdrawals will only be administered by a physician, physician's assistant, registered nurse, approved medical personnel, or other personnel with appropriate training in the withdrawal of a blood specimen. All specimens obtained for chemical testing will be treated as evidence and the chain of custody maintained.
- E. When a search warrant for a specimen has been obtained, the suspect can no longer refuse to provide a blood, breath, or urine specimen for testing. Officers may compel the suspect to provide a specimen up to and including the use of reasonable force to restrain the suspect to obtain a blood specimen. Use of reasonable force shall only be used in OWI cases involving serious injury or death.
- F. If officers encounter a suspect that physically resists or indicates they will physically resist an attempt to obtain a blood specimen after a search warrant has been obtained in OWI cases that do not involve serious injury or death, the officer shall not use force to restrain the suspect to obtain the specimen. The refusal, threat of physical resistance, or actual resistance shall be noted within the officer's report. Officers shall complete an affidavit for blood draw refusal and forward to the county attorney's office with jurisdiction for intake proceedings.
- G. In cases that do not involve serious injury or death where the officer has obtained a search warrant for a specimen and requests a blood specimen, but the suspect indicates they will physically resist withdraw of blood, an officer shall have the discretion to obtain a breath or urine specimen in lieu of a blood specimen based on the circumstances encountered as long as the alternate specimen will not jeopardize the case.

Chapter 7: Traffic Operations
Section 61: Traffic
Subsection 2: Traffic Collision Investigation



Policy/Procedure #: 1
Title: Traffic Accidents
CALEA Reference#: 61.2.1, 61.2.2

I. Policy: Traffic Accidents

Control of the motoring public is one of the main functions of a responsive police agency. The department's response to traffic accidents is one of the most important services offered to the community. The Urbandale Police Department shall respond to and assist all persons involved in traffic accidents within the City of Urbandale.

II. Procedure: Reporting

- A.** Regardless if on public or private property, all accidents reported to the department shall be responded to and investigated. The following incidents shall require a department accident report:
1. Accident causing death or injury.
 2. Accident in which combined property damage will exceed one thousand five hundred dollars (\$1,500.00) total.
 3. Accidents involving a hit and run. A hit and run accident shall also require a Case Investigation Report (CIR) in addition to an accident report.
 4. All accidents causing property damage involving impairment by alcohol or drugs regardless of the amount of damage.
 5. Accident causing a hazardous materials release of some significance (e.g. payload spill, large fuel tank ruptured, etc.).
 6. Accidents involving a city owned vehicle or property regardless of the amount of damage. Per supervisory approval, officers may also be called to assist neighboring jurisdictions when they have a police or city vehicle involved in a traffic accident.
- B.** If meeting the established criteria, the accident report shall be filed with the Iowa Department of Transportation (IDOT).

- C. A supervisor may temporarily suspend the investigation of property damage accidents due to a large workload and/or the availability of personnel to respond such as during a significant winter storm.
- D. Officers shall utilize discretion in cases involving reportable property damage accidents where the drivers have removed the vehicles from the vicinity of the accident scene rendering it impossible for the officer to properly investigate. The officer may decide not to attempt an investigation but rather refer the driver(s) to the IDOT to complete a Drivers Accident Report Form. This shall not apply to situations in which the drivers moved the vehicles from the travel portion of the roadway due to safety concerns.
- E. Officers responding to accidents with a total damage estimate of less than one thousand five hundred dollars (\$1,500.00) in total damage shall assist the parties involved by coordinating an exchange of information.

III. Procedure: Fatality or Serious Injury Accidents

- A. Officers responding to the scene of an accident shall immediately make the scene safe and provide medical aid.
- B. The Urbandale Fire Department shall be immediately dispatched to care for the injured. If a determination is made that a victim has died at the scene, the Polk County Medical examiner's office shall be notified to respond for an investigation and secure the body of the victim.
- C. After the victims of the accident are receiving needed care, the officer shall secure the scene for processing by an accident investigator and a crime scene investigator (If needed). The Department accident investigator and/or crime scene investigator shall be contacted pursuant to Chapter 9 Section 83.1.1(Collection and Preservation of Evidence) of the Operations Manual.
- D. Department accident investigators shall investigate all fatality and serious injury (with the potential to result in death) accidents that are the responsibility of the Urbandale Police Department. If no accident investigator is currently working, the on-call accident investigator shall be required to respond.
- E. If a serious injury accident that is not likely to result in death occurs when there is no accident investigator currently working, it shall be the on-scene supervisor's discretion if an on-call accident investigator shall be called to the scene to investigate. When a serious injury accident that is not likely to result in death occurs and an accident investigator is working a regular shift, they shall be required to respond and employ their advanced tools and training to investigate the accident. This will ensure investigative skills and equipment are maintained/developed. Supervisors shall allow the investigator additional duty time to thoroughly investigate and follow up on the accident.

- F. When an accident involves a death or serious injury that is likely to result in death the supervisor in charge shall notify the patrol division commander as soon as practical. The patrol division commander shall be responsible for notifying the chief of police as established in Chapter 2 Section 11.3.3 (Notification of the Chief of Police) of the Operations Manual.
- G. When needed, the officers may request the assistance of the Investigation Division to assist with any needed follow up investigation (e.g. interviewing witnesses, obtaining search warrants etc.).
- H. The county attorney with jurisdiction over the accident shall be notified as soon as is practical if it appears that circumstances surrounding the accident may lead to criminal charges. The county attorney may also be utilized to obtain needed documents and personnel for the drawing of blood at the medical facility.
- I. In fatality and serious injury (with the potential to result in death) accidents where the use of drugs is suspected, a drug recognition expert may be contacted to assist in the investigation. The drug recognition expert will focus their attention and effort on the driver suspected of driving while impaired unless instructed otherwise by the supervisor in charge.
- J. If media demands or activity starts to interfere with on-scene duties, the public information officer may be called to the scene to coordinate media efforts and inquiries as stated in Chapter 6 Section 54.1.1(Public Information) of the Operations Manual.

IV. Procedure: Response to Other Types of Accidents

A. Hit and Run:

1. Officers shall respond to and investigate all hit and run accidents to include finding and the contacting the driver of the vehicle that left the scene, taking enforcement action when appropriate, and contacting the victim of the hit and run with the appropriate investigative information. Any contact with the victim shall be documented. When time allows, officers shall follow up on any leads available.
2. The crash investigation unit (crash unit) shall be responsible for review and follow up investigation on any hit and run accidents that have not been successfully cleared. Only after all investigative leads have been exhausted shall the case be suspended. The victim of the hit and run will be contacted and informed of the disposition. Contact with the victim shall be documented in the case file.
 - a. The patrol supervisor assigned to the crash unit shall be responsible for assigning all unsolved hit and run cases for follow-up investigation to a crash unit investigator. The crash unit investigator assigned to the case will be considered the principal investigator.

- b. The criteria to be used to determine whether a hit and run case shall continue to receive further investigative attention shall be established by the patrol division commander or designee with input from the assigned crash unit investigator. Cases may require different criteria to determine the need or extent of continued investigative efforts. The patrol division supervisor assigned to the crash unit or designee will review all cases assigned for follow up investigation to determine appropriate current case status.
 - c. In addition to the criteria identified above, the following solvability factors shall also be considered when assigning cases for follow-up investigations:
 - Victim and/or witness availability and reliability.
 - Suspect and/or vehicle description or identity.
 - Physical evidence/property identifiable or traceable.
 - Available informant/intelligence information.
 - Information linking an incident to another incident or to an ongoing investigation.
 - The quality of the preliminary investigation.
 - Outside law enforcement agency requests.
 - Belief that a crime may be solved with publicity and/or reasonable additional investigative effort.
 - Minor incidents which may attract more than usual publicity or public concern.
 - Command staff requests for follow-up of incidents of special concern.
3. The patrol division commander has the responsibility of determining the amount of manpower and physical resources that will be committed to hit and run follow-up investigations.
4. The patrol supervisor assigned to the crash unit shall review all follow-up reports as the case progresses to determine what point the investigation should be suspended due to investigative leads being exhausted.
5. The patrol division supervisor assigned to the crash unit shall log all case assignments in a case management system within the computerized records management system. The case management system shall be accessible to crash unit personnel, support services personnel and command staff as needed. The case management system shall contain the following information:
 - a. Case number
 - b. Type of criminal activity
 - c. Date case was assigned
 - d. Case status
 - e. Date of case status

f. Investigator assigned

6. Written supplemental reports generated through follow-up investigations shall be submitted to the patrol division supervisor assigned to the crash unit by the case investigator no more than sixty (60) days after assignment. After a review of the investigation, the supervisor may approve a change in case status or continuance of the investigation. No case status shall be changed without the approval of a supervisor. Continuances of investigations may be granted by the patrol division supervisor for a maximum of thirty (30) days at which time another review shall occur to determine if additional investigation is warranted.
- B. Pedestrian/bicycle vs motor vehicle accidents:
 1. Pedestrian/bicycle vs motor vehicle accidents involving fatalities and serious injuries shall be handled the same as noted in the fatality and serious injury section above.
 2. Pedestrian/bicycle accidents involving minor or no injury shall be investigated by an accident investigator. If no accident investigator is working, an officer shall take the initial report and do any follow up needed. An accident investigator will review all pedestrian/bicycle accident reports and complete any needed follow up investigation the initial officer was unable to complete. All involved parties will be contacted regarding final disposition of the case. This contact shall be documented in the case file.
- C. Operating While Intoxicated (OWI): When the driver of a vehicle involved in an accident is suspected of being intoxicated, the supervisor shall assign one officer to investigate the accident while another officer investigates the OWI. The OWI shall be investigated as established in Chapter 7 Section 61.1.9 (Operating While Intoxicated) of the Operations Manual.
- D. Damage to Public Vehicles or Property: When a vehicle or property owned by the City of Urbandale is involved in an accident, even if there appears to be no damage, officers shall complete an accident report. If a Police Department vehicle is involved, the accident investigation shall be conducted by a supervisor. If a police vehicle is involved in an accident in which there are injuries or death, an outside agency, generally the Iowa State Patrol, shall be contacted to conduct the investigation. The supervisor shall ensure proper investigative techniques are utilized by the outside agency based on the severity of the accident.
- E. Fire hazard or Hazardous Materials: Accidents involving a fire hazard, hazardous materials or chemical spills may necessitate the following:
 1. Response by the Urbandale Fire Department to evaluate and contain the situation. Based on the size and type of incident, the Fire Department may activate other entities to assist.

2. Response by Urbandale Public Works or IDOT road maintenance to assist with equipment and manpower to contain a spill.
 3. Notification to the Iowa Department of Natural Resources as established in Chapter 5 Section 41.2.4 (First Responder Notifications) of the Operations Manual.
 4. Contacting IDOT enforcement officers to assist in the investigation.
 5. Based on the scope of the fire hazard, hazardous materials or chemical spill, activation of the Incident Command System as established in Chapter 5 Section 46.1.1(Critical Incidents) may be warranted.
- F. Disturbances between Parties:** Accidents can result in heated arguments, intimidation, or even assaultive situations between the parties involved. Officers shall be cognizant of these situations and respond to accidents as quickly as possible. Officers shall separate parties engaged in an argument and become the liaison for the incident. This is where facilitating information exchange on minor accidents is beneficial.
- G. Major Traffic Congestion Due to an Accident:** Traffic congestion should be a factor when investigating all accidents. Traffic congestion, especially in unexpected areas, greatly increases the chance of more accidents occurring. The following shall be applied to reduce the amount of traffic congestion when addressing an accident:
1. When investigating minor accidents, the responding officer shall assess the scene quickly and if needed mark the location of the vehicles involved. Once the officer has all the information they need for the investigation, the vehicles involved shall be removed from the roadway while the officer completes needed reports.
 2. When a vehicle is disabled due to damage from an accident, the officer shall immediately determine who the owner/operator of the vehicle would prefer tow the vehicle and have communications contact the company and start their response. This will be a private arrangement between the tow company and the owner/operator. If the owner/operator is unsure who to call and asks for assistance, the officer may recommend the tow service utilized by the Department for impounds. If the owner/operator of the vehicle is unable to request a tow company, the officer shall impound the vehicle as established in Chapter 1 Section 1.2.4 (Search and Seizure/Impound Inventory) of the Operations Manual.
 3. While investigating an accident in which the scene needs to be secured for an extended period the following may be applied:
 - a. Rerouting of traffic in order to ensure preservation of evidence and scene safety.
 - b. Opening of the roadway but restricting lane usage.

- c. Marking the scene in order to return at a later time when traffic congestion would be less of an issue.

V. Procedure: Responsibility

- A. The officer assigned an accident shall have scene responsibility unless relieved by a supervisor as established in Chapter 2 Section 12.1.2 (Command Protocol) of the Operations Manual. This responsibility shall include:
 - 1. Protecting the scene for the safety of parties involved and to preserve needed evidence.
 - 2. Identifying and assisting with injured persons
 - 3. Identifying the need for fire or rescue personnel
 - 4. Collecting all needed information to sufficiently report the accident.
 - 5. Securing valuables and other property belonging to victims.
- B. If an accident investigator is requested, they shall assume control of the scene in respects to collecting all needed information to sufficiently report the accident and preserving needed evidence.
- C. Fire and rescue personnel shall operate under their own command structure. Once on scene, fire personnel shall assume scene command in accidents involving a fire or hazardous material spill and returning scene control to the Police Department once these incidents have been resolved.
- D. Once on scene, rescue personnel shall have control of all aspects of victim triage and transportation but overall incident command shall remain with the Police Department.
- E. When needed, the Incident Command System as established in Chapter 5 Section 46.1.1(Critical Incidents) of the Operations Manual may be implemented to handle a large or severe accident scene, hazardous material spill, or other conditions.
- F. Patrol officers assigned to an accident investigation are responsible for the State of Iowa accident report, any needed follow up investigation, and all supplemental reports. At the end of the investigation, the assigned officer shall review the case file to ensure all needed reports have been submitted. When appropriate, an accident investigator and/or the Investigation Division may be called in to assist (e.g. fatalities, alcohol involved). When an accident investigator responds to assist, they shall assume case responsibility and ensure all case work is completed. At the end of the investigation, the accident investigator as well as the supervisor managing the crash unit shall review the case file to ensure all needed reports have been submitted.

VI. Procedure: Reporting

- A. Excluding standard accident reports, any accident investigated in whole or in part by a member of the crash unit shall be reviewed and approved by the supervisor managing the crash unit.

- B.** The supervisor managing the crash unit shall produce quarterly statistics and information to the patrol division commander or designee regarding the crash unit. The statistics may include but not be limited to the following:
 - 1.** Total number of accidents (delineated by type)
 - 2.** Summary and current status of all hit & run, pedestrian, and bicycle cases.
 - 3.** Number and type of cases investigated by the crash unit to include the number of cases cleared, suspended, closed, etc.
 - 4.** Any recommendations for traffic calming devices, signage, engineering improvements, etc. that may minimize or eliminate future accidents at a particular location.
- C.** Annually, the patrol division commander shall submit a summary report of the crash unit's activities to the chief of police.

VII. Procedure: Training and Equipment (Crash Unit)

- A.** The supervisor managing the crash investigation unit shall be responsible to coordinating in-house training of crash unit members as needed. All training will be documented on a department lesson plan.
- B.** Any outside training schools needed by members of the unit shall be submitted on a school/training request form to the supervisor managing the unit for initial approval. The request form will then move to the patrol division commander and the chief of police as necessary.
- C.** The supervisor managing the unit is responsible to maintain all equipment needed to perform accident investigations by the crash unit.
- D.** During the budget process, the supervisor managing the crash unit shall be responsible for submitting any budgetary items needed for the upcoming fiscal year to the patrol division commander.

Chapter 7: Traffic Operations
Section 61: Traffic
Subsection 3: Traffic Direction and Control



Policy/Procedure #: 1

Title: Traffic Direction and Control

CALEA Reference#: 61.3.1, 61.3.2, 61.3.3, 61.4.1, 61.4.2

I. Policy: Traffic Direction and Control

The safe and efficient flow of traffic throughout the City of Urbandale is a joint partnership between Engineering Department, Public Works, and the Police Department. A policy is established to ensure information is properly transferred to appropriate entities and departmental personnel are informed, equipped, and trained to address traffic direction and control.

II. Procedure: Traffic Engineering

- A.** Traffic engineering is primarily a function of the Urbandale Engineering Department, Urbandale Public Works Department, and the Iowa Department of Transportation (IDOT). The Department maintains a liaison with and provides data to these engineering authorities to maintain a safe and efficient road system.
- B.** The Patrol Division Commander shall be the liaison to the Engineering Department and the IDOT in matters involving road safety and efficiency. The Patrol Division Commander is responsible for coordinating the following activities related to traffic engineering records:
 - 1.** When needed, obtain traffic surveys or studies.
 - 2.** Forward information concerning physical conditions that contribute to traffic accidents and traffic congestion.
 - 3.** Forward information concerning parking needs, parking restrictions, and/or improvements.
 - 4.** Identifying high accident locations by forwarding traffic collision and enforcement data to the Iowa Department of Transportation and the Engineering Department. This data may be transmitted in the form of written reports or TRACs electronic data transmission.
 - 5.** Forward citizen complaints of possible engineering deficiencies

- C. Decisions on traffic control measures that involve the correction of engineering problems remains with local and state traffic engineering authorities who employ personnel trained in survey methods and techniques, traffic control measures, traffic planning, and traffic data analysis. Police personnel are encouraged to complete memorandums on traffic, road, and parking problems and to forward related suggestions through the chain of command.

III. Procedure: Traffic Direction

- A. Manual traffic direction may be used in the following situations:
 - 1. Failure of traffic control signals
 - 2. Emergencies.
 - 3. Accidents.
 - 4. Traffic control devices are not present or adequate.
 - 5. Other situations to alleviate traffic congestion or hazards.
- B. Effective manual traffic direction depends upon the use of clear and easily understood gestures and the high visibility of the person directing the traffic. In order to provide for officer safety and driver recognition and response, reflective high visibility vests/coats shall be made available to all officers. High visibility vests/coats shall be worn by all personnel when performing manual traffic direction activities unless an emergency situation prevents the officer from donning the vest/coat. In emergency situations, the officer shall don the vest as soon as practical.
- C. Officers performing traffic direction and control shall ensure their presence and purpose are appropriately indicated to drivers and pedestrians by the following actions:
 - 1. Selecting a position where they can be seen clearly by all, usually in the center of an intersection or street.
 - 2. Keeping hands and arms at their sides, except when gesturing.
 - 3. Stand facing or with back to stopped traffic and with your sides toward traffic being directed to move.
 - 4. Utilizing signals and commands that are easily understood.
 - a. To stop: Stand with shoulders parallel to the traffic, raise arms forty-five degrees above the shoulders, with hand extended and palm towards the moving traffic to be stopped. To stop traffic from both directions repeat the above actions for the traffic from the opposite direction while continuing to hold the other stopped traffic with arm outstretched and palm towards the traffic. Ensure the lead car has come to a complete stop before turning your attention away by observing the vehicle come to a stop and by making eye contact with the driver when possible.
 - b. To move: Stand with shoulders parallel to the traffic to be moved. Extend the right arm and hand full length, at shoulder height towards the traffic to be moved, with fingers extended and palm up.

Bring the hand up in the direction the traffic is to be moved. Repeat the movement with the left arm and hand to start traffic from the opposite direction.

- c. Right turns: Vehicles turning right shall be directed to perform their turn by extending the arm towards the direction in which the turn is to be made.
 - d. Left turns: Left turns are to be made only when there is a gap in traffic or oncoming traffic is completely stopped. When it is safe to do so, vehicles turning left shall be directed to perform their turn by extending the arm towards the direction in which the turn is to be made.
- D. Officers directing traffic may utilize a police vehicle, flashlights, traffic cones, barricades and/or road flares while manually directing traffic to increase visibility and ability to control and restrict vehicle movements.
- E. Officers directing traffic shall remain calm and professional when directing traffic. There are times when drivers and pedestrians do not understand officers or may refuse to obey directions. The officer shall handle these instances with courtesy and professionalism within the guidelines of accepted procedures.
- F. Officers shall utilize their patrol vehicle's emergency equipment to assist in directing traffic at the scene of an accident. If it becomes necessary to perform manual traffic direction, officers shall utilize the procedures noted above to safely move traffic around an accident scene. Use of a second unit to assist with traffic direction and control may be necessary while managing the accident scene. Officers shall work in conjunction with responding fire or rescue units.
- G. During an accident, scene safety for victims and responding personnel and preservation of evidence shall take precedent over traffic congestion concerns; however, as soon as practical the roadway shall be reopened.
- H. Emergency traffic direction shall be provided during any critical incident to include but not be limited to fire, medical emergency, severe weather incident, barricaded subject, hazardous materials incident, etc. Officers shall support responses to these emergencies by providing traffic direction and control. Officers shall consult with the ranking officer in charge of the emergency scene to determine their needs and provide needed support by restricting or redirecting vehicles in and around the scene.
- I. Officer shall respond to adverse road and weather conditions which may include, but are not limited to:
 - 1. Accident hazards such as debris which has fallen onto the roadway, downed power lines, fallen trees, etc.
 - 2. Acts of nature such as fog, flooding, ice on the road, etc.
 - 3. Engineering hazards such as an extensive water leak, buckled roadway, missing manhole cover, large hole in the pavement, etc.

- J. Upon discovering an adverse road or weather condition affecting safe roadway travel, department members are expected to notify communications so the proper personnel are contacted to correct the situation. When manpower allows, officers shall provide traffic direction, control services, and scene protection in the vicinity of adverse road and weather conditions, as appropriate and until the problem is corrected or protected by traffic control devices.
- K. Only under the most extreme circumstances shall a traffic signal be manipulated to be operated manually. This would require the assistance of the Engineering Department or the IDOT and would only be considered if the need for the manipulation was expected to last for an extended period of time. When necessary, officers may use manual traffic direction techniques to direct traffic against a traffic control device. Officers shall exercise extreme caution when performing this act ensuring vehicles are fully aware they must follow the officer's command and ignore the traffic signal. Multiple officers and use of aids as described above may be necessary.
- L. Generally, temporary traffic control devices shall be used in pre-scheduled special events. Temporary traffic control devices may include movable barriers, portable signs, and other apparatus intended for temporary deployment to assist in the safe and efficient movement and control of vehicular and pedestrian traffic. The devices will normally be placed and removed by the Public Works Department with the Police Department coordinating the placement of such devices. Portable and temporary stop signs may also be used in emergency cases such as accidents, natural disaster, power failures, missing traffic signs, etc.

IV. Procedure: Police Escort

- A. Escort services may be provided in situations where such services would be advantageous to traffic control and direction. Escorts may include, but are not limited to; motorcades, funerals, and oversized/hazardous loads, and parades.
- B. Emergency escorts will not be conducted. Officers encountering citizens requesting escort for a medical emergency shall summon emergency medical services. Depending upon the circumstance, the officer may consider allowing the citizen to continue on without delay if they will obey traffic laws.
- C. Requests for non-emergency escorts shall be referred to the Patrol Division Commander or designee for assignment. When necessary, members shall be assigned to key intersections to ensure safe passage.

V. Procedure: Motorist Assist

- A. Disabled vehicles on the roadway present a hazard both to the stranded motorist and to other vehicles. When possible, officers shall offer reasonable assistance to motorists who appear to be in need of aid.

- B.** Stranded motorists shall not be left unattended when they appear to be exposed to hazardous situations. Due consideration shall be afforded to stranded motorists for factors that contribute to hazardous conditions such as location, time of day, weather, and pending calls for service. When circumstances preclude an officer from remaining with the motorist, flares may be placed, or the hazard lights of the vehicle turned on and the hood raised to warn oncoming traffic and provide reasonable safety until the problem can be resolved. If the disabled vehicle is on the interstate system, the Highway Helper program may be requested to provide assistance to the motorist.
- C.** When requested, officers shall courteously provide information and directions, and shall attempt to remain familiar with various services and facilities available to help motorists.
- D.** Officers may transport stranded motorists to the nearest convenient location where assistance may be obtained.
- E.** When hazardous weather conditions exist, communications may be requested to disseminate road hazard, travel, and road closing information for the city or if outside the city, refer citizens to the roadway condition number provided by the IDOT.
- F.** In the event the owner of a disabled vehicle is unable to obtain their own towing service or have no preference, the officer may obtain towing from the designated police towing service.
- G.** In the event a person is in need of emergency medical or fire assistance, the officer shall notify communications of the nature of the emergency and request the appropriate services. The officer shall render aid within the scope of training and experience until the proper service arrives.
- H.** In emergency situations, officers operating a patrol vehicle with a push bumper are allowed to push disabled vehicles a short distance to mitigate the hazard. Officers shall only push similarly sized vehicles and only when doing so will not cause damage to their vehicle or the disabled vehicle.
- I.** Officers may attempt minor repairs to disabled vehicles to include jump-starting or changing a tire only if they are knowledgeable on how to properly and safely perform the service. Officers shall not attempt minor repairs if the disabled vehicle is in a dangerous position in relation to other vehicles on the roadway.
- J.** Officer shall be allowed to unlock vehicles for motorist who have locked their keys in their vehicles utilizing the unlocking tools provided by the Department under the following circumstances:
 - 1.** Generally, vehicle unlocking will be performed on vehicles that do not have electric wiring in the door panel or the officer is able to unlock without entering the interior of the door panel (i.e. use of the "Big Easy")

unlocking tool); however, the supervisor may temporarily suspend the unlocking service when workload conditions warrant.

2. In non-emergency situations, the officer shall advise before attempting to gain entry to a vehicle, the officer and the City of Urbandale are unable to assume any liability for damage caused by attempting to gain entry.
3. If the officer does not feel they can unlock the vehicle without causing damage, the motorist shall be referred to a locksmith or obtain approval from the requesting party with full knowledge that damage is likely to occur.
4. If the attempt to gain entry causes known damage to the vehicle, the officer shall advise communications of the damage. Communications or the officer shall record the damage information in the call log.
5. When there is a child or pet in the vehicle and the officer is unable to gain entry, the officer shall stand by for a professional locksmith. If conditions warrant or at the request of the person in possession of the vehicle, a supervisor may authorize damaging a vehicle to rescue a child or animal in distress. This would include breaking a window to gain entry when necessary.

VI. Procedure: Hazardous Roadway Conditions

- A. During normal patrol activities, officers must remain alert for unsafe or hazardous conditions on or near roadways. When hazard is discovered and the officer is unable to correct, Urbandale Public Works or the IDOT shall be notified to correct or properly secure the problem area.
- B. When roadway hazards are an imminent danger to the motoring public, officers shall initiate appropriate corrective action to remove the hazard or take action to protect the hazard until corrective action can be taken by the appropriate agency. Should a hazard require only corrective action (e.g. parking sign down), the officer shall notify communications who will notify the responsible agency when convenient.

Chapter 8: Detainee and Court Related Activities
Section 70: Detainee Transportation
Subsection 1: Transportation Operations



Policy/Procedure #: 1

Title: Transporting Detainees

CALEA Reference#: 70.1.1, 70.1.2, 70.1.3, 70.1.4, 70.1.5, 70.1.6, 70.1.7, 70.1.8, 70.2.1, 70.3.1, 70.3.2, 70.3.3, 70.4.1, 70.4.2, 70.5.1

I. POLICY: Transporting Detainees

A policy is established to guide officers during the transportation of detainees. The policy shall focus on security, safe practices, and responsibilities of the officers of the Urbandale Police Department. Acknowledging the responsibility to the community and the person detained, the Department shall take all reasonable precautions necessary to securely and safely transport detainees and prevent their escape.

II. PROCEDURE: General

- A.** Only sworn officers shall be allowed to transport detainees. Officers shall only transport detainees in a manner that provides safety and security for the detainee, the transporting officer, and the public. The transporting officer assumes responsibility for the safety and control of the detainee being transported from the time the officer accepts custody to the time custody of the detainee is relinquished to a detention facility.
- B.** All employees shall ensure detainees are not subject to discriminatory treatment based upon race, religion, nationality, disability, sex, or age.
- C.** As soon as practical, detainees shall be transported to the appropriate jail, holding facility, court, medical facility, or turned over to another law enforcement agency.
- D.** Except as noted in this policy, any time a person is detained and placed in a police vehicle, they shall be constantly monitored by the presence of an officer until release or transfer.
- E.** Upon taking or assuming custody of a detainee, the arresting and/or transporting officer shall search the subject for contraband or weapons. A proper search shall include an examination of the contents of all pockets, articles of clothing, baggage and purses as well as an appropriate pat-down of clothing. Transporting officers shall also search the detainee each

time they assume custody (e.g. after a hospital visit or any time the detainee has been removed from the transporting officers constant supervision) unless they have personally observed a search by another officer immediately prior to accepting the detainee. Officers must never assume the detainee has been searched by someone else. Search guidelines based on the gender of the detainee as stated below shall be followed:

1. A search, by means of a pat down/frisk, of all detainees shall be conducted prior to a detainee being placed in a vehicle in order to ensure officer safety.
2. A pat down/frisk shall be conducted by an employee of the same gender. A pat down/frisk by an employee of the opposite gender may be completed when exigent circumstances warrant such action. A pat/down search by a person of the opposite gender must be documented in the CIR, supplemental report, or CAD entry including details as to exigency that necessitated the action.
3. Strip searches shall only be conducted in compliance to policy and procedure as stated in Chapter 1 Section 1.2.8 of the Operations Manual.
4. When a detainee has identified themselves as transgender or the officer is unable to determine the gender of an individual, the following shall apply:
 - a. Officers shall inform the individual of their right to express a preference of gender.
 - b. Absent exigent circumstances, before performing any level of search of the individual, officers shall inform the individual of their right to request a preference of the gender of the officer that will conduct the search.
 - c. The request and response shall be video recorded when possible and documented in the officer's booking report.
 - d. If the request is not granted, the reason for not granting the request shall be documented.
 - e. Absent exigent circumstances, if the individual has a preference, at least one officer of the gender requested shall conduct the search.
 - f. The officers may take into account the reasonableness of any delay created by waiting for another officer.
 - g. If the individual does not specify a preference, at least one officer of the individual's gender expression shall conduct the search. Example: A male officer would search an individual stating no gender preference expressing themselves as a male.
 - h. When in doubt regarding search of a transgender individual, officer shall consult with a supervisor.
 - i. The identified gender or the expressed gender (if failing to identify) shall be the gender utilized and applied to all processing, supervision, privacy, and separation requirements stated in this policy.

- F.** Whenever civilians are to be transported in a Department vehicle for the purpose of public assistance or some other non-criminal matter, the officer shall use their discretion as to whether they should request a pat-down search for officer safety purposes only. If the decision is made to conduct a pat-down search, the officer shall request permission from the individual to conduct the search and explain to the individual it is for safety purposes. Refusal to submit to such a search shall justify the officer's refusal to transport.
- G.** Transporting officers are responsible for ensuring any vehicle used to transport a detainee is safe, not damaged or defective, appropriately equipped, and free of weapons and contraband. This inspection shall occur before and after a detainee has occupied the vehicle. Officers shall always be mindful of the introduction of weapons, contraband, or any other items or conditions. At the beginning of each shift, officers shall search their vehicle for any contraband or weapons that may have been left in the vehicle. Prior to a detainee being transported, the vehicle shall be examined again unless the vehicle has been in the constant control of the officer since the last inspection. In addition, any officer transporting a detainee shall search the vehicle once the detainee has been removed from the vehicle.
- H.** Officers shall not transport more than two (2) detainees at the same time in a vehicle with a full back seat safety barrier and only one (1) detainee in a vehicle with a ½ back seat safety barrier or no safety barrier. Detainees shall be seated in the vehicle's rear compartment in a manner that limits their opportunities for escape or attack as much as possible. While transporting detainees, officers shall be seated in a manner that allows them to observe the detainee at all times. Detainees shall be properly restrained and whenever practical, seat belted during transport. In cases where the detainee is combative, it is not necessary to utilize seat belts if doing so would expose the transporting officer to substantial risk of attack. Under no circumstances shall a detainee be transported in the front seat of a vehicle.
- I.** Male, female, and transgender detainees as well as juvenile and adult detainees shall not be transported in the same vehicle. Exceptions may be granted by a supervisor based on the relation of the detainees and the reason for their detention (e.g. husband and wife both arrested for shoplifting).
- J.** Unless there is an incident involving grave and imminent danger and the transporting unit is the only unit able to respond, transporting officers shall not be assigned to handle other calls, interrupt their transportation to handle a call, or make any stops between the point of detention and the detention facility. In the rare event an incident of this nature occurs, a supervisor shall authorize the transporting officer to respond. Transporting officers shall remain mindful of the possibility of diversionary tactics that may be deployed to divert the officer, place the welfare of the detainee in jeopardy, or facilitate the detainee's escape. In all

instances, the officer shall only render assistance in a way that poses the minimum danger to the detainee or risk of the detainee's escape. Only when the risk to the detainee is minimal and the risk to a third party is grave shall an officer render assistance while transporting a detainee. Officers shall use extreme caution in these situations and shall not lose visual contact with the detainee. Officers are not authorized to make an emergency response while transporting a detainee.

- K. Due to the inherent difficulty in maintaining safety and security for the public, the detainee, and the transporting officer, a detainee being transported shall not be allowed to communicate with others. The detainee's right to communicate with their attorney and others shall not be exercised during the period the detainee is being transported. If special circumstances arise that necessitates an exception, supervisory approval shall be gained.
- L. Officers shall be required to notify communications of the start time, start location, end time, and end location when transporting a detainee. This information shall be logged by communications creating a permanent record.
- M. Except for offenses that by state law require a court appearance, all detainees shall be afforded the opportunity to post bond in lieu of continued custody. Posting of bond shall be completed at the appropriate jail or holding facility. As the Department no longer operates a holding facility, no bond will be accepted at the Urbandale Police Department.
- N. No employee shall transact business with any detainee, nor shall any employee arrange through another party any business transaction with a detainee. Employees shall abide by the Department's Code of Ethics as established in Chapter 1 Section 1.1.1 of the Operations Manual. This prohibits employees from using their official positions to secure privileges for themselves or others and prohibits employees from engaging in activities that constitutes a conflict of interest.
- O. When a detainee is received from an outside agency, positive identification shall be made of the person presenting the detainee. The official's name and/or agency as well as how the officer verified the authority to make the commitment shall be recorded by the accepting officer in a supplemental report or a computer aided dispatch entry. After the presenter is identified, the officer will verify the official's authority to make the commitment. Identification shall be verified in at least one of the following ways:
 - 1. The outside agency official is known to the officer.
 - 2. The outside agency official is in full uniform and/or is operating a fully marked police vehicle from a known police agency.
 - 3. The accepting officer requests official identification from the presenter.
 - 4. If identification is still an issue, the accepting officer will contact their supervisor for assistance and approval.

III. Procedure: Detainee Health

- A.** Officers shall seek immediate medical attention for detainees in their custody who are sick or injured. If an individual requests medical attention or if the officer determines medical attention is needed, the arresting or transporting officer must make all reasonable efforts to ensure medical attention is given. Any medical attention received or the refusal of such treatment, shall be documented in a supplemental report.
- B.** Any person who is obviously injured, ill, or unconscious shall be examined by qualified medical personnel before being transferred to a holding facility or jail.
- C.** Any detainee in need of medical assistance shall be transported to Broadlawns Medical Facility in Des Moines. If Broadlawns is unable to provide the needed care, other medical facilities may be utilized. Any requests to utilize a facility other than Broadlawns shall be approved by a supervisor. If the detainee is transported to Broadlawns, their current condition including any known allergies and past medical/surgical history shall be given to the hospital.
- D.** Detainees shall be observed for behaviors or physical characteristics consistent with signs of being under the influence of alcohol or other drugs, or violent, self- destructive behavior. This information shall be provided to the holding facility or jail. If the detainee presents a safety risk to themselves or others, holding facility or jail staff shall be notified prior to arrival at the facility to allow for staff precautions, enhanced observation, or possible segregation.
- E.** Medications, prescription or over the counter, shall not be administered by Urbandale Police Department employees. When a detainee is in need of medication, even if they have the medication in their possession, they shall be transported to a hospital or medical clinic. Hospital or medical clinic staff may administer medications pursuant to a physician's orders. If needed, Urbandale Fire and Rescue personnel may also administer needed medications during an emergency situation.
- F.** If a detainee has legally obtained medication in their possession when detained and the detainee requires medical treatment, the medication shall be transported under control of an officer or Urbandale Fire Department personnel to the medical facility or hospital. This will allow administration of the medication by a physician if deemed necessary.
- G.** When a subject is detained and is on medication, no action by the officer is necessary if custody of the subject detained will be terminated or transferred to another agency prior to the need for the medication. Any agency accepting a transfer of custody will be made aware of the detainee's need of medication at the time of the transfer.
- H.** At no time shall an officer request or require a detainee be sedated. The need for sedation of a detainee is a medical determination and shall be made by qualified medical personnel without influence from Urbandale Police personnel. When possible, the sedation of a detainee shall be completed at a hospital by qualified medical staff based on their medical evaluation of the detainee.

- I. During times when there is no means of immediate access to court, a person arrested on a charge constituting a simple misdemeanor and believed to be mentally ill, and due to that illness is likely to physically injure the person's self or others, shall be transferred to the Polk or Dallas County jail or other holding facility only after the arresting officer has demonstrated a reasonable effort to comply with the emergency hospitalization procedure as provided in Iowa Code section 229.22.

IV. Procedure: Detainee Property

- A. Officers shall be responsible for the safe handling and security of any property removed from a person during detention even if that detention is temporary.
- B. Any items that will be seized as evidence shall be listed on a property sheet and entered into property/evidence as stated in Chapter 9 Section 84.1.1 (Property and Evidence).
- C. Detainees shall not be allowed to retain custody of baggage, purses or other items. Plastic bags shall be available to all officers to hold a detainees items during transport. All items shall be kept in the driver's compartment or in the trunk of the transporting vehicle where the detainee does not have access.
- D. If a detainee has personal property items in their possession the arresting officer shall complete a detainee personal property log listing the items. Inventory of the property shall occur in plain view of the officer's body worn camera or the holding facility/jail camera system. Upon transfer of custody to the jail or holding facility, release to another law enforcement official, or release of the detainee in lieu of continued custody, one of the following procedures shall be completed:
 1. The official accepting the transfer of custody shall sign the personal property log accepting the items. The accepting official should verify all property listed on the inventory sheet is complete and accurate.
 2. When released in lieu of continued custody or upon transfer to another facility or law enforcement official, the detainee shall sign for the return of their personal property. All property listed on the personal property log should be verified as complete and accurate by the detainee prior to release.
 3. If a detainee is uncooperative, incapacitated or for other reasons it is unsafe or impractical to have the detainee sign for their property, a second officer shall verify the detainee's property prior to transfer of custody. Officers shall indicate on the personal property log the reason for not obtaining the detainee's signature.
- E. The transfer of personal property items to the jail, holding facility, other officer or official, or return to the detainee shall be captured on the officer's body camera or facility video recording (If applicable).

V. PROCEDURE: Transfer to Detention Facility

- A. Officers shall adhere to the following guidelines when arriving and departing with a detainee at the Polk or Dallas County Jail:

1. If the facility has a "sally port" or secured enclosure for unloading a detainee, the officer shall not remove the detainee from their vehicle until the enclosure is secured.
 2. The officer must secure their firearm and/or other weapons as prescribed by the facility in their designated safe area. The prescribed weapons shall be secured prior to removing any restraints from the detainee.
 3. No restraints shall be removed from the detainee until they are inside the secure area of the facility.
 4. All required documentation shall be delivered at the time custody is transferred to the accepting facility.
 5. The transporting officer shall notify the facility staff verbally and by written documentation if the detainee has any medical or security risks.
 6. Transfer of custody of the detainee to the facility shall be relayed to communications for the purpose of recording the date and time of the transfer.
 7. When departing with a detainee, the officer shall ensure the detainee is properly restrained prior to leaving the secure area and prior to retrieving their secured weapon. When possible, the detainee shall be secured within the vehicle prior to the officer opening the secure enclosure where the vehicle is parked.
- B.** If the detainee is being transferred to another agency or facility and they pose an unusual security risk, the transporting officer shall be responsible for notifying the agency or facility of the risk in advance of their arrival. This will allow the agency or facility to make needed preparations for accepting the detainee. This advanced notification shall be documented in a supplemental report or a computer aided dispatch entry.
- C.** Before transporting a detainee from any detention facility, the officer assigned to transport must verify the detainee's identification through booking records, photo identification, or other appropriate means. The officer shall ensure they have all needed documents to transfer the detainee. This may include a booking sheet, property log, any accompanying information needed to substantiate current charges or reason for detention. Prior to transfer, the transporting officer shall review all documents for completeness and accuracy. Verification of identity, including method used, shall be recorded in a supplemental report or in a computer aided dispatch entry.
- D.** Prior to the transport, transporting officers shall inquire as to any escape or suicide attempts, unusual illnesses or health risks, or any tendencies toward violent behavior. If applicable, this information shall be recorded in a supplemental report or a computer aided dispatch entry.
- E.** While transporting detainees from a jurisdiction located in a state other than Iowa, the officer must have in his possession a valid warrant authorizing extradition or a legally signed waiver of extradition. Transporting officers shall ensure the identity of the person being released to them is in fact the same person being sought by the Urbandale

Police Department, utilizing booking records, photo identification, or other means. This information shall be recorded in a supplemental report or a computer aided dispatch entry.

VI. PROCEDURE: Escape during Transport

A. In the event a detainee escapes from custody while being transported, the following procedures will be followed:

1. The transporting officer shall immediately notify communications of the escape and provide at a minimum the following information:
 - a. The location of the escape and the detainee's last known direction of travel.
 - b. A complete physical and clothing description.
 - c. The charges for which the person was being detained and whether the detainee is a danger to the public, other officers, or themselves.
 - d. The transporting officer shall also immediately notify their supervisor of the escape.
2. As soon as possible, communications shall notify surrounding agencies of the escape as well as coordinate with supervisor requests for any needed assistance.
3. The supervisor shall assume control of the incident and has the responsibility for coordinating the search efforts and if necessary, request any additional personnel or assistance from outside agencies.
4. As soon as practical, the supervisor shall notify the division commander of the officer handling the transport.
5. The transporting officer shall be responsible for completing an offense report detailing the escape, a chronicle of the events leading up to the escape, and other pertinent information regarding the detainee that are relevant.

B. The division commander of the transporting officer shall review the escape and the subsequent response. Documentation shall be submitted to the Chief of Police detailing any needed areas of improvement and/or failure to follow policy or procedure that contributed to the escape.

VII. PROCEDURE: Restraining Devices

A. The Department shall utilize the following types of restraints to secure detainees prior to transportation or for temporary detention:

1. Handcuffs – Handcuffs shall be the recommended method for restraining persons. Handcuffs may be chain or hinged type.
2. Leg Restraints -- Leg restraints shall be utilized when transporting a person that is deemed a risk to escape or when transporting a person long distances which may require stops before reaching a destination.
3. Flex Cuffs -- These restraints are intended as temporary, emergency restraining devices. Officers utilizing flex cuffs shall replace flex cuffs with handcuffs as soon as practical. If flex cuffs are not removable, only a safe cutting device shall be utilized to clip or cut the flex cuffs off. At no time shall an officer utilize a knife to cut off flex cuffs due to the risk of injury.

4. **Waist Restraint Device-** A waist restraint device may be utilized with handcuffs to secure a detainee's hands in the front of their person. The waist restraint device shall only be used for transports to or from facilities outside of Polk or Dallas County, during transports by medical personnel, or for special circumstances as determined by a supervisor. At no time shall the waist restraint device be used to secure a detainee other than as the manufacturer of the device has intended.

- B. Officers utilizing handcuffs to restrain detainees or to temporarily detain persons shall make every effort to handcuff the individual's hands behind their back. Handcuffs must not be applied in a manner that intentionally inflicts injury or pain to the detainee. In instances where the individual cannot physically place his hands behind his back, the officer may elect to use two sets of handcuffs linked together. Such circumstances may be due to the physical stature of the person being handcuffed or due to an injury or illness sustained by the detainee. In rare instances, the officer may elect to handcuff the individual in front, but due to the additional risks of such a tactic, the officer shall obtain supervisory approval and exercise extreme caution during the remainder of their contact with the detainee. Notation for the reason to handcuff in front shall be documented in a supplemental report or a computer aided dispatch entry.
- C. It shall be prohibited for an officer to restrain any person in a manner commonly referred to as "hog tying." "Hog tying" is where a detainee's hands are restrained behind their back and attached in some manner to the feet. Restraining a detainee in this manner may lead to positional asphyxiation.
- D. Officers shall ensure no detainee, once handcuffed, is allowed to lie face down on the ground. As soon as practical, a handcuffed individual shall be placed in a sitting or standing position. If necessary, an individual may be placed on their side but shall be constantly monitored for any signs of distress. While in any type of restraining device, the detainee shall be constantly monitored by personal observation of an officer.

VIII. PROCEDURE: Transporting Sick, Injured or Disabled Detainees

- A. Following the completion of medical treatment, regardless if such treatment is actually accepted by the detainee or delivered by medical personnel, the detainee shall be searched for contraband prior to being transported.
- B. A supervisor shall determine if a detainee needing transported to receive medical treatment may be transported by ambulance or police vehicle. If transported by ambulance, the supervisor shall also determine if an officer should ride in the ambulance or follow the ambulance to the hospital. In making the determination, the supervisor shall consider the security risks of the detainee and their current medical condition. When practical, the detainee shall be restrained in an ambulance by using a waist restraint device or handcuffs.

- C. When a detainee who is in the custody of the Urbandale Police Department is transported to a hospital or other medical facility, the transporting officer shall follow the following procedures:
 - 1. The transporting officer shall request the hospital staff place the detainee alone in a room, away from other patients.
 - 2. The transporting officer shall ensure the detainee is not left alone or unobserved.
 - 3. Privacy concerns for detainees shall be granted to the extent they do not endanger the detainee, the officer, other parties, and escape is not possible.
 - 4. Restraints shall be utilized for the duration of the visit unless a request by the hospital staff is made to remove them for treatment purposes.
- D. If the detainee is to be admitted to the hospital, the following procedure shall be observed:
 - 1. If the charges against the detainee necessitate the detainee remain under constant police supervision, the officer shall notify his immediate supervisor who shall arrange for a temporary security schedule. The supervisor shall notify the division commander of the officer that has the subject detained so plans for extended security can be made. The security of the detainee shall be the responsibility of the division that has detained the subject. Requests for assistance from other divisions for maintaining supervision of a detainee shall be directed to the division commander from whom the assistance is needed.
 - 2. If the detainee cannot be cited and released while at the hospital and a supervisor determines the charges against the detainee does not warrant a continued police presence, the transporting officer shall notify the respective hospital's security department and arrange for the hospital contact the Department when the detainee is scheduled to be released.
 - 3. When released from treatment by the hospital, the detainee's condition shall be closely monitored. All post-release instructions by medical personnel shall be obtained in writing and included in the detainee's property.
 - 4. When an officer is assigned to pick up a detainee from the hospital, the officer shall search the detainee prior to placing him in a police vehicle. If transporting the detainee to a county jail, the officer shall apprise jail personnel of the treatment as well as instructions for future treatment or medications both verbally and through written documentation.
- E. On occasion, a detainee may require special care or attention while being transported because of a physical or mental impairment. The transporting officer, with approval and assistance of their supervisor, shall arrange for any special equipment or special vehicles to facilitate the transport in a safe and secure manner. Special vehicles, such as an ambulance, shall be used when safe transportation cannot be accomplished using a police vehicle. Any medication for the detainee as well as mechanical aids,

unless required for life support, shall be retained in the control of the transporting officer. Transporting officers shall use the appropriate equipment required to securely restrain the detainee without causing injury. All special arrangements shall be documented in a supplemental report or a computer aided dispatch entry.

IX. PROCEDURE: Special Situation Transports

- A.** Urbandale Police Department personnel shall transport detainees when directly related to a legitimate law enforcement activity, when directed by a court, or when authorized by the Chief of Police. If a special situation requiring detainee transportation is directed by a court or authorized by the Chief of Police, the following procedures shall apply:
 - 1.** The transporting officer shall search the detainee prior to placing them in the transport vehicle and shall assume the detainee has not been searched by someone else.
 - 2.** The transporting officer shall utilize the appropriate level of restraint for the detainee at all times during the transport.
 - 3.** The detainee shall remain within sight of the officer at all times during the transport.
 - 4.** The transporting officer shall comply with all other policies regarding the transportation of detainees during special transport situations.

X. PROCEDURE: Transport Equipment

- A.** Marked patrol units assigned to routine patrol functions shall be equipped with a safety barrier to prevent the detainee from having access to the driver's compartment. If a patrol unit is not equipped with a safety barrier, it shall not be utilized to transport a detainee unless a second officer or matron is available to ride in the rear of the vehicle next to the detainee.
- B.** If a detective needs to transport a detainee, they should utilize a patrol unit with a safety barrier. If not utilizing a patrol unit, the detainee shall be properly restrained (handcuffs, etc.) and seat belted in the rear seat of the transport vehicle with an officer or matron in the rear seat next to them. The officer shall take a position in the rear seat with their weapon side away from the detainee. If utilizing a matron, the detainee shall be seated on the passenger side of the rear seat. At no time shall any police vehicle without a safety barrier be utilized to transport a detainee that is combative or a security/escape risk.
- C.** Patrol units utilized for detainee transports shall have all rear passenger window controls and door handles disconnected and/or removed to prevent detainee escape.
- D.** Spit hoods are temporary protective devices designed to greatly reduce the ability of a detainee to project saliva or mucous through spitting. A spit hood may be placed on a detainee when the officer reasonably believed the detainee has or will spit on the officer or others. Officers utilizing a spit hood shall ensure the hood is properly placed on the detainee to allow adequate ventilation and normal breathing. A spit hood shall not be used if the detainee has a medical condition that compromises their ability to breath normally. The spit hood shall be removed immediately if the

detainee experiences any difficulty breathing or vomits. Detainees that have been exposed to chemical deterrent shall be thoroughly decontaminated prior to the application of a spit hood. When utilizing a spit hood, a detainee shall be constantly monitored and shall not be left unattended at any time. Spit hoods shall be available in all patrol vehicles and shall be discarded and replaced after use.

XI. Procedure: Detainee Records

- A.** The security and privacy of criminal records and individual criminal histories shall be governed by chapter 692 of the Code of Iowa and by Title 28 of the Code of Federal regulations.
- B.** All records pertaining to detainees, such as arrest reports, records, etc., shall be maintained in such a manner as to safeguard them from unauthorized disclosure.
- C.** A separate medical record shall be maintained for each detainee receiving medical care. The record shall include the illness being treated, medication administered and the name of the attending health professional or institution. The record may be kept in the detainee's file but must be labeled "confidential."
- D.** All records of an arrest by the Urbandale Police Department shall be maintained by the Support Services Division. The records are located in a locked and controlled environment not accessible to the public or unauthorized persons.
- E.** Upon a detainee's release or transfer, all records pertaining to the detainee shall be forwarded to the Support Services Division. Any release of information or requests for information shall be handled in accordance with the Freedom of Information Act and applicable Department policy as stated in Chapter 9 section 82 of the Operations Manual.

Chapter 8: Detainee and Court-Related Activities
Section 71: Processing and Temporary Detention Area
Subsection 1: Organization, Administration and Management



Policy/Procedure #: 1

Title: Processing and Temporary Detention

CALEA Reference#: 71.1.1, 71.2.1, 71.2.2, 71.3.1, 71.3.3, 71.4.1, 71.4.2, 71.4.3

I. Policy: Processing and Temporary Detention

A policy is established to govern the processing and temporary detention of persons at the Urbandale Police Department to ensure the safety and security of the person being detained and the employees. Persons subject to arrest or detention shall only be held at the Urbandale Police Department for the amount of time necessary to properly record the arrest/detention and prepare documentation to release the subject on a citation or transfer to an authorized holding facility or immediate court appearance.

II. Procedure: Designated areas and training:

- A.** The following areas within the Urbandale Police Department are authorized and designated for processing, testing, and temporary detention of persons under arrest or juveniles under detention:
1. Sally port #1-Secure area for loading and unloading detainees.
 2. Temporary Detention room #5- Booking and OWI processing.
 3. Temporary Detention room #4- Detainee restroom and drinking water.
 4. Temporary Detention room #6- Holding room
 5. Temporary Detention room #8- Visitation room
 6. Temporary Detention Room #9- Visitation room (physical contact requested)
 7. Temporary Detention Identification Room- Fingerprinting and photographing.
 8. Temporary Detention main hallway- Field sobriety testing.
- B.** All sworn officers and reserve officers shall receive initial training on use of the processing and temporary detention area. At a minimum, the training shall include:
1. Requesting emergency assistance.
 2. The location of fire suppression equipment.
 3. Key location.
 4. Evacuation training.

5. Use of designated processing and testing rooms.
- C. New officers/reserve officers shall receive documented initial training as part of their field training program.
- D. All sworn officers and reserves shall complete a documented initial and annual review of the department policy and procedures related to the use of processing and testing areas within the temporary detention facility.
- E. All sworn officers and reserve officers shall receive refresher (in-service) training at minimum once every 4 years.

III. Procedure: Physical Conditions

- A. All aspects of the processing and temporary detention areas shall be maintained proper working order. The facility shall meet the following minimum conditions for detainees:
 1. Adequate lighting. At no time shall the lights in a detention area be turned off when the area is occupied.
 2. Circulation of air. The area shall be maintained at an appropriate temperature comparable to the rest of the police facility. If needed, the detainee may be supplied with a facility blanket.
 3. Access for detainees to a restroom, drinking water, and other basic needs as encountered.
- B. Drop cords shall not be used as permanent wiring in the processing and temporary detention area. All electrical service shall meet the requirements of the City code for electrical service. Any appliances shall plug directly into a fixed receptacle. Emergency generator power shall be available to the processing and temporary detention area in the event of a power failure. The emergency generator power shall be tested at regular intervals not less than monthly. A record of test dates shall be maintained.

IV. Procedure: Safety and Sanitation

- A. The processing and temporary detention area is equipped with automatic fire, smoke and heat detection equipment. The equipment shall be approved, inspected and tested annually with the assistance of the Urbandale Fire Department or a certified private vendor.
- B. The processing and temporary detention area shall also adhere to the following requirements:
 1. An emergency evacuation plan for the facility.
 - a. During an emergency evacuation, all detainees shall be removed from the facility through the north exit door to the north parking lot or through the east exit door into the sally port and then through the sally port overhead door to the north parking lot.
 - b. Once in the north parking lot detainees shall be secured in patrols cars and as soon as possible transported the Polk or Dallas County jail.
 - c. Relevant portions of the evacuation plan shall be posted in the processing and temporary detention area.
 - d. All sworn officers and reserve officers shall receive training on evacuation of the processing and temporary detention area as part

of the initial training noted above with refresher (in-service) training every four years.

2. A designated and properly signed emergency exit directing persons to hazard free area.
- C. The processing and temporary detention area shall be inspected monthly as part the facility inspections conducted by the command staff for sanitary conditions, any damage or defacement, and any conditions that would promote the presence of vermin or pests. The inspection shall also ensure all doors and locks are functioning properly.
- D. A first aid kit shall be placed in the processing and temporary detention area in an accessible location. The first aid kit shall be inspected as part of the command staff monthly inspection. When supplies are needed, a request should be forwarded to support services division via repair/service request form or the monthly inspection report.

V. Procedure: Security and Control

- A. All detainees shall be searched for weapons and contraband prior to entering the facility.
- B. Access of nonessential persons to the processing and temporary detention area shall only be allowed when no detainees are in the facility. All nonessential persons allowed into the processing and temporary detention area shall be supervised at all times. Exceptions to constant supervision may be granted by the support services division commander for specific projects (e.g. long term construction projects, daily cleaning, technical support, etc.). At the conclusion of any maintenance or construction other than general cleaning and prior to use of the facility for detention, an inspection shall be completed by support services division personnel or designee to ensure all tools and equipment have been removed.
- C. Non-detained persons entering the processing and temporary detention area may be subject to a search for contraband and weapons. Non-detained persons shall be denied admission if they refuse to consent to a required search. A search notice shall be posted in a conspicuous place.
- D. All firearms shall be secured prior to entering the processing and temporary detention area. In an emergency where a detainee has armed themselves with a weapon, an officer may enter the processing and temporary detention area with their firearm so that all aspects of the force continuum are available.
- E. Officers are allowed to enter the processing and temporary detention areas with all department approved less lethal weapons.
- F. Whenever an employee enters an occupied detention room, an officer must be assigned to guard the open door. The guard on the door shall have keys to the detention room door.
- G. All sworn officers and reserve officers shall have electronic key card access to the processing and temporary detention area. Civilian personnel with needed access for public fingerprinting duties shall also be

granted access but shall only be allowed in the area when no detainees are present.

- H. The manual keys to the detention rooms, the emergency exit, storage areas, and the facility control panel shall be stored in the top left drawer of the booking desk. The manual keys shall not be removed from the processing and temporary detention area at any time. Duplicate emergency keys to the detention rooms and the facility control panel shall be stored on the keyboard inside the firing range.
- I. All processing and temporary detention area doors leading out of the facility, processing and temporary detention area storage room doors and processing and temporary detention room doors, including meal and viewing window doors, shall be closed and secured at all times. When there is a need for segregation of detainees by sight and sound, the hallway door leading to the detention rooms shall be closed but not secured. Based on the need for segregation while booking, the door to the identification room may be open or closed. The door to the booking room shall remain open at all times.
- J. Officer shall be required to do a security inspection, including a search for weapons and contraband, prior to and immediately following the use of a detention room. This includes holding and booking detention rooms. If any deficiencies, contraband or weapons are located, the shift supervisor shall be contacted immediately, and an alternative room or area shall be used until the issues are resolved.
- K. No meals will be served within the processing and temporary detention area.
- L. Employees in the processing and temporary detention area should utilize a portable radio or the processing and temporary detention area base radio unit as a means to contact WestCom communications center or other employees in the event of an emergency.

VI. Procedure: Escape and Threats to the Facility

- A. In the event a detainee escapes from the processing and temporary detention area the following procedures will be followed:
 - 1. The officer discovering the escape shall immediately notify communications of the escape and provide at a minimum the following information:
 - a. If known, the detainee's last known location or direction of travel.
 - b. A complete physical and clothing description.
 - c. If the detainee is armed.
 - d. The charges for which the person was being detained and whether the detainee is a danger to the public, other officers, or themselves.
 - 2. The officer shall also immediately notify their supervisor of the escape.
 - 3. As soon as possible, communications shall notify surrounding agencies to inform them of the escape, as well as coordinate with supervisor requests for any assistance that may be needed.
 - 4. A supervisor shall assume control of the incident and has the responsibility for coordinating the search efforts, and if necessary,

requesting any additional personnel or assistance from outside agencies.

5. As soon as practical, the supervisor shall notify the patrol division commander. If the subject was being detained by a division other than Patrol, the commander of that division shall be notified as soon as practical. The commander of the division that had custody of the detainee shall notify the chief of police as soon as practical.
 6. The officer who had detained the subject shall be responsible for completing an offense report detailing the escape, including a chronicle of the events leading up to the escape, as well as other pertinent information regarding the detainee that the reporting officer believes to be relevant.
- B.** The division commander of the officer reporting the escape shall review the incident and the subsequent response. Documentation shall be submitted to the chief of police detailing any needed areas of improvement and/or failure to follow proper procedure that contributed to the escape.
- C.** All incidents that threaten the facility or any person therein require that a report be submitted through the chain of command to the chief of police. Examples of incidents include, but are not limited to:
1. Deaths.
 2. Suicides or attempted suicides.
 3. Use of force.
 4. Escapes or attempts.
 5. Fire.
 6. Occurrences of infection or exposure to infectious disease.
 7. Assaults, including sexual assault.
 8. Injuries occurring within the facility.
 9. Hostage situation.
 10. Discovery of weapons or contraband.

VII. Procedure: General

- A.** No person will be confined or released from the processing and temporary detention area without appropriate process or order from the court.
- B.** Combative or uncooperative detainees shall be transported directly to the Polk or Dallas County jail and shall not be processed at the Urbandale Police Department.
- C.** All employees shall ensure detainees are not subject to discriminatory treatment based upon race, religion, nationality, disability, sex, or age. Discrimination on the basis of a disability is prohibited in the provision of services. Facility services shall be available on an equitable basis to both males and females.
- D.** Reasonable accommodations, with concern for safety and security, shall be provided for detainees with disabilities.
- E.** At the earliest possible convenience, all detainees brought to the processing and temporary detention area shall be brought before the court having jurisdiction over the matter, released on a citation, or transferred to an appropriate holding facility.

- F.** As persons are only being temporarily detained for processing, no bond will be accepted at the Urbandale Police Department. Detainees seeking to post bond shall be allowed to do so upon transfer to a holding facility or county jail.
- G.** A detainee shall have reasonable access to a telephone. No detainee's telephone conversations shall be recorded or monitored while in the processing and temporary detention area. All phone calls made and received by the detainee while in the processing and temporary detention area shall be logged including the date, time and person contacted.
- H.** No person working in the processing and temporary detention area shall transact any business with any detainee, nor shall any person working in the processing and temporary detention area arrange through another party any business transaction with a detainee. Employees shall abide by the department's code of ethics as established in Chapter 1 section 1.1.1 of the Operations Manual. This prohibits employees from using their official positions to secure privileges for themselves or others and prohibits employees from engaging in activities that constitute a conflict of interest.
- I.** Except in an emergency, only one detainee shall be placed in a detention room at any given time.
- J.** If a group of individuals are arrested in such a number they would exceed the capacity of the processing and temporary detention area, alternative facilities such as Polk and Dallas County jails. The following procedures will be utilized:

 - 1.** The supervisor in charge will contact alternate facilities to gain approval for acceptance of the detainees and if needed, help in transporting.
 - 2.** The supervisor shall evaluate the situation to determine if additional personnel and/or additional transport vehicles are needed. If larger capacity transport vehicles are needed, a request will be made to the appropriate agencies to aid in transport.
 - 3.** Adequate manpower shall be acquired to ensure an efficient, effective, and safe processing of all detainees.
 - 4.** Notification shall be made to the division commander(s) of the officer(s) effecting the arrests as well as notification to the chief of police.
 - 5.** If arrested by officers from the Urbandale Police Department, the officer(s) making the arrest(s) shall be responsible for processing but may gain assistance from other agencies in booking/identification procedures.
- K.** When a detainee is received from an outside agency, positive identification shall be made of the person presenting the detainee. The official's name and/or agency as well as how the officer verified the authority to make the commitment shall be recorded by the accepting officer in a supplemental report or a computer aided dispatch entry. After the presenter is identified, the officer will verify the official's authority to

make the commitment. Identification shall be verified in at least one of the following ways:

1. The outside agency official is known to the officer.
 2. The outside agency official is in full uniform and/or is operating a fully marked police vehicle from a known police agency.
 3. The accepting officer requests official identification from the presenter.
 4. If identification is still an issue, the accepting officer will contact their supervisor for assistance and approval.
- L. During times when there is no means of immediate access to court, a person believed to be mentally ill that is arrested on a simple misdemeanor and due to that illness is likely to physically injure themselves or others, shall not be processed at the Urbandale Police Department and may be admitted to another holding facility only after the arresting officer has demonstrated a reasonable effort to comply with the emergency hospitalization procedure as provided in Iowa Code section 229.22.
- M. Juveniles shall only be detained in the processing and temporary detention area pursuant to Iowa Code 232.22.
- N. Annually, the support services division commander or designee shall complete an administrative review of the processing and temporary detention areas inspections, policies, and procedures ensuring the facility is being utilized as intended and is adequate for the department's needs.

VIII. Procedure: Detainee Records

- A. Employees are required to document the identity of all detainees brought into the temporary detention area including date, time in, and time out of the facility.
- B. The security and privacy of criminal records and individual criminal histories shall be governed by chapter 692 of the Code of Iowa and by Title 28 of the Code of Federal regulations.
- C. All records pertaining to detainees, such as arrest reports, records, etc., shall be maintained in such a manner as to safeguard them from unauthorized disclosure.
- D. If a detainee will require medical care during the brief time they are processed, they shall not be processed at the Urbandale Police Department. Detainees needing medical care shall be transported to a medical facility if appropriate to their needs or directly to the Polk or Dallas County Jail. Jail staff shall be informed of the medical care needed by the detainee.
- E. All records of a detention by the Urbandale Police Department shall be maintained by the support services division. The records are located in a locked and controlled environment not accessible to the public or unauthorized persons.
- F. Upon a detainee's release or transfer, all records pertaining to the detainee shall be forwarded to the support services division. Any release of information or requests for information shall be handled in accordance

with the Freedom of Information Act and applicable Department policy as stated in Chapter 9 Section 82 of the Operations Manual.

IX. Procedure: Detainee Property

- A.** Officers shall be responsible for the safe handling and security of any property removed from a person during detention even if that detention is temporary.
- B.** All detainees brought to the processing and temporary detention area shall have their property removed and inventoried. The removal and inventory of a detainee's property shall be conducted prior to placing a detainee in any detention room. The following procedures shall be followed when conducting the removal and inventory:
 - 1.** All property shall be removed from a detainee prior to being placed in a detention room. Property shall be all items except clothing. Clothing shall include a top, a bottom, undergarments, shoes, socks, and belt. If an emergency situation occurs and a detainee must be placed in a detention room prior to removal of their property, the detainee shall be continuously visually monitored until the detainee can be safely removed from the detention room and their property removed.
 - 2.** A search, by means of a pat down/frisk, of all detainees shall be conducted prior to a detainee being placed in a detention room in order to ensure removal all property items.
 - 3.** A pat down/frisk shall be conducted by an employee of the same gender. A pat down/frisk by an employee of the opposite gender may be completed when exigent circumstances warrant such action. A pat/down search by a person of the opposite gender must be documented in the CIR or a supplemental report including details as to exigency that necessitated the action.
 - 4.** Strip searches shall only be conducted in compliance to policy and procedure as stated in chapter 1 section 1.2.8 of the Operations Manual.
 - 5.** It may be necessary to remove the detainee's clothing for safety or other reasons. Refer to the detainee processing section of this policy for procedures to be utilized when removing a detainee's clothing.
- C.** A detainee's property shall be inventoried on a detainee personal property log. Any items that will be seized as evidence shall be listed on a property sheet rather than the detainee personal property log. Inventory of personal property shall be clearly captured on body camera or facility video recording. A second officer may also be used to verify the inventoried property on the detainee personal property log.
- D.** After inventory, the personal property from the detainee shall be sealed in a clear property bag marked with the detainee's name and placed in a secure location. The bag shall remain sealed in the secure location until returned to the detainee upon release or transferred to the custody to another agency. Any detainee property that is too large to be sealed in a property bag shall be placed in a tub and secured in the storage room in

the processing and temporary detention area. The tub shall clearly identify whose items are contained therein.

- E. If a detainee has personal property items in their possession the arresting officer shall complete a detainee personal property log listing the items. Inventory of the property shall occur in plain view of the officer's body worn camera or the holding facility/jail camera system. Upon transfer of custody to the jail or holding facility, release to another law enforcement official, or release of the detainee in lieu of continued custody, one of the following procedures shall be completed:
 - 1. The official accepting the transfer of custody shall sign the personal property log accepting the items. The accepting official should verify all property listed on the inventory sheet is complete and accurate.
 - 2. When released in lieu of continued custody or upon transfer to another facility or law enforcement official, the detainee shall sign for the return of their personal property. All property listed on the personal property log should be verified as complete and accurate by the detainee prior to release.
 - 3. If a detainee is uncooperative, incapacitated or for other reasons it is unsafe or impractical to have the detainee sign for their property, a second officer shall verify the detainee's property prior to transfer of custody. Officers shall indicate on the personal property log the reason for not obtaining the detainee's signature.

X. Procedure: Detainee Processing

- A. Officers shall complete an arrest report on all subjects brought to the processing a temporary detention area. The arrest report shall contain identifying and arrest information to include the following:
 - 1. Arresting/processing officer
 - 2. Reason for the detainment
 - 3. Date of the detainment
 - 4. Time in and time out of the processing and temporary detention area.
- B. Males and females, adults and juveniles may be in the processing and temporary detention area at the same time for booking/identification only and must comply with the following restrictions:
 - 1. Immediately after the identification/booking process, either the male or female detainee will be transferred to another facility or released.
 - 2. Immediately after the identification/booking process, either the juvenile or the adult detainee will be transferred to another facility or released.
 - 3. Processing and temporary detention rooms and doors shall be utilized to maintain sight and sound separation at all times during the booking/identification process.
 - 4. At no time shall male and female or adult and juvenile detainees be held in the same detention room or in adjacent detention rooms where sight and sound separation cannot be maintained.
 - 5. Male and female or adult and juvenile detainees shall not be outside of their detention room in the detention facility at the same time.

- C. When processing individuals that have identified themselves as transgender or the officer is unable to determine the gender of an individual, the following shall apply:
1. Officers shall inform the individual of their right to express a preference of gender.
 2. Absent exigent circumstances, before performing any level of search of the individual, officers shall inform the individual of their right to request a preference of the gender of the officer that will conduct the search.
 3. The request and response shall be video recorded when possible and documented in the officer's booking report.
 4. If the request is not granted, the reason for not granting the request shall be documented.
 5. Absent exigent circumstances, if the individual has a preference, at least one officer of the gender requested shall conduct the search.
 6. The officers may take into account the reasonableness of any delay created by waiting for another officer.
 7. If the individual does not specify a preference, at least one officer of the individual's gender expression shall conduct the search. Example: A male officer would search an individual stating no gender preference expressing themselves as a male.
 8. When in doubt regarding search of a transgender individual, officer shall consult with a supervisor.
 9. The identified gender or the expressed gender (if failing to identify) shall be the gender utilized and applied to all processing, supervision, privacy, and separation requirements stated in this policy.
- D. If an officer has any information through observation and/or direct questioning of the detainee that indicates they may be suicidal or violent, the detainee will not be processed at the Urbandale Police Department and will be transported directly to the Polk or Dallas County Jail for processing. Officers with knowledge of a substantial risk a detainee intends to commit suicide shall take one or more of the following measures to abate the risk:
1. Continuous face to face contact with the detainee for the duration of their detention.
 2. As soon as practical, transfer of the detainee to another facility for more intensive supervision of the detainee (e.g. hospital, Polk or Dallas County jail).
 3. Removal of all items that may be used to harm themselves including clothing items if necessary.
 4. Referral to the Mobile Crisis Unit for assistance.
- E. Detainee clothing may be removed for the following reasons:
1. Protection of the detainee and/or the officer (e.g. suicidal detainees).
 2. Limit or eliminate exposure to blood borne pathogens.
 3. Evidence in an investigation, e.g. a burglary, sex crimes, homicides, assaults (note: A search warrant, consent, or exigency may be needed to seize clothing as evidence).

- F. Any person who is obviously injured, ill, unconscious, or suspected of having a contagious or communicable disease shall not be processed or detained at the Urbandale Police Department. Officers shall have the subject examined by qualified medical personnel before being admitted to the appropriate holding facility such as the Polk or Dallas County Jail.
- G. All observations and actions related to the detainee's behavior shall be recorded in either the case investigative report (CIR) or in supplemental reports if there is a need for upgrading safety precautions for the detainee.
- H. Prior to release, a detainee shall be positively identified by photo identification, booking information or other means. The means by which identification was made shall be noted in the officer's report and/or a copy of the identification used will be placed in the case file noting the date and time of release.
- I. Releasing detainees that are under the influence of alcohol and/or drugs shall be completed as follows:
 - 1. The individual who is seeking the release of a detainee must sign a WAIVER AND ACCEPTANCE OF RESPONSIBILITY FORM before the detainee may be released.
 - 2. An officer has the authority to deny the immediate release of a subject under the influence of alcohol or drugs when it is not in the best interest of the public, the individual, or the Department. The decision not to release shall be reviewed and approved by a supervisor.

XI. Procedure: Detainee Medications and Medical Care

- A. Medications, prescription or over the counter, shall not be administered by Urbandale Police Department employees. When a detainee needs medication, even if they have the medication in their possession, they shall be transported to a hospital, medical clinic, or holding facility with appropriate medical staff. Hospital/medical clinic staff or medical staff at the appropriate holding facility may administer medications pursuant to a physician's orders. If needed, Urbandale Fire and Rescue personnel may also administer needed medications during an emergency situation.
- B. If a detainee has legally obtained medication in their possession when detained and the detainee requires medical treatment, the medication shall be transported under control of an officer or Urbandale Fire Department personnel to the medical facility or hospital. This will allow administration of the medication by a physician if deemed necessary.
- C. When a subject is detained and is on medication, no action by the officer is necessary if custody of the subject detained will be terminated or transferred to another agency prior to the need for the medication. Any agency accepting a transfer of custody will be made fully aware of the detainee's need of medication at the time of the transfer.
- D. Any detainee in need of medical assistance shall be transported to Broadlawns Medical Facility in Des Moines. If Broadlawns is unable to provide the needed care, other medical facilities may be utilized. Any requests to utilize a facility other than Broadlawns shall be approved by a supervisor. Transportation to the facility shall be provided as stated in

Chapter 8 Section 70.1.1 of the Operations Manual. If the detainee is transported to Broadlawns, their current condition, including any known medical history, shall be given to the hospital.

XII. Procedure: Supervision of Detainees

- A.** Both adult and juvenile detainees shall be constantly supervised at all times during their detention through face-to-face observation or officer presence. Officers shall remain in the processing and temporary detention area except as noted in this policy. If an officer is unable to maintain face to face observation with the detainee for the duration of their processing, the detainee must be placed in a detention room, and visual checks shall be completed at a minimum of once every 15 minutes. All checks shall be documented on a detainee observation log. If the detainee is under the influence of drugs or alcohol or exhibits any other unusual behavior characteristics, they shall be monitored with constant face to face observation. If the detainee is under constant face to face observation while being detained, the detainee observation log is not required.
- B.** Use of force shall be restricted to instances of justifiable self-protection, the protection of others, protection of property, or the prevention of escape. Use of force shall follow the policy and procedures outlined in Chapter 1 Section 4.1.1(Use of Force) of the Operations Manual.
- C.** Detainees shall have the same right to file a complaint on employees of the Department as any other citizen. The complaint shall be addressed as stated in Chapter 3 section 26.3.1 (Complaint Procedure) of the Operations Manual.
- D.** Deprivation of clothing or facility blanket shall not be used as discipline or punishment. These items may be taken or withheld from any detainee who the employee reasonably believes would destroy such items or use them as weapons, for self-injury, to aid in escape, or interfere with the normal operation of the facility.
- E.** If a detainee is being processed during a shift change, the responsibility for the detainee shall remain with the arresting or designated processing officer unless explicitly transferred to another officer after gaining supervisor approval. Any transfer of responsibility for a detainee shall be documented.
- F.** There shall be two officers or an officer and a reserve officer who are trained and qualified to assist in the processing and temporary detention area present during a detention unless the detainee is secured in a detention room. In order to conduct searches and maintain the privacy rights of the detainee, one employee shall be the same gender as the detainee when staffing allows.
- G.** Monitoring of activity in the processing and temporary detention area by audio and video equipment shall occur through use of cameras and microphones in the following locations:
 - 1. Video in the sally port.
 - 2. Audio and video in the North/South and East/ West hallways.

3. Audio and video in the booking room and identification room.
- H. No video monitoring shall occur in any detention room. Audio monitoring of the detention rooms is established through use of microphones in the hallways and the booking room.
- I. When a visual check is being conducted on a detainee of the opposite gender, notice shall be given to the detainee prior to the check to maintain the privacy of the detainee.
- J. All detainees have the right to counsel and the right to meet with counsel in a private setting. The processing and temporary detention room #8 visitation room shall be utilized for detainee meetings with their legal counsel. The detainee's conversation shall not be monitored or recorded when meeting with legal counsel.
- K. Visitors for detainees shall be restricted to legal counsel. Exceptions may be allowed by the supervisor on duty based on the situation. Visitations shall be held in the processing and temporary detention area room #8 visitation room. The date, beginning and ending time, and the person visited shall be recorded. Under normal circumstances, the detainee shall have no physical contact with visitors; however, at the request of an attorney, physical contact may be allowed with a detainee's attorney. If an attorney requests to meet with their client without a protective barrier, the following procedure shall be used:
 1. Physical contact visitation shall only be allowed for the detainee and their attorney and only when requested by the detainee or the attorney.
 2. Physical contact visitation shall be held in room #9 of the processing and temporary detention area. No audio or video monitoring of this room shall occur during the meeting.
 3. All attorneys utilizing physical contact with a detainee shall be thoroughly searched and shall surrender all personal property prior to entry into the processing and temporary detention area. All personal property surrendered shall be documented on a personal property log. The attorney shall be allowed to use a pen and paper supplied by the department during a physical contact visitation. Any other items requested by the attorney to be used in the physical contact visitation room shall be approved by the officer.
 4. Under normal circumstances attorneys shall not be subject to a pat down search. If an officer believes a pat down search is needed, they shall gain supervisor approval prior to conducting the pat down search. The pat down search shall be conducted by an employee of the same gender as the attorney.
 5. When safety of an employee, the attorney, or the detainee may be in jeopardy, physical contact visitation shall not be allowed. An officer shall make this determination, and the reasoning shall be articulated in their report.
 6. No restraints shall be used on the detainee in the physical visitation room. If it is unsafe to have the detainee without restraints, the physical contact room shall not be utilized.

7. Prior to returning to any other area of the processing and temporary detention area at the conclusion of a physical contact visitation, the detainee shall be thoroughly searched.
- L.** When under control of the Investigation Division, a supervisor may allow for legal counsel or other visits with detainees in the interview rooms located in the Investigation Division based on the needs of an investigation. If allowed to meet with their attorney, the conversation shall not be audio recorded; however, the detainee shall be under constant supervision while outside of the processing and temporary detention area. The detainee shall be searched upon returning from the interview rooms outside of the processing and temporary detention area.
- M.** Except during entry and exit from the facility, restraint devices to include handcuffs shall be used within the processing and detention area only when a detainee is a threat to self or others or jeopardizes processing and temporary detention area security. Once the determination is made a detainee must be placed or remain in restraining devices within the facility, they shall immediately be transferred to the Polk or Dallas County Jail and will no longer be processed at the Urbandale Police Department. At no time will any type of restraint be utilized to secure a detainee to a fixed or immovable object.
- N.** The processing and temporary detention area shall not be used by outside agencies.

Chapter 8: Detainee and Court Related Activities
Section 74: Legal Process
Subsection 1: Criminal Process



Policy/Procedure #: 1

Title: Legal Process and Arrest Warrants

CALEA Reference#: 74.1.1, 74.1.2, 74.1.3, 74.2.1

I. Policy: Legal Process and Arrest Warrants

A policy is established to control and record all civil and criminal legal process and arrest warrants handled by the Urbandale Police Department.

II. Procedure: Legal Process

- A.** All legal process documents, civil and criminal, accepted by the Urbandale Police Department and/or received in the mail addressed to the Urbandale Police Department will be processed by the Support Services Division. Mailed documents addressed to a specific employee are the sole responsibility of the addressee unless the mail is visibly marked as a subpoena. If the mail is marked as a subpoena, Support Services Division personnel shall open and process the subpoena.
- B.** If the legal process is intended for an employee of the department, the Support Services Division shall be responsible for service or attempted service. The Support Services Division shall also be responsible for service of all legal process intended for reserve officers. Service shall be completed in the following manner:
- 1.** A copy of the legal process shall be placed in the employee's departmental mailbox
 - 2.** An email containing a copy of the legal process shall be sent to the employee's departmental email account.
 - 3.** The work schedule for the employee(s) listed on the legal process shall be checked to ensure they will return to work prior to the date listed. If the employee will not be back to work prior to the date listed, contact shall be made with the issuing authority to inform them service cannot be completed.
 - 4.** If the legal process is for the employee's first day back to work, contact shall be made with the employee by phone to inform them of the legal

process. If unable to make contact with the employee, the legal process shall not be considered served and the issuing authority shall be notified.

5. A legal process tracking sheet shall be completed and retained as prescribed below.
- C. If the legal process is intended for a person not employed by the department and who lives or works within the city of Urbandale, the Patrol Division shall be responsible for service. If the person lives outside the city of Urbandale and does not work within the city of Urbandale, the Investigation Division shall be responsible for service.
- D. The following information shall be recorded for all legal process documents on a legal process tracking sheet which contains the following:
 1. Date and time received.
 2. Type of legal process, civil or criminal.
 3. Nature of document.
 4. Source of document.
 5. Name of plaintiff/complainant or name of defendant/respondent.
 6. Name of division or officer assigned for service.
 7. Date of assignment.
 8. Case number, citation number or court docket number.
 9. Date service due, if any.
 10. Employee and/or witness the document is directed to.
 11. Name of the person on whom legal process was served/executed.
 12. Date and time service was executed or attempted.
 13. Name of person attempting or executing service.
 14. Method of service or reason for non-service.
 15. Address of service/attempt.
 16. Any notes concerning the attempt of service.
- E. If the legal process is a subpoena from the city attorney listing multiple employees on one document, a single tracking sheet may be utilized breaking down appropriate fields by employee name.
- F. Once the legal process has been served, the Support Services Division shall store the tracking sheet and the legal process in Laserfiche.
- G. Upon successful delivery/execution of a legal process document, any return of service or other attachments shall be completed by the employee and returned to the Support Services Division. If necessary, the Support Services Division shall forward the completed documents to the issuing authority.
- H. When the legal process is unable to be served, the following procedures shall be followed:
 1. The reason for non-service shall be noted on the tracking sheet and approved by a supervisor.

2. The Support Services Division shall be responsible for contacting the issuing authority and informing them of the inability to serve the process.
3. Documentation of contacting the issuing authority and disposition requested by the issuing authority shall be entered in the notes field of the tracking sheet.
4. The Support Services Division shall dispose of the legal process as prescribed by the issuing authority (e.g. destroyed, returned, forwarded).
5. The tracking sheet and a copy of the legal process shall be entered into Laserfiche by the Support Services Division.

III. Procedure: Arrest Warrants

- A. All arrest warrants must have documented supervisory approval prior to submitting an affidavit to the court. Supervisors shall ensure probable cause has been established and the identity of the subject of the arrest warrant has been verified.
- B. All arrest warrants obtained by employees of the Urbandale Police Department that are not able to be served shall be recorded, tracked, and entered by WestCom Emergency Communication Center (WestCom). The file containing the arrest warrants shall be accessible twenty four (24) hours a day to allow timely verification.
- C. Only sworn officers are authorized to serve an arrest warrant. An officer obtaining a warrant for a person they are not able to arrest shall complete the arrest warrant tracking sheet. The arrest warrant tracking sheet along with the original copy of the arrest warrant shall be forwarded to the Support Services Division. Support Services shall enter the warrant in the records management system (RMS). Once entered in RMS, the original warrant and the warrant tracking sheet shall be sent via email or other secure method to WestCom by Support Services Division personnel for filing and entry into the Iowa/NCIC computer system. Copies of the warrant shall be placed in the case file in Laserfiche. The arrest warrant tracking sheet will contain the following information:
 1. Date received.
 2. Name and the date of birth of the defendant.
 3. Criminal charge against the defendant.
 4. Officer name and date of any attempt to serve the warrant.
 5. The source of issuance along with the police case number or warrant number.
- D. If in the officer's discretion, the arrest warrant needs expedited entry in the Iowa/NCIC computer system, the warrant and the tracking sheet may be sent directly to WestCom for entry and filing by the officer. If sent directly to WestCom, the officer shall ensure a copy of the warrant and the tracking sheet is submitted to Support Services for entry in the RMS.

- E.** Arrest warrant entry of Urbandale Police Department warrants in the IOWA/NCIC systems shall be completed by WestCom. The IOWA/NCIC printout(s) will be attached to the arrest warrant and placed into the arrest warrant manual file. WestCom will maintain an arrest warrant log. The arrest warrant log shall contain the following information:
1. Date warrant was received.
 2. Case or warrant number.
 3. Source of the warrant (Polk or Dallas County).
 4. Name and birth date of the defendant.
 5. Date the warrant was entered into either IOWA and/or NCIC.
 6. Date the warrant was cancelled from IOWA and/or NCIC.
 7. Date and reason for cancellation.
- F.** All simple misdemeanor warrants originating from the Urbandale Police Department processed through WestCom shall be entered into the Iowa computerized warrant system. All serious misdemeanor, aggravated misdemeanor and felony warrants shall be entered into the Iowa and NCIC computerized entry system. Before entering a wanted person into the Iowa or the NCIC computerized warrant system it is the responsibility of the officer to determine whether a mileage limitation has been specified by the court issuing the warrant, (i.e., will only transport if the subject is apprehended within 100 miles, or 200 miles). If mileage limitation is established, this information must be included in the miscellaneous field on the computerized entry, as well as on the original warrant.
- G.** Without any notation from the court on pick up radius, simple misdemeanor and traffic related misdemeanor warrants shall be entered with a pick up radius of bordering counties only.
- H.** Extradition limits on serious misdemeanor, aggravated misdemeanor, and felony warrants entered into the Iowa /NCIC system are predicated on approval by the Department and the county attorney's office.
- I.** Once a warrant has been served, cancelled, recalled, etc. a supplemental report shall be written or a copy of the change in status of the warrant shall be forwarded to Support Services Division personnel for placement in the original case file. This shall include a copy of the return of service for the warrant completed by the serving officer.
- J.** All requests to validate arrest warrants will be commensurate with the IOWA/NCIC warrant verification requirements and will also include the viewing of the original arrest warrant.
- K.** All incoming information from other jurisdictions concerning Urbandale Police Department arrest warrants will be recorded in the "officer notes" section on the arrest warrant tracking sheet for that particular arrest warrant by the officer/dispatcher receiving such information.
- L.** Upon the execution of an arrest warrant by a police officer, WestCom shall be notified to cancel the warrant from the IOWA/NCIC computerized entry

system. The original warrant is to be removed from the manual arrest warrant file.

- M.** The original arrest warrant, the arrest warrant tracking sheet and the computer printout reflecting the cancellation of the warrant from the computerized entry system shall be forwarded to the arresting officer for inclusion in the case. If the defendant is arrested by another jurisdiction, the associated paperwork explaining the defendant's status will be forwarded to the Support Services Division for entry and disposition.

Chapter 8: Detainee and Court Related Activities
Section 74: Legal Process
Subsection 3: Criminal Process



Policy/Procedure #: 1
Title: Execution of Criminal Process
CALEA Reference#: 74.3.1, 74.3.2

I. POLICY: Execution of Criminal Process

The Urbandale Police Department shall establish a policy to govern the execution of all criminal process to include arrest and search warrants. The policy shall address how a warrant is to be served to ensure the safety of the suspect(s) and the officers involved.

II. PROCEDURE: Obtaining and executing arrest warrants

- A.** All arrest warrants shall be served by sworn officers authorized by law.
- B.** All arrest warrants must have documented supervisory approval prior to submitting an affidavit to the court. Supervisors shall ensure probable cause has been established and the identity of the subject of the arrest warrant has been verified.
- C.** All arrest warrants shall be obtained by a sworn officer submitting an affidavit to the appropriate prosecuting attorney with jurisdiction on the matter for review and approval. Once approved by the prosecuting attorney, the arrest warrant shall be presented to a judge with jurisdiction on the matter for review, approval, and issuance. Either the prosecuting attorney or the judge may deny the issuance of an arrest warrant.
- D.** All non-uniformed personnel serving an arrest warrant shall wear a distinctive article of clothing and/or a police badge that clearly identifies them as police officers. When practical, an arrest team shall include a uniformed officer.
- E.** When possible, the department shall attempt to serve a warrant when it is received. When officers are unable to serve an arrest warrant, it shall be processed according to the procedures in Chapter 8 Section 74.1.1 of the Operations Manual.
- F.** Effort shall be made to serve warrants for persons known to be violent or potentially dangerous as soon as possible.

- G.** Officers serving an arrest warrant shall verify the warrant is valid prior to service.
- H.** The use of the Suburban Emergency Response Team (S.E.R.T.) to serve an arrest warrant shall follow the procedure established in Chapter 5 Section 46.2.2 of the Operations Manual.
- I.** Any attempted arrest warrant service not utilizing S.E.R.T. shall utilize a minimum of two (2) officers.
- J.** When an officer is attempting service of an arrest warrant they shall do the following:
 - 1.** Notify WestCom Emergency Communications Center or the emergency communications center of the jurisdiction in which they are attempting service.
 - 2.** When outside of Urbandale, officers should request the presence of an officer from the jurisdiction in which they are attempting service.
 - 3.** When an arrest is made, the officers are to process the defendant according to departmental policy and in compliance with the Code of Iowa.
 - 4.** The defendant shall be transported to the Polk or Dallas County jail unless the subject is in need of medical treatment. If needing medical treatment, officers shall request emergency medical personnel respond or if a minor issue, transport the subject to a medical facility.
- K.** If there is an arrest warrant for a person and the officer has reasonable cause to believe a person whom the officer is authorized to arrest is present on any private premises the officer may, upon identifying themselves, demand they be admitted to such premises for the purpose of making the arrest. If such demand is not promptly complied with, the officer may thereupon enter such premises to make the arrest using such force as is reasonably necessary. Reasonable cause includes but is not limited to:
 - 1.** The officer's visual sighting of a wanted person entering or inside a structure.
 - 2.** The officer having reliable information of a wanted person's location.
- L.** Unless exigent circumstances exist, an officer shall gain supervisor approval prior to making a forceful entry to serve an arrest warrant.
- M.** Unless federally deputized, Urbandale police officers shall have no official authority to effect and arrest outside of the State of Iowa.
- N.** When an arrest on an Urbandale warrant is made outside of the state of Iowa, the patrol supervisor working shall be notified. The supervisor from patrol shall be responsible for notifying a supervisor from the Investigation Division. If occurring overnight, the notification can be made in the morning during regular hours unless exigent circumstances require immediate notification.
- O.** The Investigation Division shall make a request to the appropriate county attorney to assist in the extradition of the wanted individual from the applicable jurisdiction.

- P. Once extradition is approved, the Investigation Division shall coordinate transportation arrangements for the wanted person. The Investigation Division shall also be responsible for filing any needed documentation with the court for reimbursement of extradition costs.

III. PROCEDURE: Search Warrants (General)

- A. All search warrants shall be served by sworn officers authorized by law.
- B. All search warrants must have documented supervisory approval prior to submitting an affidavit to the court. Supervisors shall ensure probable cause has been established and the person, place or object to be searched has been properly verified.
- C. All search warrants shall be obtained by a sworn officer submitting an affidavit to the appropriate prosecuting attorney with jurisdiction on the matter for review and approval. Once approved by the prosecuting attorney, the search warrant shall be presented to a judge with jurisdiction on the matter for review, approval, and issuance. Either the prosecuting attorney or the judge may deny the issuance of a search warrant.
- D. Search warrants shall be served with the following goals in mind:
 - 1. Accomplishment of a thorough and legal search.
 - 2. Observation of the constitutional rights of person(s) the warrant is being served upon.
 - 3. Minimization of the level of intrusion experienced by those who are having their premises searched while still accomplishing a thorough search.
 - 4. Providing for the highest degree of safety for all persons concerned.
 - 5. Establishing a detailed record of the entire search warrant execution process.
- E. All search warrants shall have a case officer designated. The case officer shall be the most knowledgeable about the case and/or responsible for the investigation. If the case officer is not present during the service of the search warrant, at least one member of the search warrant team shall have direct knowledge of the investigation and location. The officer with direct knowledge of the investigation and location should have been to the location previously or have conducted surveillance prior to the service of the warrant. The investigation and location information shall be verified by a supervisor prior to service to ensure the accuracy of the warrant and intended target.
- F. All non-uniformed personnel serving a search warrant shall wear a distinctive article of clothing and/or a police badge that clearly identifies them as police officers. When practical, the team should include a uniformed officer.
- G. At a minimum, all officers serving a search warrant shall wear body armor until the site has been secured. This requirement may be waived by a supervisor if they can articulate the reason to not wear body armor and still maintain the safety of all personnel.

H. A search warrant shall be executed as soon as practicable within the expectations of the law. Circumstances that may necessitate a delay executing include but are not limited to:

1. Coordination with searches that may be taking place elsewhere.
2. The probability of significant resistance.
3. Informant protection.
4. The presence of certain suspects.
5. The presence of children or uninvolved persons.

IV. PROCEDURE: No Knock warrants:

- A. Search or arrest warrants that do not require officers to knock and announce their presence shall only be utilized in very specific high-risk situations where there is sufficient information indicating officers knocking and announcing their presence will be placed in immediate danger. Search warrants not requiring officers to knock and announce their presence must receive specific prosecuting attorney and judicial approval. The ability to serve the warrant without knocking and announcing must be clearly delineated in the warrant.
- B. Search or arrest warrant requests submitted to a prosecuting attorney or judge requesting a “no knock” provision must first be approved by a division commander or designee.
- C. All “no knock” warrants shall meet all of the requirements of a search or arrest warrant as established in this policy and shall be executed by the Suburban Emergency Response Team (SERT) unless the area to be searched has already been secured by law enforcement.

V. PROCEDURE: Search warrant operations plans

- A. Prior to execution of a search warrant, the case officer shall complete an operation plan. The operation plan shall include information gained from the planning stage of the search warrant execution.
- B. The use of S.E.R.T. to serve a search warrant shall follow the procedure established in Chapter 5 Section 46.2.2 of the Operations Manual.
- C. The planning stage of the search warrant execution is designed to gather as much information about the location to be searched, its surroundings, and the individuals involved as possible. This information is essential in determining the type of entry that will be made, the number of officers required, and the types of armament and equipment necessary. The case officer, with assistance from the supervisor, may include the following information gained during the planning stage to establish their operation plan:
 1. Interior diagrams of the search site.
 2. Photographs or video of the search site and surrounding area.
 3. Pedestrian and vehicular traffic in the immediate area.
 4. Photographs and criminal history checks on all known suspects and all other occupants of the search site. Consideration shall be given to caring for children, the elderly, or disabled who may be found on site.
 5. Identification of the best route for approaching the location.

6. Any known fortifications to doors and windows and the possibility of weapons, vicious animals, etc.
- D. Exceptions to the operations plan requirement may be made by a supervisor based on the place to be searched. Reasons for not completing an operation plan include but are not limited to:
 1. The place to be searched has already been secured by law enforcement personnel.
 2. The place to be searched does not contain or is unable to contain any persons.
 3. Any other reason deemed appropriate by the supervisor in charge of the operation.
- E. Prior to executing a search warrant, the case officer or the supervisor shall conduct a briefing of the search warrant execution, utilizing the operation plan if applicable, and shall include all involved personnel. The briefing will include the actual order of events and procedures the team will follow. Photographs, maps, charts and diagrams may be used if appropriate. Additionally, the case officer or designee shall ensure proper equipment is available to complete the search warrant.
- F. Part of the search warrant briefing shall include which member of the search warrant team will knock and announce in a loud and clear voice "POLICE, SEARCH WARRANT." This command will be repeated until a response is received or a reasonable amount of time has passed. If there is no response within a reasonable amount of time, if, how, and by whom forcible entry shall be made to execute the search warrant will be predetermined.
- G. Prior to departure for the search site, the case officer shall ensure the warrant is accurate, valid and complete and all areas and persons to be searched are adequately described.

VI. PROCEDURE: Search Warrant Execution

- A. The case officer shall ensure the entire search warrant execution process is documented including the need for photographs or video. If approval has been obtained and a "no knock" search or arrest warrant is executed, the details of the "non knock" execution shall be documented within the case report.
- B. WestCom or the appropriate emergency communications center of the jurisdiction in which the search warrant is being served shall be notified prior to and at the conclusion of the execution of the search warrant. Notification should include the location, time and personnel involved in the warrant.
- C. At the conclusion of the warrant, the case officer or designee shall be responsible for removing all equipment used and any evidence seized.
- D. Once entry is gained in the structure, a security sweep to ensure officer safety shall be conducted.
- E. After the site is secured, the warrant will be read to the person having custody of the premises. A copy of the warrant will be furnished to this

person. If no one is present, a copy of the warrant, accompanied by a list of items seized, will be left in a conspicuous place on the site.

- F.** As the search commences, the person having been previously designated will be responsible for receiving, preserving, and documenting all items seized until possession is transferred to the case officer or the property and evidence officer.
- G.** Should damage occur during the entry that would prevent the securing of the property that will be left vacant, arrangements shall be made to guard the premises until it can be secured.
- H.** If damage occurs during the execution of the warrant, it shall be documented in a report detailing the damage and the actions that caused the damage. This report should be accompanied by photos or other visual recordings.

Chapter 9: Auxiliary and Technical Services
Section 81: Communications
Subsection 1: Administration



Policy/Procedure #: 1

Title: Communications

CALEA Reference#: 81.1.2, 81.2.1, 81.2.2, 81.2.3, 81.2.4, 81.2.5, 81.2.6, 81.2.7, 81.2.8

I. Policy: Communications

The City of Urbandale and the Urbandale Police Department have joined with several agencies to form WestCom Emergency Communications (WestCom). WestCom serves as the emergency communications system for the Urbandale Police Department. The Department shall establish policy to address operational procedures with WestCom.

II. Procedure: General

- A.** The Support Services Division shall have primary responsibility and control of communications and communication equipment for the Department.
- B.** The Department's radio operations will be conducted in accordance with the Federal Communication Commission's (FCC) procedures and requirements at all times. WestCom shall remain current on all licensing requirements of the FCC and show proof of licensing upon request. A copy of the FCC's current rules and regulations shall be available to Department personnel through WestCom.
- C.** WestCom shall provide the Urbandale community with twenty four (24) hour toll free voice and TDD telephone access systems for emergency calls for service.
- D.** WestCom shall establish policy for obtaining and recording the following information for each call for service or self-initiated activity:
 - 1. Control number.
 - 2. Date and time of request.
 - 3. When possible, name and address of complainant.
 - 4. Type of incident.
 - 5. Location of incident.
 - 6. Identification of officers assigned as primary and backup.
 - 7. Time of dispatch.
 - 8. Time of arrival.

- 9. Time of officer return of service.
- 10. Disposition or status of reported incident.
- E. WestCom personnel shall be informed of the supervisor or officer in charge and all assigned patrol officers at the beginning of every patrol shift. All officers assigned shall be considered active unless WestCom is informed of a change in status.
- F. The Office of the Chief of Police shall ensure WestCom has an updated roster including telephone contact information for all current Department personnel.
- G. WestCom shall maintain a current plan or data on the following:
 - 1. Maps detailing the Department's service area
 - 2. A written procedure and contact information for procuring emergency and necessary external services for the Department.
 - 3. A tactical dispatching plan.
- H. WestCom shall establish an incident interview technique to be utilized by communications personnel when responding to calls for service. The interview shall determine if the call for service is an emergency or non-emergency. Regardless of the type of call, communications personnel shall inform the caller of the Department's response to include direct department assistance or referral to another agency or service provider.
- I. The Department shall maintain victim and witness assistance and referral information on a 24-hour basis through WestCom and through in person response by police officers.
 - 1. Communication personnel shall make a determination, based upon the scope of the call for service, if the victim or witness needs direct emergency medical service (EMS) and/or physical police response or referral. If either the EMS or police are needed, communications personnel will promptly dispatch appropriate personnel. In cases of a referral, referral lists are maintained at WestCom and agency contact phone numbers shall be kept updated.
 - 2. If physical police response is necessary, the responding officer shall determine whether overt police actions such as written reports, notifications, arrests, or transportation are required or if the need exists for other types of assistance or intervention (e.g. contact with Polk County Victim Services, Rape Crisis Center, Polk County Family Violence Center, domestic abuse services, or the Mobile Crisis Unit).
- J. The Department provides and utilizes alternate methods of communication to ensure effective, efficient and proper communication between employees. Methods of alternate communication include cellular telephones and email.
 - 1. Upon hire, employees are assigned an email account through the City of Urbandale to be used in day-to-day business operations of the Department. Department employees shall adhere to the City of Urbandale email and internet usage policy and procedures.
 - 2. The Chief of Police may assign cellular telephones to employees when a valid mission-related purpose exists. While cellular telephones can

be used in lieu of radios and strict adherence of radio procedures is not mandatory, employees must be professional with their communications. Employees issued a department cellular telephone shall adhere to the City of Urbandale cellular telephone policy and procedures.

III. Procedure: Recordings

- A.** All communications occurring on the two-way radio system and any telephone line answered by WestCom shall be recorded. The recording system shall allow for the immediate play back of the recording while continuing to record any additional communications.
- B.** WestCom shall establish the manner in which the records are securely handled and stored, and the length of time the records are maintained. The procedure for destruction for each record shall also be defined. All applicable federal, state, county, city, and local regulations related to the maintenance of records shall be followed. All recordings shall be maintained for a minimum of ninety (90) days. A division commander may request in writing a specific official recording be maintained for a longer period of time, the request shall identify the time frame to be maintained.
- C.** There are essentially two types of recordings:
 - 1.** WestCom shall make available to the Department two (2) access passes into the Eventide recording system. The Chief of Police shall designate to the WestCom director who has access to the system and will be responsible for monitoring its use. The Department shall have access to all of its assigned radio channels as well as the 9-1-1 phone lines.
 - 2.** Any recording made by the Department shall only be used for internal quality improvement activities. At NO TIME will internal operational recordings be released to anyone outside the Department.
- D.** Recordings shall only be reviewed for official purposes (e.g. procedural review, complaint investigation). When a recording is needed for a complaint investigation that may result in suspension, demotion, or termination, it shall be an official recording as described above.

IV. Procedure: Criminal Justice Information Systems

- A.** All officers and other employees required to access the Iowa and the National Crime Information Center (NCIC) criminal justice information system shall maintain proper certification as required. The Support Services Division shall maintain all needed records to verify employees have met the standards of each system including initial certification, periodic recertification as required, and updating approved user access.
- B.** Criminal justice information systems contain confidential information. All employees shall be responsible for knowing and understanding the rules and regulations that govern the use and distribution of this information and will be held accountable for failure to comply with said rules and regulations.

- C. The Criminal Justice Information Services (CJIS) produces a comprehensive security policy to establish a minimum set of security requirements for access to FBI CJIS systems and information and to protect and safeguard criminal justice information. The Department shall adopt this security policy and shall adhere to the requirements therein.
- D. The Department shall establish the following positions to comply with the CJIS security policy. The positions shall assume all roles and requirements as established in the CJIS security policy.
 - 1. Terminal Agency Coordinator (TAC): The TAC serves as the point-of-contact at the Department for matters relating to CJIS information access. The TAC administers CJIS systems programs within the Department and oversees compliance with CJIS systems policies. The TAC position for the Department shall be the A supervisor within the Support Services Division. The designated supervisor may delegate TAC duties to subordinates but shall retain overall authority and responsibility for compliance to CJIS security policy requirements.
 - 2. Local Agency Security Officer (LASO): Due to the technical nature of the duties of the LASO, the City of Urbandale Information Technology Department (City IT) shall assume this role. The LASO shall have the following responsibilities:
 - a. Identify who is using the State of Iowa Technology Services Bureau approved hardware, software, and firmware and ensure no unauthorized individuals or processes have access to the same.
 - b. Identify and document how the equipment is connected to the state system.
 - c. Ensure personnel security screening procedures are being followed as stated in this policy.
 - d. Ensure the approved and appropriate security measures are in place and working as expected.
 - e. Support policy compliance and ensure the State of Iowa Technology Services Bureau is promptly informed of security incidents.

V. Procedure: Radio Communications

- A. When on duty, all officers shall be assigned a portable two-way radio that allows direct communication with WestCom.
- B. All police owned vehicles utilized for enforcement activity shall be equipped with a mounted two way radio system that allows communication with WestCom. Exceptions may be granted for vehicles assigned to task force officers as they may be operating under a different communication system or the vehicle may be utilized for undercover operations.
- C. Each radio shall have an emergency alarm that when activated will send an alert to WestCom personnel. The emergency alarm shall be activated by an officer when they encounter a dangerous situation in which they need immediate backup and are unable to communicate due to the situation. When an emergency alarm is activated, WestCom shall attempt

to quickly check the status of the officer to confirm their location and check for accidental activation. If an emergency is confirmed or no response is received, WestCom shall immediately dispatch a supervisor and one additional officer to assist. An emergency alarm activated by an officer shall be handled with the highest priority.

- D.** Each officer shall be assigned a radio identification number to be utilized during all radio communications.
- E.** When on duty, patrol officers shall primarily utilize the two way radio system to inform WestCom personnel of their status. This allows WestCom and other officers to remain cognizant of the officer's activity, location, and current status. Officers may also utilize a mobile data terminal or a cell phone to inform WestCom and other officers of their status. Officers outside of patrol may utilize the two way radio system when appropriate to inform WestCom of their actions. All officers shall be required to notify communications personnel of any type of enforcement activity and shall have a two way radio system immediately accessible when taking action. Officers working covert and undercover assignments are exempt from this requirement.
- F.** The Department uses plain language as their communication protocol. All transmission will be courteous and professional in nature. At no time shall profanity be used on the radio.
- G.** Employees shall be reminded all radio communications and mobile data information can become public record according to Iowa Code.
- H.** Officers shall keep WestCom advised of their status following their arrival at calls of unknown or possibly dangerous circumstances.
- I.** Only pertinent or emergency information shall be transmitted on the two-way radio system. Officers shall follow procedures developed by WestCom for the use of radio channels for specific purposes. Secondary channels shall be designated as information channels in efforts to keep the main radio channels open for priority or emergency communications.
- J.** Officers shall keep their portable radios on when away from vehicle or station based radios unless the situation warrants otherwise (e.g. bomb threat, officer safety, etc.).
- K.** Officers shall keep WestCom aware of their status. This shall include but is not limited to the following:
 - 1. Upon initiating police action.
 - 2. On arrival and at completion of an assignment.
 - 3. During lunch periods and breaks.
 - 4. When out of service for any reason.
- L.** Officers and WestCom personnel shall not argue or contest assigned calls.
 - 1. If there is a problem, the involved personnel shall contact their supervisor.
 - 2. When there is an issue that needs corrective action, it shall be handled by the supervisor. Sensitive matters shall be handled over the telephone or in person.

- M. Call assignments may be altered by the supervisor based on information, need, and staffing. Officers not specifically assigned to a call shall refrain from including themselves. If further assistance is needed, WestCom personnel or the supervisor will assign backup units.
- N. Officers shall monitor other agencies radio communications as designated by their supervisor while performing routine patrol duties.
- O. In the event of a major crime or medical emergency, a specific channel shall be restricted to use for that incident. Anytime an officer is responding to a dangerous situation, radio use shall be restricted to emergency communication only. Officers shall notify dispatch when the situation has been resolved so the channel can be cleared for normal use.
- P. Officers shall use the following procedures when stopping a motor vehicle:
 - 1. Upon stopping a vehicle, an officer shall notify WestCom by giving their radio number and advising "traffic." They shall stand by until acknowledged by a dispatcher before giving further information.
 - 2. The officer shall give license number of vehicle, his/her location, vehicle color, year, make, model and number of occupants. WestCom shall run an Iowa /NCIC query of the vehicle after being advised of the license number.
 - 3. After making contact with the occupants of the vehicle, if the officer feels the situation is under control, they shall advise WestCom they are "OK." After an officer gives their status as "OK" the dispatcher will not need to check his/her welfare unless the officer is out for an extended period of time.
- Q. When an officer anticipates being out of radio contact, they must notify WestCom of their location and the reason for leaving. WestCom must be able to reach the officer at all times. If radio communication is not possible, the officer may utilize a cellular phone to keep WestCom informed.
- R. Officers and WestCom personnel have access to other agencies via the Iowa Statewide Interoperability Communications System (ISICS), mutual aid, and other radio channels. Use of other channels by officers shall be limited to emergency or urgent communications. Proper radio procedure shall be followed when using other channels.

VI. Procedure: Mobile Computers

- A. The mobile computer supplements the existing WestCom two-way voice radio system. The mobile computer is not intended to replace two-way voice radio communications. The mobile computer is intended to be used for sending and receiving information, making and/or receiving routine inquiries and receiving supplemental information, thus allowing the voice channels to be more available for high priority traffic. The mobile computer may also be used to access the Department's records and computer aided dispatch systems.
- B. Department personnel using the mobile computer shall be aware messages sent on the system may be public records according to Iowa law. Messages shall be restricted to business use. No personal

messages shall be sent. No obscene, improper, or off-color language will be used in the messages. Officers shall not allow unauthorized users to access their mobile computers.

- C. It shall be prohibited to do any of the following actions on the mobile computer:
 - 1. Send messages that may be construed as threatening or intimidating.
 - 2. Unless it is incidental to an investigation or as part of an official inquiry/response or report, send images that contain nudity, or to send images or words of a sexually suggestive nature, even if the recipient has consented or requested such material.
 - 3. Send jokes or comments that tend to disparage a person or group because of race, ethnicity, national origin, religion, gender, sexual orientation, age, or mental or physical disability.
 - 4. Send messages in any other inappropriate manner.
 - 5. Use another employee's computer ID and password without that person's permission and a supervisor's permission.
- D. All usage of the mobile computer to access the IOWA/NCIC systems will be governed by IOWA/NCIC system's rules and regulations.
- E. Any installation of software or modification of existing software on the mobile computer shall adhere to the policy established in Chapter 2 Section 11.4.4 (Computer Software) of the Operations Manual.
- F. All calls for service shall be dispatched by voice and may also be sent by computer. Mobile computers shall be utilized by officers for inquiries, to send administrative messages, to complete needed reports, or to access and update the Department's records and CAD systems.
- G. Officers should perform their own status changes (arrive, busy, available, complete) on their mobile computer. They will continue to use the radio system to alert other officers and supervisors of their change in status.
- H. All officers shall query their own driver license, registration and warrants unless circumstances require a verbal request.
- I. When able, officers shall obtain all incident times and numbers by mobile computer. Officer shall be responsible for entering the trip narrative and disposition.
- J. When the mobile computer system is down, all activity shall revert back to the two-way voice radio system.
- K. Officers shall practice officer safety techniques. Do not allow operation of the mobile computer to reduce situational awareness, especially in cases involving violators or suspects.
- L. Caution shall be exercised when operating the mobile computer when the vehicle is moving. Only when the operation can be done in a safe manner may an officer operate the mobile computer while the vehicle is moving. When operation of the mobile computer requires more than a few key strokes or the touching of the computer screen, the officer shall pull over at a safe location to perform the task.

VII. Procedure: Response to Calls for Service:

- A. One unit will generally be dispatched to handle routine calls for service. The nature of some calls, however, may require additional units for purposes of safety and effectively handling the call. Under most circumstances, two (2) or more units will initially be dispatched in the following instances:
 - 1. Officer calling for help or an activation of an emergency alert.
 - 2. Alarms.
 - 3. Suspicious persons/circumstances.
 - 4. Domestic disturbances.
 - 5. Any call involving a weapon.
 - 6. Crimes in-progress.
 - 7. Any call that poses a risk to the officer.
 - 8. Any call where, in the judgment of a supervisor, additional units are needed.
- B. Supervisors may use their discretion when responding to calls; however, there are circumstances that require the presence of a patrol supervisor for the purpose of assuming command. These incidents shall include but not be limited to:
 - 1. Officer calling for help, assaulted, or an activation of an emergency alert (not including false alerts).
 - 2. Death investigations
 - 3. Natural or man-made disasters.
 - 4. Hostage/barricaded subject.
 - 5. Injured officers.
 - 6. Fatal or potentially fatal accidents.
 - 7. Accidents involving department vehicles or department employees.
 - 8. Incidents where a forced entry is necessary.
 - 9. Vehicle and foot pursuits.
 - 10. Aggravated assault, assault with weapons, severe injuries due to an assault.

VIII. Procedure: Entering information into Iowa NCIC systems

- A. WestCom shall be responsible for entry and removal of all information into the Iowa /NCIC computerized data systems for the Urbandale Police Department.
- B. When meeting Iowa/NCIC system requirements for entry, officers taking a report in which a vehicle, article, gun, or security have been reported stolen shall request WestCom to enter said item. WestCom shall be provided a copy of the incident report (CIR) by the officer to facilitate entry. When an item is entered in the Iowa/NCIC system, officers are required to document the entry in the narrative section of the CIR.
- C. When meeting departmental and Iowa/NCIC system requirements for entry, officers taking a report on a missing person shall be required to immediately forward the information to WestCom for entry of the missing person in the Iowa/NCIC system. The reporting officer or designee shall complete a missing person computer entry request form and forward to WestCom. WestCom personnel shall ensure there is an immediate entry

into the system. A copy of the request form shall be maintained in the main case file. At their earliest convenience, officers shall also provide WestCom with a copy of the CIR on a missing person.

- D.** Refer to Chapter 8 Section 74.1.1 (Legal Process and Arrest Warrants) of the Operations Manual for arrest warrant entry, removal, and documentation procedures.
- E.** When an item or missing person is located and requires removal from the Iowa/NCIC system, the officer responsible for the recovery shall notify WestCom to remove the entry by providing a supplemental report requesting the removal. The officer shall also submit the supplemental report to the main case file. When WestCom is notified by another agency that an item or person has been located, the detective assigned the case shall be notified and be responsible for producing a supplemental report requesting the removal with copies to WestCom and the main case file.
- F.** On a monthly basis, the State of Iowa shall produce a validation report for the Department on all outstanding entries into the Iowa/NCIC system entered for the Urbandale Police Department. The Investigation Division shall be responsible for researching said entries for validation. When it is discovered an item or person is no longer valid for entry in the Iowa/NCIC system, the Investigation Division shall notify WestCom for removal and produce a supplemental report stating it has been removed.

Chapter 9: Auxiliary and Technical Services
Section 82: Central Records
Subsection 1: Administration



Policy/Procedure #: 1

Title: Records Administration

CALEA Reference#: 82.1.1, 82.1.2, 82.1.3, 82.1.4, 82.1.5, 82.1.6

I. Policy: Records Administration

A policy shall establish procedures to govern records maintenance, access, and release. Records administration is a vital function of an effective law enforcement agency. The Department shall develop a records administration system to meet management, operational, and informational needs. The Urbandale Police Department shall conduct all records related functions in accordance with all applicable federal and state law as well as departmental directives.

II. Procedure: Responsibility and Security of Records

- A.** The legal custodian of all police records shall be the Chief of Police. The records function shall be the responsibility of the Support Services Division. Duties associated with this responsibility include supervising records personnel, storage, purging, release, and access to records as directed by the Chief of Police.
- B.** Records include all official reports and documents generated during the course of business including tickets, case files, photographs and other types of files utilized to record police activities.
- C.** Department records shall be secured, retained, disseminated, and purged in accordance with federal and state law as well as Department policy.
- D.** All records captured in any medium by employees of the Department are the property of the Urbandale Police Department and shall remain within the police building, a secure storage facility, or secure computer network unless otherwise approved by the Chief of Police or a division commander for removal or distribution.
- E.** The records area in the police facility shall be secured at all times to prevent unauthorized access. All Department employees with a right and need to access the police records area shall have access 24 hours a day.

- F. Records information shall be accessible to Department personnel as determined by the Support Services Division Commander or the Chief of Police. When able, police records shall be maintained by the records function in electronic format. Only employees with a right and a need to know shall have access to the records. Electronic records shall be accessible to personnel 24 hours a day.
- G. Employees shall only access Department and other law enforcement agency records for official Urbandale Police Department purposes. Accessing Department or other law enforcement agency records for personal use, curiosity or other reasons not related to work assigned at the Urbandale Police Department shall be strictly prohibited and shall result in disciplinary action up to and including termination.
- H. The Department shall comply with all of the provisions of Iowa Code 692 in regard to computerized criminal history access and security.
- I. The City of Urbandale Information Technology Department (City IT) shall perform the following functions to ensure the security of police records:
 - 1. Restrictions to deny unauthorized access shall be placed on the electronic files by utilizing passwords. Passwords to gain access to police records shall be changed on a schedule determined by the City IT and in compliance with CJIS requirements.
 - 2. City IT shall ensure the Department maintains adequate data storage capabilities for all forms of police records.
 - 3. City IT shall ensure the electronic files of the records management system are backed up on a schedule determined by the Department and the city's IT department.
- J. When a record is maintained in paper format. The files shall be maintained in a secure location within the Department or at a secure off-site facility supplied by a document management service.
- K. Records may be shared and reproduced for outside law enforcement agencies assisting with case investigations or review at no cost to the agency.
- L. Records personnel shall perform a weekly audit of the records management system to ensure required reports have been submitted, the case numbering system is correct, and there are no duplication or missing reports. If a discrepancy is found, a Support Services Division supervisor shall be notified. The Support Services Division supervisor shall follow up with the appropriate supervisor or officer to rectify any discrepancies.

III. Procedure: Release of Police Records to the Public

- A. "Public Record" means any record, document, tape or other information stored or preserved in any medium pursuant to Iowa Code 22.1.
- B. Requests to view records are legal in any form including written, electronic, telephone/faxed or verbal requests. The requestor is not required to provide their name or the purpose for the request; however,

the requestor's information may be necessary if records need to be reproduced and provided at a later time to the person making the request or if payment is required in advance. Identification may be requested under limited circumstances when access to the record is restricted such as court orders, autopsy reports, etc.

- C.** Iowa Code 22.8(4) (d) allows a reasonable delay of 20 calendar days to respond to a request for police records. Under normal circumstances, the delay should not exceed 10 business days. This should allow the Department sufficient time to consult with the appropriate attorney's office about the ability or requirement to release the requested records.
- D.** The examination of records is allowed during normal business hours unless the requestor and the lawful custodian agree on a different time. Business hours are Monday – Friday 8:00am to 5:00pm. Every person making the request to examine a record is permitted to do so without charge. This includes taking photographs of the records or making copies if they bring a portable copy machine.
- E.** A supervisor shall not relinquish control of the records. They shall provide a place for examination/copying and shall supervise the review of the records in order to preserve all original documents.
- F.** Records that are confidential shall not be released for inspection or copying. Records protected by Iowa Code for confidentiality purposes include but are not limited to:
 - 1. Intelligence data pursuant to Iowa Code 692.8A.
 - 2. Registered victim information pursuant to Iowa Code 915.
 - 3. Social security numbers (Federal Privacy Act).
 - 4. Identity of a child victim under the age of 12 pursuant to Iowa Code 232.
 - 5. I.D.O.T. accident reports, except immediate facts and circumstances pursuant to Iowa Code 321.271.
 - 6. Presentence investigation reports.
 - 7. Minutes of evidence.
 - 8. Investigative reports/autopsy reports of medical examiner 22.7(41).
 - 9. DCI criminal history information pursuant to Iowa Code 692.8A.
 - 10. Work products of an attorney, particularly the city attorney pursuant to Iowa Code 22.7.
 - 11. Peace officers investigative reports especially when disclosure would plainly and seriously jeopardize an investigation or pose a clear and present danger to the safety of an individual or officer pursuant to Iowa Code 22.7(5).
 - 12. Except for cases alleging a forcible felony, all official juvenile court records in delinquency cases are presumed confidential and are no longer public records. This includes the law enforcement complaint, information pertaining to a child 10 or older who is taken into custody

for a public offense, and all resulting petitions, court orders and pleadings. A delinquency complaint alleging a forcible felony by child 10 or older, or information pertaining to such a child taken into custody on a forcible felony, can be released to media/public by law enforcement.

- G.** All confidential records including criminal history and intelligence data protected by Iowa Code 692 shall remain with the case file; however, these records shall be conspicuously marked or stamped to prevent release under the open records laws.
- H.** When there is a question as to the confidentiality of any record or part therein or if the record involves a juvenile, records personnel shall request a supervisor review the record prior to public release. Supervisors and staff are encouraged to review Iowa Code 22.7 in its entirety to determine confidential issues prior to releasing or permitting inspection of a record. If the supervisor is unsure as to the confidentiality of a record, the City Attorney, a county attorney, or the state attorney general's office shall be consulted prior to release.
- I.** Requests by the public for criminal history data shall be made in writing to the Department of Public Safety and the history may only be released if the person is identified by name and date of birth. The release of the records shall be made to the named individual or an individual's attorney per Iowa Code 692.2.
- J.** Due to anti-stalking laws found in Iowa Code 708.11, the Department shall not provide driver license or vehicle license registration information to the public. If the request is made pursuant to an abandoned vehicle complaint, an officer shall be assigned to investigate the complaint.
- K.** Denial of an open records request must be approved by the Chief of Police, or designee(s).

IV. Procedure: Juvenile Records

- A.** Juvenile records shall be distinguished in the incident report by date of birth, age, and other required information. The records management system shall also track and sort offender information into juvenile or adult records based on the date of birth. The booking information contained in the arrest report shall also require an officer to indicate if the offender is a juvenile or an adult.
- B.** Pursuant to Iowa Code 232.149 the taking of a child into custody under provisions of 232.19 (e.g. runaway) shall not be considered an arrest and as a result the record shall not be considered public.
- C.** Except for cases alleging a forcible felony, all official juvenile court records in delinquency cases are presumed confidential and are no longer public records. This includes the law enforcement complaint, information pertaining to a child 10 or older who is taken into custody for a public offense, and all resulting petitions, court orders and pleadings. A

delinquency complaint alleging a forcible felony by child 10 or older, or information pertaining to such a child taken into custody on a forcible felony, can be released to media/public by law enforcement.

- D. Fingerprints and photographs shall be taken of a juvenile if applicable under Iowa Code 232.148 for a public offense other than a simple misdemeanor as stated in Chapter 5 Section 44.1.1 (Juveniles) of the Operations Manual. These records shall be maintained by the Department of Public Safety and shall not be released to the public by the Urbandale Police Department.
- E. Any juvenile who escapes from detention as stated in Iowa Code 232.22 may have their name released under public record to include the facts surrounding the escape and the offense resulting in the placement of the juvenile.
- F. Juvenile records shall be maintained as stated in the records retention section of this policy regardless if the juvenile has subsequently reached adult age.
- G. Any juvenile record sealed or expunged by the order of the court pursuant to Iowa Code 232.150 shall not be released unless permitted by court order. Any sealed or expunged juvenile record shall be clearly marked as sealed or expunged to prevent disclosure.

V. Procedure: Personnel records for public release

- A. Prior to the release of any personnel records to the public, the Human Resources Department for the City of Urbandale and the City labor attorney shall be consulted. Personnel records that may be available for public release include:
 - 1. Employee compensation.
 - 2. Employee sick leave (including hours and days, but not specific reason for the sick leave).
 - 3. Employee promotion dates and years of service.
 - 4. Employee awards and certificates of accomplishment.
- B. Employee confidential records that may be released at the discretion of the Chief of Police include:
 - 1. Employee job performance records.
 - 2. Limited personal information about employees.
 - 3. Training records supported by the City budget.
- C. All other types of employee records shall be reviewed by the Human Resources Department and the City labor attorney to determine confidentiality and the need for public release.

VI. Procedure: Cost of Public Records

- A. There shall be no cost to reproduce a record for another law enforcement agency involved in the investigation of case related to an Urbandale police record.

- B.** There shall be no cost to reproduce a record for the media unless the record(s) requested will take substantial effort to produce and/or requires a search within historical files or stored documents. At the discretion of a division commander or the Chief of Police, the fee may be waived.
- C.** The following charges shall be assessed for producing records for the public. There shall be no charge for a basic record request that takes less than 30 minutes to produce. If the request takes more than 30 minutes to produce, a basic charge of \$10.00 reflects the 30 minutes of clerical labor hours and includes the first 10 pages. Each additional page beyond the initial 10 pages shall be \$.10 per page. For any request that exceeds thirty (30) minutes of work to retrieve, the agency may charge for actual labor of the person conducting the work and \$.10 per page. The agency will estimate as closely as possible the amount to be charged and the fee will be collected in advance of any record being reproduced. At their discretion, a division commander or the Chief of Police may waive this fee.
- D.** Audio and video reproductions require a lengthier process to reproduce. Per request, the average labor hours involved to reproduce and disseminate a single audio and video file averages thirty (30) minutes. A basic charge of \$14.00 per audio or video item includes material cost of reproduction and thirty (30) minutes labor cost. Items exceeding the basic labor rate of thirty (30) minutes will be pro-rated in fifteen (15) minute intervals. Below is a basic summary of fees to be assessed for producing records for the public:

Incident Reports and local records checks- No charge if taking less than 30 minutes to produce.

Incident Reports and local records checks- \$10.00 for 10 single-sided pages or less if the request takes more than 30 minutes to produce.

Each additional page	\$0.10 per single page
Video Tapes, CD's, DVD's	\$14.00 per reproduction
Audio, CD's	\$14.00 per reproduction
Photograph(s)	\$5.00 per page, 4 photographs per page

Accident reports- \$5.00 per report

VII. Procedure: Records Retention

- A.** All records will be retained according to the current City of Urbandale policy for record retention.
- B.** Audio/video from the recordings not specifically identified as evidence shall be retained on the following schedule:

1. In-car and body worn camera recordings shall be retained as stated in Chapter 5 Section 41.3.8 (In-Car & body Worn Recording System).
2. Police station security camera recordings shall be retained for 90 days.

VIII. Procedure: UCR/NIBRS

- A.** The Department shall submit crime data to be utilized in the National Incident Based Reporting System (NIBRS) program. Statistical data generated by the records management system shall be submitted to the Iowa Department of Public Safety on a monthly basis. The Iowa Department of Public Safety then transmits data to NIBRS.
- B.** Records personnel shall internally audit and correct errors prior to submitting the data to the State of Iowa.
- C.** Audit reports returned from the State Of Iowa on the Department's monthly submissions shall be addressed as soon as practical to correct any reported errors. Corrections shall be automatically submitted during the next data submission.

Chapter 9: Auxiliary and Technical Services
Section 82: Central Records
Subsection 2: Field Reporting and Management



Policy/Procedure #: 1

Title: Reporting and Record Maintenance

CALEA Reference#: 82.2.1, 82.2.2, 82.2.3, 82.2.4, 82.2.5, 82.3.1, 82.3.2, 82.3.3, 82.3.4, 82.3.5, 82.3.6

I. Policy: Reporting Record Maintenance

The Urbandale Police Department shall develop a systematic and thorough reporting procedure for documenting and disseminating incidents of a criminal or public safety nature and any follow up activity completed during the investigation of the incident. The Department shall also maintain complete and accurate records and reports detailing all activities and work products.

II. Procedure: General

- A.** A report shall be generated for every incident occurring within the jurisdiction of the Urbandale Police Department to include:
 - 1. Citizen reports of crime.
 - 2. Citizen complaints.
 - 3. Incidents resulting in an employee being dispatched or assigned.
 - 4. Criminal and noncriminal cases initiated by employees.
 - 5. Incidents involving arrests, citations, or referral to other criminal justice agencies.
- B.** The responding/reporting officer or a supervisor shall determine based on the circumstances if a case number shall be issued to an incident. If a case number is requested, communications personnel shall assign a unique number to the incident. The case number shall begin with the year in which the incident occurred followed by a sequential number unique to the prescribed incident. If based on their investigation the responding/reporting officer does not feel the incident requires a case number, the incident will be given a unique call number in the computer aided dispatch (CAD) system for documentation purposes.
- C.** In some situations it may be necessary to receive the information requiring a police incident report by phone. Although an in person response is the preferred method of receiving information for a police incident report, the situation encountered may dictate the information be received by phone.

Below are the requirements for receiving information requiring a police incident report by phone:

1. There is a valid reason not to take the information in person. The reasoning may include but not be limited to the following:
 - a. Health and safety of the reporting party or the officer (e.g. pandemic).
 - b. The reporting party does not reside in Urbandale and it is not feasible for them to respond in person to the station or for the officer to respond to their location.
 2. The information provided by the reporting party can be verified as being truthful, accurate, and complete.
 3. Adequate report information is able to be obtained to meet the reporting requirements of the Department.
 4. Supervisory approval.
- D. All reports shall be completed in a neat, accurate, and timely manner in order to provide the required documentation for follow-up investigations and use in other components of the criminal justice system.
- E. The majority of report forms utilized for documenting an incident shall be maintained electronically as stated in Chapter 2 Section 11.4.2 (Agency Forms) of the Operations Manual. The Support Services Division shall be responsible for maintaining an adequate supply of any form that is not stored electronically.
- F. All employees shall maintain a thorough working knowledge of all report forms and their use.
- G. Reports must contain all required information. Upon review, supervisors shall return incomplete reports to the employee for correction.
- H. The field training program shall ensure officers are properly trained in the following:
 1. The reports are required for specific incidents.
 2. Properly completing reports.
 3. Process to submit reports once complete.
- I. Persons taken into custody by the Urbandale Police Department that are required to be fingerprinted and photographed shall be assigned a unique identifying number for their custody file.
- J. Identification information, fingerprints, and photographs from the custody shall be stored by the State of Iowa Department of Public Safety.

III. Procedure: Reports

A. Case Investigation Report:

1. The Case Investigation Report (CIR) is to be used to record the preliminary information on all criminal occurrences for which a police report is required to facilitate either police or court action. The CIR may also be utilized to record non-criminal incidents where documentation may be needed for future reference or referral (e.g. juvenile runaway, attempted suicide, death investigations, etc.).
2. Incidents that do not warrant a CIR or other documentation shall be recorded in the Computer Aided Dispatch (CAD) system.

3. The supervisors shall monitor the use of the CIR to ensure the necessary information is completed. Failure to properly document an incident in a CIR and accompanying forms may result in disciplinary action. Supervisors who approve incomplete and inadequate reports may also be subject to disciplinary action.
4. CIRs shall be completed and submitted to the shift supervisor prior to the end of a tour of duty. A CIR may be held for completion at a later time with the approval of the shift supervisor. When a CIR is held and may be of significance to the Investigation Division or Support Services Division, the supervisor shall make the appropriate division(s) aware of the status of the case.
5. All appropriate sections of the CIR shall be completed to include summary, offense, offender, victim, vehicle, property, narrative, and any other fields provided that assist in documenting the incident.
6. The narrative portion of the CIR shall contain a complete written account of the incident. The narrative portion shall explain how the call originated, and the officer's response and observations.
7. Any use of force shall be thoroughly and completely documented in the CIR.

B. Arrest Reports:

1. An arrest report shall be completed for the arrest of any person charged with a criminal offense that will be filed by the Urbandale Police Department.
2. An arrest report is not required for nuisance violations (e.g. dog at large, DPQ) that are cited at the scene.

C. State Accident Reports:

1. Accidents involving death, personal injury, hit and run, or property damage totaling an amount established by the State of Iowa Department of Transportation shall be reported on the State of Iowa accident report. Guidelines for accident reporting are stated in Chapter 7 Section 61.2.1(Traffic Accidents) of the Operations Manual.
2. All accident reports shall be submitted at the end of an officer's tour of duty. Accident reports may be held upon approval of the shift supervisor. When appropriate, the supervisor shall advise the Support Services Division when an accident is being held for completion.

D. Field Interview Reports:

Field Interview reports shall be completed on all persons encountered in suspicious circumstances where a CIR is not required. The Field interview report shall be filled out in detail, to include a brief summary of the circumstances in which the person was interviewed.

E. Complaint/Probable Cause:

The appropriate complaint/probable cause form based on the location of the offense (Polk or Dallas County) and whether the offender is a juvenile or an adult will be completed for anyone arrested for a criminal offense or a traffic offense that is classified by Iowa Code as a serious misdemeanor, aggravated misdemeanor, or felony.

F. Vehicle Impound Report:

The vehicle impound report will be used for impounding vehicles and shall be used in lieu of a CIR where there is no other incident involving the vehicle other than the impound. See Chapter 1 Section 1.2.4 (Search and Seizure/ Vehicle Impound and Inventory) of the Operations Manual.

G. Supplemental Report:

A supplemental report shall be used to document any action taken on an incident that was not captured in the original narrative section of the CIR.

H. Traffic Citation:

1. A traffic citation shall be utilized when an offender is charged with a traffic offense other than a traffic offense classified by Iowa Code as a serious misdemeanor, aggravated misdemeanor, or felony.
2. Traffic citations are issued electronically. Each electronic citation shall be issued a unique number by the system. Employees shall not be allowed to delete citations from the system. If an error is made, the citation shall be placed in an archive file. Once a citation has been issued to a violator, approval must be obtained from the Chief of Police to void the citation.
3. Citations are electronically transferred to the records management system, the State of Iowa, and the appropriate court.
4. When necessary due to failure of electronic equipment, hard copy citations may be issued to violators. Information from the hard copy shall be entered into the Records Management System and the originals shall be forwarded to the appropriate court.

IV. Procedure: Submission and Distribution of Reports

- A.** Supervisors shall be required to review and approve all reports. The supervisor shall ensure required reports are not missing and submitted reports do not contain incomplete information. When discovered, the supervisor shall instruct the submitting officer to correct deficiencies.
- B.** After supervisory approval, reports shall be forwarded to Support Services Division for entry into the records management system. Documents that cannot be submitted electronically shall be submitted in paper form.
- C.** Once the reports have been submitted, Support Services Division personnel shall enter the reports into the Department's record management system (RMS). Images of the reports shall also be saved in the electronic case file system (Laserfiche).
- D.** The Support Services Division shall be responsible for the distribution of all reports and departmental records to include:
 1. Distribution to the other divisions within the Department.
 2. Distribution to the appropriate prosecuting attorney's office.
 3. Distribution to other law enforcement agencies.
 4. Distribution to the public in the form of an open records request as stated in Chapter 9 Section 82.1.1(Records Administration) of the Operations Manual.
- E.** Officers or staff who have case related items (pictures, video, documents, etc.) that need to be forwarded to the Criminal Investigation Division shall

utilize the specific email account established for submission. The CID email account specified for submissions may also be utilized by victims, witnesses and others to directly submit items to CID.

V. Procedure: Records Maintenance

- A.** The Support Services Division records section shall be the central repository of all original offense, incident, arrest, and traffic accident reports.
- B.** Operational components (patrol, investigations, support services, etc.) are allowed to maintain files on cases being actively investigated. Once the case is no longer active, it is the responsibility of the officer maintaining the working file to transfer all information to the main case file.
- C.** Images of case file reports shall be maintained electronically. All paper copy case files shall be maintained until they have been electronically copied into Laserfiche. Once electronically stored, case files shall be maintained indefinitely.
- D.** The Investigation Division shall maintain the original records involving departmental intelligence. See Chapter 5 Section 40.2.3 (Criminal Intelligence) of the Operations Manual for information on intelligence files.
- E.** All required divisional reports shall be maintained by the commander of each division either electronically or in paper form. When appropriate, the reports shall be stored in the Laserfiche Imaging System.
- F.** The City of Urbandale Human Resources shall maintain the Department's personnel records.
- G.** The Department's training records shall be maintained by the Support Services Division.
- H.** The Office of the Chief of Police with the assistance of the Support Services Division shall be responsible for the maintenance of all administrative records.
- I.** Complaint and internal affairs investigations shall be maintained by the Internal Affairs Administrator.

VI. Procedure: Identification Number and Criminal History File

- A.** Custodial arrested shall be defined as any person arrested and transported to a holding facility or jail for processing. For the purpose of this policy, persons detained and cited for a violation(s) at the scene shall not be considered a custodial arrest.
- B.** Juveniles custodial arrested for violations that are simple misdemeanors shall not be fingerprinted or photographed per Iowa Code 232.148. Juveniles custodial arrested for all other crimes serious misdemeanor, aggravated misdemeanor, or felony be fingerprinted and photographed.
- C.** When an adult is custodial arrested for a violation classified by Iowa code as an enhanceable simple misdemeanor, serious misdemeanor, aggravated misdemeanor, or felony, they shall be fingerprinted and photographed. The fingerprints, photographs, and other identifiers (e.g. scars, marks, and tattoos) shall be submitted to the Iowa Department of Public Safety Division of Criminal Investigations (DCI). Based on the custodial arrest, the DCI shall issue the person a unique identification

number (DCI number). The DCI number shall be unique to the individual arrested. Any future custodial arrests of the person for an enhanceable simple misdemeanor (adults only), serious misdemeanor, aggravated misdemeanor, or felony shall utilize the same unique DCI number for identification and criminal history file maintenance. The information from the custodial arrest, including information from any previous or subsequent custodial arrests classified by Iowa Code as an enhanceable simple misdemeanor (adults only), serious misdemeanor, aggravated misdemeanor, or felony, is available to department personnel through a secure login to DCI data bases. Searches may be conducted by name, identifiers, or the uniquely assigned DCI number.

Chapter 9: Auxiliary and Technical Services
Section 83: Collection and Preservation of Evidence
Subsection 1: Administration



Policy/Procedure #: 1

Title: Collection and Preservation of Evidence

CALEA Reference#: 83.1.1, 83.2.1, 83.2.2, 83.2.3, 83.2.4, 83.2.5, 83.2.6, 83.3.1, 83.3.2

I. Policy: Collection and Preservation of Evidence

The proper collection and preservation of evidence is essential to the effective investigation and prosecution of criminal activity. The Urbandale Police Department is committed to utilizing best practices in collecting and preserving evidence including the use of outside expertise when warranted.

II. Procedure: Qualified Personnel

A. The Department shall maintain a group of qualified crime scene investigators (CSI) trained to process scenes for evidence. CSI personnel shall be on a twenty four (24) hour on-call rotation to ensure availability at all times. A current on-call list shall be provided to the WestCom Communications Center to facilitate notification. CSI shall be utilized in the following situations:

1. All serious person crimes in which collection of evidence and/or photographing the scene is critical to the investigation. CSI shall only be used for property crimes with supervisor approval.
2. At the request of a supervisor or accident investigator, assist in documentation and preservation of evidence in a motor vehicle accidents in which there is a fatality or a strong possibility a fatality will occur.
3. All death investigations except when the following are present:
 - a. The death was a foreseen medical event, the deceased was in the care of a physician, and the supervisor in charge determines there are no suspicious circumstances.
 - b. Due to the age and medical condition of the deceased, the medical examiner has made an initial determination the cause of death was natural causes and the supervisor in charge determines there are no suspicious circumstances.
4. When the supervisor in charge determines the use of a CSI is needed to properly document and preserve a scene.

- B. The Department shall maintain a group of qualified motor vehicle accident investigators trained to properly document motor vehicle accident scenes. Accident investigative personnel shall be on a twenty four (24) hour on call rotation to ensure availability at all times. A current on-call list shall be provided to WestCom Communications Center to facilitate notification. Accident investigators shall be utilized in the following situations:
 - 1. All fatal motor vehicle accidents
 - 2. All motor vehicle accidents in which the injuries sustained are likely to result in a fatality.
 - 3. When the supervisor in charge determines the use of an accident investigator is needed to properly document and preserve a scene.
- C. When needed, accident Investigators may utilize CSI personnel to assist in documenting the scene and preserving evidence at a motor vehicle accident scene.

III. Procedure: Evidence Collecting, Processing and Preserving

- A. The Department shall provide employees with guidelines and uniform procedures which incorporate scientific methods for the collection and preservation of physical evidence. A thorough, detailed evidence collection process will ensure the following:
 - 1. The integrity of the chain of custody of evidence is maintained.
 - 2. The evidence will contribute to the success of an investigation.
 - 3. The evidence will facilitate the prosecution of criminal offenders.
- B. All officers shall receive evidence handling and collection training in their initial academy and during the field training process.
- C. It is the responsibility of the first officer arriving on the scene of an incident to secure the scene from all nonessential persons. The incident scene must be secured as soon as possible to prevent the contamination, disturbance, or loss of evidence. When necessary, the securing officer shall request assistance from the supervisor in protecting the crime scene. The supervisor in charge of the scene shall make a determination if a CSI or an accident investigator is needed.
- D. If the incident is a homicide or other serious incident, the officer securing the scene shall initiate a log or include in his supplemental report the name, time, and reason for all personnel who enter the scene until the responsibility is relinquished to the Investigation Division.
- E. The securing officer will ensure all personnel on the scene do not disturb or touch physical evidence while waiting for the arrival of the Investigation Division, a CSI, or an accident investigator. An exception to this would be situations where a danger exists of the evidence being lost or destroyed or a victim needing medical attention. In this type of situation, it is the responsibility of the securing officer, whenever possible, to secure and preserve the evidence in an appropriate manner utilizing all available means at their disposal, pursuant to procedures outlined in this policy.
- F. The securing officer shall remain on the scene until turned over to the Investigation Division, a CSI, an accident investigator, or relieved by a

supervisor. Any time an officer having security over a crime scene or evidence in the field releases the scene or evidence to another officer, investigator, CSI, etc., the transfer and the reason shall be documented.

- G. The assigned CSI or accident investigator shall have the primary responsibility for processing the scene unless they are relieved by a supervisor. When assigned to an incident, the CSI is responsible for photographing, collecting, preserving, transporting, and submitting all evidence to property/evidence.
- H. The documentation of all chain of custody events from the time of seizure until the final disposition of an item shall be meticulously recorded.
- I. If the incident is a property crime or minor in nature, evidentiary items may be collected, preserved, inventoried, transported, and submitted by the on-scene officer(s) pursuant to procedures outlined in this policy. When needed, officers shall request the items be examined and processed by a CSI at the earliest convenience.
- J. When an officer or CSI personnel collect or process evidence as part of a crime scene, they shall complete a report detailing their examinations, observations, and activity. These reports shall be submitted for supervisory approval and entry into the records management system.
- K. Officers assigned to investigate an accident shall ensure proper documentation of the event is recorded in an accident or supplemental report. When a motor vehicle accident investigator is assigned to investigate an accident, they shall ensure the responding officer has completed the state accident report and offer assistance completing the report as needed. The accident investigator shall complete any supplemental reports needed to detail the findings of their investigations. The reports shall be approved by a Patrol Division supervisor and submitted to the Support Services Division for entry into the records management system.
- L. When large property or evidence items are seized, officer may request the assistance of the property/evidence officer to assist in transporting the items to the Police Department utilizing the Support Services Division pickup truck. After hours, officer may utilize the pickup truck as needed to transport large items.

IV. Procedure: Requesting a CSI or Motor Vehicle Accident Investigator

- A. A supervisor may request a CSI or a motor vehicle accident investigator for any incident that requires photography or the preservation or collection evidence that cannot be adequately accomplished by officers on the scene or when additional manpower is needed to free patrol officers for other duties. When unsure, the supervisor shall contact the CSI or accident investigator for assistance in determining the value of a response. The decision to have the CSI or the accident investigator respond shall remain with the supervisor.
- B. When requesting a CSI the following factors shall be considered:

1. The crime is a persons related crime that is serious in nature. Under normal circumstances, property crimes will not warrant a CSI response unless mitigating circumstances exist (e.g. linked to a person crime that is serious in nature).
 2. A suspect is in custody or a known person is suspected and evidence may place them at the scene.
 3. There is a strong likelihood of obtaining latent fingerprints suitable for comparison or other physical evidence that may link an unknown suspect(s) to the scene at a later date.
 4. There are visible footprints or tire impressions believed to have been left by the suspect(s).
 5. There is visible blood or trace evidence present.
- C.** When calling out a CSI or an accident investigator, the supervisor requesting shall attempt to convey the need for any special equipment (e.g. camera equipment, latent fingerprint collection equipment, plaster casting kit, barrier tape, total station, etc.).
- D.** Scenes that may contain evidence or documentation require a prompt response. CSIs and accident investigators shall be able to respond to a scene within one (1) hour. If unable to respond in this time frame, the supervisor requesting shall be made aware along with an anticipated time of arrival.
- E.** In the event the supervisor has made every effort to contact an on-call CSI with negative results, other department CSI personnel shall be contacted for assistance. If none are available, the supervisor may request outside assistance from another agency after receiving permission from the Division Commander. At the earliest convenience, the Chief of Police shall be notified of the need to utilize outside agency assistance.
- F.** In the event the supervisor has made every effort to obtain an on-call accident investigator with negative results, other department accident investigators shall be contacted for assistance. If none are available, the supervisor may request outside assistance from another agency after receiving permission from the Division Commander. At the earliest convenience, the Chief of Police shall be notified of the need to utilize outside agency assistance.
- G.** Once the assigned CSI or accident investigator arrives on the scene, the securing/reporting officer or their supervisor and the investigator shall review the scene and any events including details on possible evidence or items of special interest. Protocol for scene security are as follows:
1. In all major incidents, the securing/reporting officer will remain on the scene until the arrival of the investigator called.
 2. With the approval of a supervisor, the reporting officer may leave the scene prior to the on-call investigators arrival on minor incidents. The supervisor will only grant his approval if there is a reasonable expectation the area(s) targeted for evidence technician processing will remain secure or security is not an issue. Availability of manpower may be a primary consideration in this decision.

3. In some situations, the on-call investigator may request the securing officer and/or reporting officer remain on the scene to provide assistance and/or security. This request will be made to the supervisor in charge for approval.
- H. The assigned CSI or accident investigator shall cooperate with the Investigation Division including:
1. Forwarding supplemental reports to the Criminal Investigation Division supervisor.
 2. Making immediate notification to the assigned detective and/or the Investigation Division supervisor of any significant scene findings or discoveries.
 3. Upon request, provide a briefing to a division commander or the Chief of Police detailing the results of the scene processing.
- V. **Procedure: Inter-Agency Coordination**
- A. The Investigation Division Commander shall be responsible for ensuring all CSIs are properly trained and equipped.
- B. CSI shall be responsible for the following:
1. All evidence equipment is maintained in operational readiness condition.
 2. The evidence processing room is maintained in a clean and functional manner.
 3. Adequate supplies are maintained and replenished.
 4. Any supply or equipment problems will be brought to their supervisor's attention.
 5. Submission of a detailed report documenting all activities involved in processing a scene.
- C. The Patrol Division Commander shall be responsible for ensuring all motor vehicle accident investigators are properly trained and equipped.
- D. The accident investigator shall be responsible for the following:
1. All needed equipment is maintained in operational readiness condition.
 2. Adequate supplies are maintained and replenished.
 3. Any supply or equipment problems will be brought to their supervisor's attention.
 4. Submission of a detailed report documenting all activities involved in processing a scene.
- VI. **Procedure: Outside Agency Assistance**
- A. In some cases, it might be advantageous to the Department to utilize the services of an outside agency for assistance in processing a scene (e.g. Division of Criminal Investigation, Iowa State Patrol, Des Moines Police, A.T.F., F.B.I., etc.). In these situations, manpower availability, experience, and complexity of the crime scene will be considered.
- B. Except in the situation noted above where no personnel from the Department are able to respond, the decision to request the services of an outside agency shall be made by the Chief of Police.
- C. If an outside agency is to be utilized, a request will be made to the applicable personnel to allow the Department's assigned investigators to

assist and/or observe in the crime scene processing. This will allow for increased coordination between the two agencies and the enhancement of skills for the Department's investigators.

VII. Procedures: Photography and audio/video recordings

- A.** The Department shall only utilize digital photography and digital audio/video during the collection and preservation of a crime scene or other evidentiary documentation. Conventional photography and audio/video tapes shall no longer be utilized. Upon being called to an incident, photographing and/or audio/video recording crime scenes and other incidents shall be the responsibility of the CSI. Patrol officers, investigators, and supervisors may photograph and/or audio/video minor incidents and accidents where a CSI is not warranted. Preceding the photographing or audio/video recording of any scene, the first frame shall be the information placard stating the case number, date/time, and the officer taking the photograph or audio/video. When utilizing the in-car audio/video recording equipment, the placard is not required and all audio/video files captured on the system shall be processed according to Chapter 5 Section 41.3.8 (In-car recording system) of the Operations Manual. Photographs and/or audio/video of the scene shall be taken utilizing the most appropriate equipment based on the conditions. Under normal circumstances, photographs and/or audio/video of the scene shall be taken prior to any items being moved, altered, or collected.
- B.** When photographs are taken by patrol officers utilizing the digital cameras in each patrol car, the officer taking the photographs shall inform the on-duty sergeant and the property/evidence officer there are photographs from a specific case on a patrol car camera. The property/evidence officer shall download the digital photographs and save them to the appropriate secure server categorized by case number unless the photographs are copied to a disk or other type of storage device as established in section VII (D) of this policy.
- C.** Evidentiary photographs and audio/video recordings shall be saved on the appropriate secure server categorized by case number. Photographs and video placed on the secure server shall be retained for three (3) years. If the photographs or audio/video have been copied to a disk or other type of storage device and placed in evidence as established in section VII (D) of this policy, they shall not be placed on the secure server.
- D.** Any photographs or audio/video taken by Department personnel as part of a case or incident investigation shall be saved in the designated location on the Department's secured server. If the incident produces an extremely large amount of audio and/or visual data (i.e., computer forensic evidence, cell phone extractions, electronic storage devices, etc.) personnel shall consult with their supervisors and determine if the items need to be saved on an external storage device. Audio and/or visual data copied to an external storage device shall be entered into evidence and shall not be saved on the secure server.

In-car and body worn camera audio/video files have their own set of established procedures and shall be preserved as stated in Chapter 5 Section 41.3.8 (In-car recording system) of the Operations Manual.

- E. When the exact size of an item being photographed is required, a scale will be placed next to the item to add dimension and aid in the development of scale prints. In these situations a second identical photograph of the item will be taken without the scale, or anything else introduced into the field of view.
- F. Under most circumstances, a CSI shall utilize a photograph log sheet. The photograph log sheet shall assign a number to each photograph and contain the date, time, location, subject, photographer's name, and case number.
- G. All digital photographs and audio/video files shall be the property of the Urbandale Police Department. Digital photographs and audio/video files shall not be released without authorization of the Chief of Police or his/her designee except in the following situations:
 - 1. The recording/photographs have been requested by the city attorney, county attorney, the attorney general's office, or the United States attorney's office as part of a criminal prosecution.
 - 2. The recording/photographs have been subpoenaed by an attorney and the release has been approved by a supervisor after checking with the appropriate prosecutor.
- H. As stated in Chapter 3 Section 26.1.1 9 (Departmental Rules and Regulations) Except in emergency situations, employees on-duty shall not use personally owned cellphones or other personally owned devices to capture audio, video, or photographs of any calls for service or other official police operations. If a personal device is used to capture an emergency situation, the file shall become the property of the Department. The details of capturing the event shall be entered into a report and the file shall be downloaded into the appropriate format and entered into evidence. Once entered into evidence, the file shall be deleted from the personal device.

VIII. Procedure: Crime Scene Sketches or Digital Renderings

- A. When crime scene sketches are drawn or a digital rendering of the scene are produced, pursuant to the procedures outlined for the collection and preservation of evidence, they will generally contain the following information:
 - 1. Dimensions.
 - 2. Relation of the scene to other buildings, geographical features and/or marks, or roads.
 - 3. Address, floor or room number, as appropriate.
 - 4. Location of significant features of the scene, including the victim (if applicable).
 - 5. Date and time of preparation.
 - 6. Identification of the officer(s) preparing the sketch or digital rendering.
 - 7. Indication of north.

8. Exact location of evidence.
- B. Generally, the investigator processing the scene shall make rough sketches/digital renderings and measurements, including sufficient information so a final scale drawing or rendering can be made at a later time.
- C. These rough and final sketches or digital renderings shall be retained in the appropriate secure server.

IX. Procedure: Collection of Known Source for Comparison

- A. A significant amount of the value of laboratory examinations is the identification of substances and the comparison of these substances with materials from known sources.
- B. To facilitate this process, whenever practical, the following procedures will be followed when the types of physical/trace evidence specified below are collected for crime lab examination:
 1. Hair. A known standard sample will be collected from the victim/suspect. Hairs shall be plucked (never cut). A minimum of twenty-five (25) hairs shall be pulled from the head in groups of five (5). These head hairs will be obtained from different sections of the head (front, back, top, sides). When able, a minimum of twelve (12) hairs shall also be collected from the pubic area. Hair samples collected from different areas will be packaged separately. In the case of rape victims, the rape kit is used for this purpose and collected by hospital staff.
 2. Fibers. A known standard sample of the fiber/material will be collected from the applicable source. The samples will be packaged separately to avoid contamination.
 3. Paint. Paint can appear in the form of chips, flakes, smears, or impact paint on an object. A known standard sample shall be chipped or scraped from the applicable source.
 - a. Flakes or Chips. If slightly adhered to an object, it shall be carefully removed and placed into a suitable evidence container. Do not use lifting tape, scotch tape, or plastic bags.
 - b. Paint Smears. If possible, this shall be left intact on the object and packaged.
 - c. Glass. A known standard sample shall be collected from the applicable source. It shall be packaged in such a manner as to prevent further breakage. All glass shall be safely packaged to prevent breakage and injury. The exterior packaging shall clearly indicate the item is glass or fragile.
 - (1) In cases where the glass has been broken out of a frame, if possible, the broken fragments and frame shall be removed intact for future reconstruction.
 - (2) If not possible to remove the frame, the pieces shall be marked as to their inside/outside surfaces and position in the frame.
 4. Soil. A known standard sample shall be collected from applicable scene areas.

- a. Soil samples shall consist of a minimum of two (2) tablespoons of soil. Samples shall not be collected from deeper than one (1) inch.
 - b. Samples from different areas are to be packaged separately.
 - c. The collection tool must be thoroughly cleaned after each sample is collected.
 - d. If soil is found on a suspect's shoe, comparison samples shall be taken from any observable foot prints at the scene.
- 5. Wood. A known standard sample shall be collected from applicable crime scene areas.
 - a. Whenever possible, the entire wooden object shall be collected and packaged appropriately.
 - b. If it is not practical to remove the entire object, a sufficient portion of the wooden object shall be carefully cut off. Prior to removing the sample, the area to be removed will be photographed showing its location on the entire object. The method of removal will be documented in a supplemental report.
- 6. Blood. A known standard sample shall be collected from the victim/suspect. All such blood samples will only be collected by a physician licensed to practice medicine, a registered nurse, medical technologist or by a trained phlebotomist acting under the direction of a licensed physician.
 - a. Two vials of blood will be collected and inventoried. The property custody report will include the following:
 - (1) The collecting facility.
 - (2) Name of the collecting attendant.
 - (3) Time and date collected.
 - b. All blood sample collections will be witnessed by a police officer, preferably the case officer, in such manner the officer can testify in court as to the source of the sample.
 - c. The officer who witnessed the collection must sign each of the two samples by completing and affixing labels.
- D. Whenever the collection of a known standard for comparison purposes involves a suspect (e.g. hair, blood, items belonging to or in possession of the suspect), the appropriate prosecuting attorney's office shall be contacted for approval. It may be necessary to obtain a search warrant or court order prior to collection.
- E. The location and/or the source from which the samples are taken are critical to the investigation and shall be documented by the recovering officer on a supplementary report.

X. Procedure: Latent Prints

A. Processing:

- 1. When processing for latent prints an officer shall determine those items and surfaces known to be touched by or most likely to have been touched by the perpetrator.
- 2. Look for surfaces that are smooth (e.g. glass, metal etc.).

3. Examine the surface to be processed, using a light if necessary, looking for visible latent prints.
 4. Note where possible prints are observed.
 5. If clearly visible prior to developing, a photograph of the print shall be taken.
- B. Developing:**
1. Using a contrasting color powder, apply a small amount of powder onto a latent print brush and begin applying to the surface.
 2. Apply the powder in a circular motion, with the tip of the brush barely touching the surface.
 3. Build powder onto the ridges and stop when the latent print reaches the point of sufficient clarity.
 4. Clean excess powder from between the ridges using a smaller brush if necessary.
 5. Examine the latent print using a light source. If the print appears to be of sufficient quality for identification, photograph the developed print. Ensure scale is used in the photograph.
- C. Lifting:**
1. Lift the print using clear latent print tape.
 2. Place the tape onto the surface starting on one edge and work across the print until reaching the other edge.
 3. Lift the tape from the surface reversing the direction the tape was placed on the surface.
 4. Place the tape onto a clear lift print plastic or onto an appropriate contrasting latent print lift card.
 5. Make note of where the print was located and include in your report.
- D. Labeling:**
1. Mark the case number, date and initials of the lifting officer on the lift card
 2. Place the latent print card into an evidence bag, label, and submit to property evidence control per department policy.
- E.** It may be necessary to submit elimination finger and palm prints of victims/witnesses. This shall be determined by the detective or supervisor assigned to the investigation.
- F. Cyanoacrylate Fuming:** The following procedures shall be conducted by trained CSI personnel only:
1. Place the items to be fumed into the fuming chamber. Be careful not to place the items next to the heating element. (Items with fluid shall be emptied before processing)
 2. Fill the glass jar with water and place it near the heating element. The humidity will assist in the development of prints.
 3. Place the cyanoacrylate liquid onto an aluminum cup and place the cup on the heating element.
 4. Close the access door and lock. Make sure the Defumigator hose on the right side of the chamber is attached to both the chamber and the Defumigator.

5. Turn on the heating element(s). Allow the cyanoacrylate to heat for about 45 minutes.
6. Turn off the heating element and turn on the Defumigator using the "30 minute" button. Allow the Defumigator to complete the 30 minute cycle. Repeat this process an additional 2 to 3 times depending on the amount of fuming done.
7. Put on protective eyewear and mask. Open the chamber and remove the items. **Use caution, cyanoacrylate fumes can cause contacts lens to glue to the eyes**
8. Place the items to be processed into the air hood and process for latent prints.
9. Examine any latent prints developed from the process. If the print appears to be of sufficient quality for identification, photograph the developed print. Ensure scale is used in the photograph.
10. Use the same procedures for lifting and labeling the latent print as described above.

XI. Procedure: DNA and Other Physical Evidence Collection

- A. Every officer, from the first responding patrol officer to the experienced detective and the crime scene technician, shall be aware of important issues involved in the identification, collection, transportation, and storage of DNA and other physical evidence. Because extremely small samples of DNA and other items can be used as evidence, attention to contamination issues are necessary. Evidence can be contaminated when DNA or other physical evidence from another source gets mixed with DNA or other physical evidence relevant to the case. With DNA evidence, this may even occur when someone sneezes or coughs over the evidence or touches his or her mouth, nose or other part of the face and then touches the area of the evidence containing the DNA.
- B. All officers shall receive training in the collection, storage, and transportation of DNA and other physical evidence.
- C. The following procedures shall be utilized to store DNA and other physical evidence:
 1. The item must be completely dry before packaging. Officers collecting DNA or other physical evidence that needs to be dried can transfer custody of the item to CSI personnel for drying. CSI personnel shall secure the item in the lab for drying prior to entering into property evidence control. Custody and control must be maintained.
 2. DNA evidence shall be packaged in paper type packaging (e.g. envelope, paper sack, cardboard box, etc.). No plastic packaging shall be utilized. Other physical evidence may also warrant packaging in non-plastic packaging. If in doubt, consult with CSI personnel for direction on proper packaging.
 3. DNA evidence shall be stored at room temperature. Cooler temperatures are acceptable. A hot storage environment is not acceptable. All DNA evidence shall be stored on the lower shelves in property/ evidence to avoid potential exposure to high temperatures in

the summer months. Other physical evidence may also be susceptible to damage from a hot storage environment. Any physical evidence that much be kept in a cool environment shall be noted on the packaging and the property evidence custodian notified.

4. DNA evidence shall not be stored with direct prolonged exposure to fluorescent light. Proper packaging shall, as stated above, protect the item sufficiently. If other physical evidence is susceptible to damage from fluorescent light, it shall also be packaged in a manner to protect it from exposure and damage.
- D. To avoid contamination of evidence, the following precautions shall be utilized:
1. Wear gloves. Change gloves frequently and as necessary to avoid cross-contamination.
 2. Use disposable instruments or clean them thoroughly before and after handling each sample.
 3. Avoid touching the area of the evidence where you believe DNA or other physical evidence may exist.
 4. Avoid talking, sneezing, scratching, and coughing over evidence.
 5. Avoid touching your face, nose and mouth when collecting and packaging evidence.
 6. Air-dry evidence thoroughly before packaging (not in direct sunlight).
 7. Put DNA evidence into new paper bags or paper envelopes. Do not use plastic bags, or staples. Other physical evidence may be packaged utilizing plastic bags if the bag will not corrupt the evidence.
 8. Affix bio-hazard labels on bags and envelopes when appropriate.
- E. When collecting evidence from a scene which may have DNA or other physical evidence, collecting personnel shall follow these steps:
1. When able, the entire item containing the sample shall be taken. The item shall be placed into a paper evidence bag (DNA evidence) or other appropriate packaging and transported to the police department for further processing by the CSI or lab personnel.
 2. When the original item is too large, cut the area needing collection from the original item, place it into a paper evidence bag (DNA evidence) or other appropriate packaging and transport it to the Department for further processing by the CSI or lab personnel.
 3. When collecting DNA evidence and neither taking the entire item nor removing the appropriate area is applicable, a sample of the substance may be collected using swabbing.
 4. Items containing moisture must be air dried. Care must be taken when air-drying to avoid contamination. This may be done by packaging the item in a container that will allow air circulation such as a paper sack, or envelope. Wet clothing, bed sheets and other similar items shall be hung to dry. Do not fold such items together since certain types of analysis may be lost if transfer stains are made on the item.
- F. Collection of control samples from a scene or item is necessary to provide comparison samples to lab technicians in their process for testing DNA

and other physical evidence. To collect control samples the collector shall follow these steps when not providing the full original item to the lab:

1. Collect a portion of apparently unstained fabric or surface. (NOTE: If stain cut from original item, include unstained portion with cutting, keeping the two samples in separate paper bags to prohibit contamination.)
2. If the sample is dried slightly, moisten a clean cotton-tipped swab with sterile water. No water is needed if sample is moist.
3. Wipe the cotton tipped swab into the sample.
4. As with fingerprints, the effective use of DNA may require the collection and analysis of "elimination samples." These samples are necessary to determine whether the evidence came from the suspect or from someone else.

G. Collection of DNA Evidence from persons shall be handled in the following manner:

1. Photograph the sample before collection, package correctly, and initial and date each sample.
2. Blood collection will be in accordance with the provisions listed above.
3. Cheek swab (buccal) shall be collected using the DNA collection kit. The cotton tipped-swab shall be scrubbed on the inside of the cheek. Do not just moisten with saliva. The collector shall ensure the provider of the sample has not eaten or drank anything for 20 minutes before collection.
4. Semen and saliva samples shall be collected in the same method as blood from an inanimate object. If collecting from a human source, semen can be swabbed from a body in the same procedure as one would swab blood. The officer must wear protective gloves during this procedure. In all cases, saliva and semen samples must be air dried, or stored in a refrigerator.
5. Hair must be collected in a manner to prevent contamination. Hair shall be collected in accordance with the provisions listed above. Hair shall be stored in a cool environment to ensure best preservation. It is not necessary to refrigerate it.

H. When transporting and storing DNA evidence and other physical evidence, keep the evidence dry and at room temperature. Once the evidence has been secured in paper bags or paper envelopes, it must be sealed, labeled and transported in a way that ensures proper identification and proper chain of custody. Place BIO-Hazard labels on packages as appropriate. Never place DNA evidence in plastic bags as the moisture retained in the bags can be damaging to the DNA. Direct sunlight and hot conditions also may be harmful to DNA. Avoid keeping evidence in places that may get hot, such as a room or vehicle without air conditioning.

I. Ultra-violet lights (UV), oblique lights, amido black, and luminol are processes that may be used to locate substances. Caution shall be utilized as some of these tests may have adverse effects on DNA evidence.

- J. All DNA sample testing will be done by the Iowa Division of Criminal Investigation Laboratory or an accredited private laboratory. Transportation of the evidence to the laboratory will follow accepted practices to maintain the chain of custody of such evidence.

XII. Procedure: Seizure of Electronic Equipment and Other Devices Capable of Storing Data in Electronic Format.

- A. Officers shall exercise extreme caution when seizing and/or examining computer equipment, cellular telephones, Personal Digital Assistants, (PDAs), thumb drives, external hard drives and other devices capable of storing data in an electronic format so as not to cause damage or the loss of valuable data.
- B. When deemed necessary, employees or outside experts possessing specialized knowledge of computers and computer security shall be consulted during the preparation and execution of search warrants. It is preferable a computer forensic investigator be present during the seizure. In situations where electronic evidence was not expected to be present, but during the search is discovered, a computer forensic investigator or person trained in the seizure of electronic equipment may be consulted.
- C. Officers shall not rely on suspects, even when they are cooperative, for any computer-related assistance. Be aware the suspect may have access to technology that may allow the suspect to remotely access the system. If a program is running that appears to be destroying the data on the system, immediately unplug the power cord from the back of the system.
- D. Observe the device and look for any running programs. When computer equipment is in operation at the time of seizure, an employee or outside expert possessing specialized knowledge of computers shall be consulted prior to taking any action as systems react differently to being powered down. Based on the type of system encountered, data cached in memory may be lost if the computer is powered down. Do not allow anyone to touch the computer keyboard or operate any electronic devices.
- E. There may be times when you need to keep these devices powered up; however, they shall be packaged to prevent any kind of electronic broadcast. In these situations, use a paint can or other type of enclosure that defeats remote access to the device.
- F. Consideration shall be given to photographing and/or videotaping on-screen images before operating computer equipment is disconnected from the power source. This procedure will ensure pertinent evidence will be captured when cached memory and/or embedded scripts are involved.
- G. Photograph and diagram the computer and all associated devices from various angles, including any connections between devices. Mark all connections attached to the computer system or other electronic devices. Photograph again as needed. Check for outside connectivity (e.g. a telephone modem, cable or DSL). If a telephone connection is present, attempt to identify the telephone number.
- H. Photograph and gather all associated property regarding the electronic device. This may include the following:

1. Instruction manuals for devices and software.
 2. All loose electronic media, such as hard drives, floppy disks, CD's, DVD's, thumb drives and any other removable storage devices.
 3. Written media that may contain user names and passwords. Also financial statements indicating internet service providers and other subscription services.
 4. All power supply cords or other cables for cell phones, PDA's and other portable electronic media.
 5. Docking stations of portable electronic media.
- I.** Non-operating computers, disks, drives, and related peripherals shall be considered fragile. Such equipment shall be appropriately packaged, handled, and transported. Special care must be taken to avoid exposing removable media, such as tapes, floppy disks, hard drives, zip disks, and jazz disks, to magnetic fields. Radio transmitters, speaker magnets and heated seats are examples of items that can damage electronic evidence.
- J.** Place evidence tape over the drive slots of a computer, as well as the power cord connection. Place evidence tape on the computer case where parts of the case connect together. For laptops, place in a paper sack and seal the bag in accordance with departmental evidence handling procedures. An alternative method for securing laptops is to place evidence tape over the power connection and battery compartment (with battery removed). Package smaller media in antistatic packaging or paper sacks.
- K.** Some types of removable media, such as zip disks and jazz disks, may be rendered useless by exposure to static electricity and physical force.
- L.** Store electronic evidence in a secure area from temperature and humidity extremes. Protect it from magnetic sources, moisture, dust and other harmful particles or contaminants. Be aware potential evidence such as data, dates, times and system configurations may be lost as a result of prolonged storage. Since batteries have a limited life, data could be lost if they fail. Therefore, appropriate personnel shall be informed a device powered by batteries is in need of immediate attention.
- M.** Interview the suspect and all computer users. Obtain information such as:
1. Owner and/or users, and logon screen names and passwords.
 2. File and software security passwords.
 3. Purpose of the system.
 4. Any unique security schemes or destructive devices.
 5. Any offsite data storage.
 6. Email accounts, including user names and passwords.
 7. Any file sharing programs installed, and their use.
- N.** Any of the measures listed above that are employed at the scene to preserve or collect evidence from device capable of storing electronic data shall be documented (i.e. device was powered down, the device was unplugged while running, the device was packaged in a metal can, etc). A person certified as a computer forensic examination shall be used to

examine electronic devices capable of storing electronic data that is seized as evidence.

- O. When possible, a copy of the hard drive shall be made before examination. The original shall be placed in secure storage and the copy used for examination purposes.
- P. The appropriate prosecuting attorney shall be consulted prior to any examination of electronically stored evidence to determine if a search warrant is appropriate.
- Q. Any computer or other electronic device forfeited to the Department shall have its hard drive cleared and other data removed prior to being placed into service or sold.

XIII. Procedure: Recovered Stolen Vehicles

- A. When a vehicle is recovered by the Department, which was reported stolen by another jurisdiction, the following procedures shall be followed:
 - 1. The officer handling the recovery shall secure the vehicle and initiate action to notify the originating agency. Once notified, the originating agency shall be given the following options:
 - a. Request the vehicle be impounded by the Department's tow service.
 - b. Request an officer stand by until the originating agency's tow service arrives and takes control of the vehicle.
 - c. Request an officer stand by until an officer from the originating agency or the owner respond to the scene and takes control of the vehicle.
 - 2. Upon special request by the originating agency and with approval of the supervisor in charge, the vehicle may be towed to the Urbandale Police Department or another secure facility and processed by a CSI from the Urbandale Police Department. The supervisor shall only allow this request if the vehicle in question is involved in crimes of a serious nature such as person crimes or other ongoing criminal activity.
- B. When a vehicle is recovered by the Department or another jurisdiction which was reported stolen to the Urbandale Police Department, the following procedures shall be utilized:
 - 1. If the vehicle is involved in crimes of a serious in nature such as persons crimes or other ongoing criminal conduct, the following action shall be taken:
 - a. If recovered in the metro area, the vehicle shall be towed to the Urbandale Police Department and secured in sally port #2 for CSI processing.
 - b. If the vehicle is recovered outside of the metro area, a request shall be made to the Department recovering the vehicle to have a CSI process the vehicle.
 - c. If it is known in advance the Department is requesting to process a stolen vehicle upon recovery due to its connection to other crimes, it shall be the case detectives responsibility to include the request

on the Iowa/NCIC entry clearing stating the need for CSI processing.

2. If the vehicle is not known to be involved in any crimes of a serious nature such as person crimes or other ongoing criminal conduct, the following action shall be taken:
 - a. If recovered in the metro area, the on-duty supervisor shall attempt to notify the owner of the vehicle to respond to the scene to take possession of the vehicle. If the owner is not available, the on-duty supervisor shall request the vehicle be impounded by the Urbandale Police Department's tow service to the tow service's lot. Patrol shall complete all needed reports for the recovery and impound. If contact was not made with the owner, the on-duty supervisor shall notify the case detective. The case detective shall be responsible for notifying the owner and ensuring the vehicle is returned as soon as possible.
 - b. If recovered outside the metro area, the on-duty supervisor shall request the agency impound the vehicle. The on-duty supervisor shall notify the case detective of the recovery and the Patrol Division shall complete a supplemental report detailing the recovery of the vehicle. The case detective shall be responsible for notifying the owner so they may make arrangements to recover their vehicle.
 - c. Upon returning a stolen vehicle to the owner, any item within the vehicle identified as not belonging to the owner shall be seized and packaged as evidence by the officer or detective handling the release. The case detective shall evaluate the recovered items for evidentiary value and further testing (DNA, latent prints) as part of their case investigation.

XIV. Procedure: Evidence Packaging

- A. When any item of evidence is recovered, department personnel shall utilize the following procedures:
 1. When practical, the item will be placed in a suitable container or packaged appropriately (e.g. evidence envelope, brown paper bag, cardboard box, plastic bag, etc.).
 2. The type of packaging used will be subject to the nature, size, and condition of the physical evidence.
 3. Employees shall rely on the recommendations by experts in the field and instruction received through training in determining which type of packaging is best suited for the type of evidence being processed.
 4. After the item is packaged or placed in a suitable container, the package or container shall be sealed.
 5. All items shall be labeled or tagged with the recovering officer's name, case number, item number, and the date of recovery.
- B. Except as noted in this policy, evidence shall not be left unsecured once it is identified as having value to a criminal case.

- C. When an item is seized or recovered, it shall be entered into the evidence management software system and a property report shall be saved to the property in-box.
- D. A record will be made each time a transfer in custody of evidence takes place. The appropriate section of the property report, "chain of custody" in the evidence management software system will be utilized for this purpose.

XV. Procedure: Suspected drugs

- A. Any substance encountered that is suspected of being an illegal drug shall only be collected after donning the proper personal protective equipment (PPE). Based on the circumstances, PPE may include nitrile gloves, eye protection, breathing mask, paper suit, and shoe covers. If an officer does not have the proper PPE, CSI personnel may be requested to assist in properly securing and packaging the substance.
- B. The use of field testing kits to make a preliminary determination of the type of drug encountered shall only be allowed when using proper PPE to include at a minimum protective nitrile gloves.
- C. The evidence processing area and the CSI lab are the only approved areas within the police facility authorized for field testing of suspected drugs. Upon completion of field testing, the area utilized will be immediately and thoroughly cleaned.
- D. Upon completion of field testing or immediately if exposure occurs, employees shall wash their hands and remove and launder any contaminated clothing. Soap and water shall be used to clean hands or any contaminated skin as hand sanitizers and bleach solutions may make it easier for substances to be absorbed through the skin.
- E. Field testing outside of the police facility shall not occur within a patrol vehicle due to contamination risk.
- F. Only field test kits purchased by the Department shall be used to field test unknown substances suspected of being illegal drugs.
- G. Proper weighing and labeling of suspected drugs shall follow the procedures in Chapter 9 Section 84.1.1 (Property Evidence Control).
- H. Training on the use of field testing drugs shall be completed during the FTO process.
- I. Fentanyl-
 - 1. Any suspected fentanyl or related analogs shall only be handled after donning the appropriate PPE. At minimum, 2 pair of nitrile glove shall be utilized. The state in which the substance is found will determine the level of protection needed. If the substance is contained, 2 pair of nitrile gloves may be sufficient. If the substance is not contained, breathing and clothing protection may be warranted.
 - 2. Any person with exposure shall immediately clean contaminated skin with soap and water and removed contaminated clothing items.
 - 3. During the collection and handling of fentanyl or related analogs, a NARCAN kit shall be immediately available in case of accidental exposure.

4. Any substance suspected to contain fentanyl or fentanyl related analogs shall not be field tested due to the extreme risk that is caused by minimal exposure.
5. Suspected fentanyl or related analogs shall be double bagged, sealed, and be prominently labeled on the package with a bio hazard and fentanyl label to mitigate exposure risk. The evidence software system shall also note the substance is suspected to be fentanyl or a related analog.
6. Any PPE utilized to secure fentanyl or related analogs including any cleaning towels/items shall be properly disposed of in an approved bio hazard red bag.

XVI. Procedure: Laboratory Analysis

- A. Periodically, it may be necessary to submit recovered items of evidence to the Division of Criminal Investigation State Crime Laboratory or other accredited private laboratory for analysis, comparison, or processing. It will be the responsibility of the assigned case officer/investigator or the prosecuting attorney to determine if it is necessary to submit evidentiary items to the crime laboratory. When submission of an item for laboratory testing will be billed to the Department, a supervisor shall approve prior to submission.
- B. When the determination has been made to submit evidence to the Division of Criminal Investigation (DCI) State Crime Laboratory, the item(s) of evidence may be transported and submitted in person by the property/evidence officer or any other officer keeping in mind the fewest transfers of the item in the chain of custody is preferred. When items are submitted to any other laboratory, the property/evidence officer shall be responsible for submission. Proper chain of custody documentation must be completed for each officer handling the item. Prior to high risk items being removed from evidence to be submitted for laboratory testing, a supervisor shall verify the request for laboratory submission. Prior to being returned to evidence, high risk items submitted for laboratory analysis shall be verified for content and proper documentation by a supervisor. High risk items are defined as controlled substances, currency, firearms, and any other exceptional, valuable, or sensitive items contained within the secure room within the property evidence storage area.
- C. Items submitted for laboratory testing shall be packaged and submitted as requested by the laboratory. The Department reserves the right to go beyond the requirements of the laboratory to meet chain of custody and security concerns. Packaging for submission to a laboratory shall use the following methods:
 1. The original evidence packaging used to seal the container/package shall be left intact. The laboratory shall be responsible for breaking the evidence seal on the evidence package to perform testing following accepted procedures.

2. If hand delivered to the DCI laboratory, no additional packaging beyond the original sealed package is required.
 3. Evidence may be shipped to an outside laboratory by secure delivery service such as United States Mail, FedEx, or United Parcel Service. If mailed to the laboratory, the evidence shall be placed in a secure outer package. The outer package shall be sufficient enough to ensure the evidence arrives free from damage. The outer package shall be as generic as possible to decrease the chance of tampering while in transit.
- D.** Items submitted for laboratory testing shall be accompanied by the proper documentation requested by the laboratory. At minimum the item submitted shall contain a description of the item, submitting agency name, return address, contact person, and the analysis, examinations, and testing to be performed. The Department shall document all chain of custody events associated with a laboratory submission on the appropriate property report or controlled in the evidence management software system. The property/evidence officer shall package the evidence for shipment and sign the chain of custody, include date, time, and item numbers indicating which delivery service is used. A copy of the delivery service's air billing or shipping label will be maintained so the item can be tracked. A signed delivery receipt shall be requested and when obtained, placed in the case file.
- E.** Upon completion of testing at the DCI state crime laboratory, an officer shall be assigned to retrieve the item and return it directly to property/evidence at the Department using approved procedures. When possible, the officer that submitted the item to the laboratory shall be utilized to retrieve the item and return it to the Department lowering the number of officers involved in the chain of custody.
- F.** Regardless of the facility utilized, a receipt to ensure maintenance of chain of custody shall be obtained when an item is submitted to and returned from a laboratory.
- G.** All laboratories are required to provide the Department with a written report on all analysis, examinations, and tests conducted. When received, a copy shall be distributed to the appropriate investigator or prosecuting attorney and a copy shall be added to the original case file.
- H.** Submission of DNA evidence to an accredited laboratory shall follow the same procedures as outlined above. In addition the following procedures shall be followed:
1. Submission of DNA evidence must ensure the item will not be exposed to extreme heat while transporting (e.g. hot car)
 2. Submission must ensure the item will not be exposed to the environment as contamination may occur.
 3. It is preferred DNA evidence be hand delivered to an accredited laboratory. If this is not feasible, the laboratory shall be contacted and proper packaging and shipping procedures for submission that are requested by the laboratory shall be followed.

Chapter 9: Auxiliary and Technical Services
Section 84: Property and Evidence Control
Subsection 1: Administration and Operation



Policy/Procedure #: 1

Title: Property and Evidence Control

CALEA Reference#: 84.1.1, 84.1.2, 84.1.3, 84.1.4, 84.1.5, 84.1.6, 84.1.7, 84.1.8

I. Policy: Property and Evidence Control

The property and evidence control function shall provide for the security and control of seized, recovered, evidentiary, abandoned, or found property in the custody of the Urbandale Police Department. It is critical the department's property and evidence control maintain strict accountability for the receipt, handling, security, and disposition of property and evidence.

II. Procedure: Definitions

- A.** Evidence is any property which is relevant in a criminal prosecution or investigation.
- B.** Contraband is property that is illegal for a citizen of the state of Iowa to possess.
- C.** Found property is any property having no evidentiary value, which comes into the custody of the department and whose rightful owner may or may not be known.
- D.** Safekeeping is any property of no evidentiary value surrendered to the department for temporary custody with the understanding the person surrendering the property has the legal right to do so, and the property will be returned to the rightful owner(s) at the end of the specified period of time, unless disposal by the department, in a manner prescribed by law, is requested by the owner(s). Additional requirements for the return of firearms are stated in this policy.
- E.** Property for destruction is any property, including firearms, released by a citizen to the department so the property can be destroyed.
- F.** Confiscated property is any property seized by department personnel, which is held so the property's relevance as evidence can be determined.
- G.** Property/Evidence personnel is either the designated property/evidence officer or the designated Support Services Division supervisors.

III. Procedure: General

- A.** All property seized or placed in control of department personnel shall be logged into agency records prior to the employee ending their shift.

- B.** All property seized or placed in control of department personnel shall be logged into property/evidence control prior to the employee ending their shift. Detectives and crimes scene investigators (CSI) must secure all evidence in a locked area or safe with controlled access at their respective facility and have items under their control logged on a property sheet prior to ending their shift. Under no circumstances are any employees allowed to place property in the department locker rooms, bring property to their home, or retain property in their vehicle other than for pending transport.
- C.** All property seized or placed in control of department personnel shall be entered in the property/evidence control system as soon as practical and include a report detailing how the property came into the employee's possession along with a description of each item seized. Exceptions to entering property/ evidence into the property evidence control system are as follows:

 - 1. In cases where the stolen property has already been recovered by the victim and department personnel have never actually taken control of the property (e.g. shoplifting from Kohl's, etc.), the employee shall list the items in the incident report. In most cases there would be no need to list these items with the property/evidence control system.
 - 2. In cases where an individual's personal effects are temporarily seized during the booking process.
- D.** All property seized or controlled by the department shall be stored within designated secure areas. Below is a list of secure areas utilized by the department and persons with access:

 - 1. Property/evidence storage lockers. All department personnel have access until locker is secured then only property/evidence personnel have access.
 - 2. Property/evidence room. Only property/evidence personnel shall have access to the outer and inner secure area. Anyone accompanying property/evidence personnel into the room shall be noted on an entry log and be supervised by property/evidence personnel at all times.
 - 3. Department crime laboratory. Only department CSI personnel shall have access to the room. Anyone accompanying CSI personnel into the room shall be noted on an entry log and be supervised by CSI personnel at all times.
 - 4. Secure lockers within the Investigation Division. The lockers shall be utilized for temporarily securing property/evidence while investigators process and/or examine the items. Once an investigator has completed processing and/or examining a property/evidence item, it shall be placed in property/evidence control as soon as possible. The lockers will be secured by specific locks issued to each detective. The Investigation Division Commander shall also have access to the lock keys.
 - 5. Secure areas within the Mid Iowa Narcotics Enforcement (MINE) Drug Task Force office. The secure areas listed below shall be utilized for temporarily securing property/evidence while investigators process

and/or examine the items. Once an investigator has completed processing and/or examining a property/evidence item, it shall be placed in property/evidence control as soon as possible.

- a. Individual lockers- Lockers are located in the secure room within the MINE office. Each detective assigned to MINE shall have their own lock and key to use on a locker making it accessible to only the detective and the MINE commander. The secure room housing the lockers shall have video surveillance.
 - b. Individual safes- Detectives assigned to MINE shall also be assigned a small safe. The safe shall be located in the secure room within the MINE office. The safe shall have a unique access code known only to the detective. The secure room housing the safe shall have video surveillance.
6. Secure room within the secure area of the property/evidence room. This room is designated for storage of controlled substances, firearms, currency, and any other exceptional, valuable, or sensitive items. Property/evidence personnel shall have access. Access to the secure room shall only be made when two property/evidence personnel are present. The two property/evidence personnel can be any combination of the property/evidence officer, the Support Services Division Sergeant, or the Support Services Division Commander. Electronic key cards shall be utilized to gain access. All items placed in the secure room shall be verified by both parties. When removing an item, the reason for removal shall be verified by two property/evidence personnel. Verification shall include reviewing appropriate documents necessitating the removal (lab request, subpoena, etc.) The verifying property/evidence personnel and the reason for removal shall be listed in the property/evidence control system.
7. Secure mailbox in the department's northeast parking lot. The mail box shall be accessible to all department personnel to deposit fireworks through a "drop box" system. The mailbox shall be secured by two locks. Key to one lock shall be retained by the property/evidence officer and key to the other lock shall be retained by the Support Services Division Sergeant and the Support Services Division Commander.
8. Secure storage container located at the public works facility. The storage container shall be utilized to hold large items. No exceptional, valuable, or sensitive items shall be stored in the container. The secure storage container is secured by two (2) different locks. The key to one lock shall be retained by the property/evidence officer and the key to the other lock shall be retained by the Support Services Division Sergeant and Support Services Division Commander.
9. Secure storage in sally port 2: When a vehicle or other item too large to store in an evidence locker and property/evidence personnel are not available, the item shall be secured in sally port 2. Sally port 2 shall be configured to allow department personnel to secure a large item and

restrict access to only property/evidence personnel. The item shall be removed from sally port 2 as soon as alternative secure storage for the item can be arranged.

- 10. Secure rental unit:** A secure rental unit shall be acquired to secure large evidence items only when no practical alternative storage is capable. No exceptional, valuable, or sensitive items shall be stored in a secure rental unit. The rental unit shall be secured with a cut resistant lock. Only property/evidence personnel shall have access to the secure rental unit. When utilized, the secure rental unit shall have documented monthly inspections by the property/evidence officer to ensure it has not been compromised. Any secure rental unit being utilized during a period when an inspection of property evidence is being conducted shall be included in the inspection to ensure it has not been compromised and security measures are in place. The storage unit facility shall have the following security features:

 - a.** Restricted access to the storage units
 - b.** Video surveillance of the storage units
- 11. Secure storage area located at a contracted tow service:** The secure area will be utilized to hold vehicles that are impounded as the result of police action or as abandoned property. Vehicles held as evidence shall not be taken to or stored at the tow service. The tow company shall have a secure lot to ensure no unattended persons have access to the vehicles during or after business hours.
- 12. Secure vehicle lot:** The secure vehicle lot will be utilized to hold vehicles that are impounded as the result of police action or due to abandonment. After all evidence processing procedures have been completed, vehicles held as evidence may also be stored on the secure vehicle lot. Only property/evidence personnel shall have access to the secure vehicle lot.
- 13. Secure hasp in the covered parking area:** The secure hasp shall be available for use by department personnel to secure found property that is too large to be placed in property evidence storage locker and is able to be secured by a hasp/chain lock. The secure hasp shall not be utilized for evidentiary items. The secure hasp shall only be utilized during non-business hours or when property evidence personnel are not available to secure the item. Once secure, only property evidence personnel shall have access to remove the item. Upon notice, property evidence personnel shall move the item to the property evidence room as soon as possible.
- E.** From the time of seizure or control until the final disposition, chain of custody shall be meticulously maintained. The department's property/evidence control system shall maintain current information on the location and status of all property in its control.
- F.** Controlled substances procured, seized, forfeited, or abandoned to the department shall not be utilized for training purposes. Any controlled substances utilized for canine training shall be obtained from the Drug

Enforcement Agency as established in Chapter 5 Section 41.1.4 of the Operations Manual.

- G.** After receiving the approval of the Investigation Division Commander and upon receipt of a court order, controlled substances procured, seized, forfeited, or abandoned to the department may be utilized for investigative purposes. The use and chain of custody shall be documented in the case file in which the controlled substances are utilized.
- H.** All weapons meeting the submission requirements for National Integrated Ballistic Information Network (NIBIN) testing that are held as evidence or for forfeiture by the department shall be submitted to the DCI laboratory or other approved NIBIN testing agency for testing and entry in the NIBIN data base.
- I.** Weapons procured, seized, forfeited or abandoned to the department shall be submitted to the Iowa Department of Criminal Investigations laboratory for destruction. If a need exists, a seized, forfeited or abandoned weapon may be utilized for training and limited use by the department after being submitted to the DCI laboratory. All documents detailing how the weapon was acquired and the approval process shall be maintained in the original case file in which the weapon was seized. Weapons utilized for training and limited use by the department shall meet the following requirements:
 - 1.** Approval of the Chief of Police
 - 2.** Approval of the Iowa Division of Criminal Investigations Crime Laboratory including documentation stating the laboratory has allowed the department to maintain the weapon for training and limited use.
 - 3.** Proper documentation in the original case files showing the disposition of the weapon.
 - 4.** Inspection of the weapon by a certified armor to ensure the weapon is safe and functioning properly.
 - 5.** Entry of the weapon into the department's firearms inventory. The inventory entry shall contain the original case number which the weapon was seized to ensure documentation of the weapons origin is readily available.
 - 6.** Once listed in the department inventory, the weapon shall be stored in the department's gun vault and included in any department weapons inventory.
 - 7.** Firearms instructors may utilize the weapon for any authorized firearms training. If the weapon is to be issued to an officer for temporary use, approval must be obtained from the Range Administrator. Upon approval, the weapons inventory shall indicate the officer in possession of the weapon.

IV. Procedure: Property Packaging

- A.** All property must contain a proper label generated from the property/evidence control system. Items without a proper label shall require the submitting employee to correct before it will be accepted into the property/evidence control system.

- B.** Department personnel taking custody of any property/evidence shall submit said item in the appropriate packaging.
- C.** All items shall be sealed in an appropriate plastic bag, sack, box, or other container based on the type of property/evidence being submitted. When needed, evidence sealing tape shall be utilized to seal all receptacles containing evidence. A supervisor or the property/evidence officer may grant exceptions for large items. All seals shall be initialed or signed by the submitting officer or crime scene investigator and include the date the item was sealed and initialed/signed.
- D.** Property items that are exceptional, valuable, or sensitive in nature shall be sealed in an appropriate package. Once entered into property evidence control, exceptional, valuable, or sensitive in nature items shall have controlled access with a minimum of two (2) levels of security to gain access. This shall include but not be limited to:
 - 1. Currency
 - 2. Jewelry of significant value
 - 3. Controlled Substances
 - 4. Firearms
- E.** Any item containing a bio-hazard shall be labeled as such using the appropriate bio-hazard labels. Any item that has the potential to become a safety hazard (e.g. broken glass, knives, etc.) shall be packaged (e.g. protective box, metal can, etc.) and labeled (e.g. caution- broken glass) in a manner that prevents the item from injuring personnel that will be handling the item. Any glass items not broken when seized shall be sufficiently protected (e.g. bubble wrap or other protective covering) to prevent breakage during the property/evidence process as broken glass is a safety hazard to property/evidence personnel.
- F.** Vaporizing devices shall have all batteries removed and placed in separate packaging within the main package to prevent combustion of the batteries or activation of the device during storage. If the battery is unable to be removed, the vaporizing device must be stored outside of the building in the secure mailbox to prevent a fire hazard. Batteries on all other devices shall also be removed and packaged separately within the main package when easily accessible but will not require outside storage if the batteries are not able to be removed.
- G.** Syringes and broken glass or ceramic drug pipes that are a sharps hazard shall not be retained. Personnel shall photograph the syringe or broken pipe and cautiously dispose of it in the appropriate sharps container. Another employee shall witness the destruction and be listed in the appropriate report as the witness. In the rare incidents where a syringe or broken drug pipe needs to be retained for a case investigation (e.g. fingerprint for a death investigation, etc.), it shall be packaged in a cylinder tube (syringe) or appropriate box (broken pipe) sealed and marked as a bio hazard. If fluid inside of a syringe needs to be retained, it shall be transferred into a sterile vial utilizing the utmost caution after obtaining

supervisory approval. The supervisor shall visually observe the transfer to ensure the utmost caution and protective gear is being utilized.

H. Controlled substances:

1. Controlled substances must be packaged separately from other items.
2. When different types of controlled substances are found together, they shall be packaged separately by type.
3. Paraphernalia shall also be packaged separately from the controlled substance.
4. Once packaged appropriately, the submitting employee shall initial and date the evidence seal. Controlled substances without initials and date on the seal of the packaging will not be accepted into the property/evidence control system.
5. Department personnel are required to obtain a gross package weight of controlled substances seized and enter the information in the property description field in the property evidence control system. The gross package weight is the weight of the item and all packaging needed to enter the item into property/evidence control except the label. The scale provided in the evidence processing room shall be utilized to determine gross package weight. The gross package weight of all controlled substances will be verified by two (2) property/evidence personnel prior to entry into the drug storage area utilizing the scale provided in the evidence processing area. If there is a significant discrepancy (more than 2 grams) in the gross package weight submitted by the employee and the verification by the property/evidence personnel, the scale will be tested for proper functioning and accuracy. If the scale is functioning properly, the item will not be accepted and the employee and their supervisor will be notified by property/evidence personnel. If the scale is not functioning properly, property evidence personnel shall require the employee to resubmit the controlled substance using a properly functioning scale.
6. If controlled substances submitted by MINE detectives are weighed on a scale other than the one being utilized in the evidence processing area to calculate the gross package weight, the package shall have two (2) verifying employees' initials and the date on the seal of the evidence packaging. The submitting detective shall identify the names of the detectives that verified the gross package weight of the controlled substance in their report. If weighed on a different scale than the one provided in the evidence processing area, controlled substances submitted by MINE detectives without two (2) employees' initials and date on the seal of the packaging will not be accepted into the property/evidence control system.

I. Controlled substances may be used for investigative or training purposes on a very limited basis under the following conditions:

1. Use must receive written approval of the chief of police or a division commander.

2. A court order signed by a judge must be obtained prior to use if the controlled substance was previously evidence in a criminal prosecution.
 3. Only controlled substances from cases that are no longer active and would qualify for destruction shall be utilized.
 4. A report documenting the conversion with a detailed chain of custody must be kept within the original case file relating to the seizure of the controlled substance and within any new cases generated from the use of the controlled substance.
 5. Once use of the substance for investigative or training purposes is no longer needed. The substance shall be returned to property/evidence ensuring proper chain of custody, documentation and packaging/logging requirements of this policy are met.
- J.** Currency must be packaged separately from other items. Prior to packaging, the currency shall be counted by the submitting employee and one additional employee to verify the total. The verifying employee shall be documented in the property/evidence control system. The total amount of currency shall be entered into the property/evidence control system and printed on the label. Once sealed, both counting employees shall initial and date the seal of the package. If the currency package does not contain two signatures, it will not be accepted by property/evidence personnel. If final disposition has not been obtained within thirty (30) days, all currency seized shall be deposited with the city of Urbandale finance department into a specific account to hold the funds until final disposition. If a prosecuting attorney makes a request in writing the actual currency be held for court, the currency shall not be deposited into the holding account with the City.
- K.** Alcoholic beverage containers shall not be placed in property/evidence storage. Department personnel are required to photograph the containers and destroy them. A supervisor or other employee shall witness the destruction. Documentation of the destruction, including identification of the employee witnessing the destruction, shall be included in the report. Exceptions to destruction of alcoholic beverage containers shall be granted for major investigations (e.g. vehicular homicide) and/or when the alcohol container needs to be processed for other evidence (e.g. fingerprints, DNA, etc.).
- L.** Firearms shall be secured with plastic ties unloaded within a firearms packaging box. The firearm must not have any ammunition in the chamber or attached magazines. When the make of the firearm allows, a plastic tie shall be used to maintain the breach in an open position. Plastic ties shall also be used to secure the firearm to the box. Firearms seized with a case may remain in the case with a label attached to the outside. At no time shall ammunition be loaded in a firearm, a firearm's case, or a property box containing a firearm when entered into property/evidence control. All ammunition shall be packaged separate from the firearm.

M. Explosives procured, seized, forfeited, or abandoned to the department shall not be entered into property evidence control and/or used for departmental investigative or training purposes. Any device that is believed to be an explosive, shall be treated as such and handled or transported only by those who have been trained in the handling, safe destruction, or transportation of such devices. All fireworks seized shall be listed in a case report with an accompanying property sheet. Fireworks seized by department personnel shall be photographed at the scene and transported in the trunk of police vehicle directly to the department. Extremely large fireworks or an extremely large number of fireworks shall require extra precautions and shall not be transported in a police vehicle. Once at the department, the fireworks shall be deposited in the secure container located in the north east corner of the north parking lot for destruction. When needed, the property/evidence officer shall contact the State Fire Marshal for destruction or submit the fireworks to the DCI for destruction. Turning over the fireworks to the State Fire Marshal or the DCI for destruction shall be witnessed by two (2) property/evidence personnel. The property/evidence officer shall detail the release for destruction to the State Fire Marshal or DCI, including the verifying official's information, in the property/evidence control system.

V. Procedure: Property submission

- A.** All items submitted by department personnel for entry into the property/evidence control system shall be placed in the secure lockers in the evidence processing room or directly to property/evidence personnel with the following exceptions:
1. Vehicles or other large items held as evidence shall be placed in sally port #2 and secured. If sally port #2 is unavailable, property/evidence personnel shall respond to assist in securing the item.
 2. Evidence items that require refrigeration or freezing shall be properly packaged and immediately transferred to property/evidence personnel for storage. If the seizure occurs when property/evidence personnel are not on duty, seizing personnel shall secure the item in a property/evidence locker and make phone contact with property/evidence personnel to make arrangements to properly store the item.
 3. With supervisory approval, property may be directly submitted to the Division of Criminal Investigation laboratory by the investigating officer or crime scene investigators.
 4. If able to be secured by a hasp/chain lock, found property that is too large to be placed into a locker may be secured to the hasp in the covered parking area (e.g. found bicycles).
- B.** Detectives, CSIs, and DREs shall be responsible for completing the Iowa Division of Criminal Investigation (DCI) laboratory receipt form for any evidence that will be submitted for examination by the laboratory. This form shall be placed with the evidence that is being submitted for examination. The property/evidence officer shall be responsible for

completing the DCI laboratory receipt form for patrol officers submitting evidence for examination by the laboratory. Property/evidence personnel shall be responsible for delivering and retrieving evidence at the D.C.I. laboratory. After an item has been submitted to property/evidence control, supervisory approval and verification must be obtained for detectives and CSI to submit and retrieve items from the DCI laboratory.

VI. Procedure: Identification/Notification of Owner/Custodian

- A.** A reasonable effort to identify and notify the owner or custodian of property in the department's control shall be the responsibility of the department personnel seizing the item and the property/evidence officer.
- B.** When the owner/custodian of seized property is known and readily available to the seizing personnel, they shall be provided a copy of the property sheet listing all items seized along with instructions on how to claim their property as provided by Iowa Code 809.3. When the owner/custodian is not readily available, the property/evidence officer shall attempt to provide this information at a later date.
- C.** Property that is found and has no value to a criminal incident shall be returned to the owner as soon as practical. When the property is not immediately returned, the seizing personnel shall log the property into the property/evidence control system and the property/evidence officer shall send notification to the owner/custodian.
- D.** Any property having a serial number shall be queried by seizing personnel through the IOWA/NCIC system to determine if it has been entered as stolen. In the event the seizing personnel is unable to do so, the employee shall indicate in a supplemental report the serial numbers have not been queried and notice will be given to the property/evidence officer. The property/evidence officer shall ensure the serial numbers are queried and add documentation to the case file indicating the items have been checked. When the item is reported as stolen, the detective assigned to the recovered stolen case shall be responsible for contacting the owner of the property. For recovered stolen vehicles, see Chapter 9 Section 83.1.1 of the Operations Manual.
- E.** If property is seized and forfeiture of the property will be sought, the investigating officer is responsible to serve the "Notice of Seizure for Forfeiture" form to the owner or claimant of the property. The form shall be sent to the appropriate county attorney's office along with a copy of the case. A copy of the form shall be placed in the main case file and a copy forwarded to the property/evidence officer.
- F.** The property/evidence officer shall ensure any items that become property of the department through civil or forfeiture process meet all State of Iowa requirements and are properly documented in the original case file. MINE Task Force personnel shall ensure any items that become property of the MINE Task Force through civil or forfeiture process meet all State of Iowa requirements and are properly documented in the original case file.

VII. Procedure: Release of Items from Property/Evidence

- A.** To release property or evidence for any reason to another party after entry into the property/evidence system the following procedure shall be required:
1. Only property/evidence personnel are authorized to release property/evidence once entered into the Urbandale property /evidence control system. Detectives are also allowed to release property/evidence items. They must obtain a signed receipt along with the name of the person accepting the evidence, date of release, time of release, the reason for release, and the detective releasing the item for the case file. Documentation shall also be entered in the property/evidence control system referencing the case file receipt.
 2. No property or evidence will be released without proper authority and identification. If there is a question as to proper authority or identity, written documentation and/or photo identification shall be required and placed in the case file.
 3. A signature must be obtained from the party accepting the property/evidence. The signature may be obtained on a printed paper receipt from the property evidence control system or by utilizing the electronic signature capabilities of the property evidence control system. In addition to the signature, the specific item being released, the name of the person accepting, the date of release, the time of release, the reason for release, and the name of the person releasing the property shall be logged into the property evidence control system.
 4. Property shall be released to the public during normal business hours based on the availability of property/evidence personnel. Department personnel or others law enforcement officials needing property released shall make arrangements with property/evidence personnel.
 5. If the evidence items are turned over to the court or the prosecuting attorney's office, a signed receipt along with the name of the person accepting the evidence, date of release, time of release, the reason for release, and the person releasing the property shall be obtained and entered into the case file by the department personnel releasing custody of the item. Documentation shall also be entered in the property/evidence control system referencing the case file receipt.
 6. Items released to the Division of Criminal Investigation State Crime lab for analysis or destruction shall require a signature of receipt and other required information as stated above. The receipt produced by the crime lab shall also be entered into the case file.
 7. Items released for internal evidence processing shall be secured in the department crime lab by CSI personnel. If the item is continuously monitored by the CSI personnel having custody, forensic examination of items outside the lab is acceptable.
- B.** Sworn personnel shall have the authority to remove items from the property/evidence control system for the following activities:
1. For use in a criminal or civil court proceeding.

2. For investigative purposes. This would include submission to the DCI or other accredited laboratories and/or in-house analysis.

VIII. Procedure: Length of Time Property is to be Held

- A. Final disposition of property held by the department shall be accomplished within six (6) months after all legal requirements have been met.
- B. Property held in criminal cases with the following dispositions shall be held as follows:
 1. Cleared by arrest – Property will be held until 60 days after the last defendant's court case verdict is determined and no appeals have been filed.
 2. Suspended – Property will be held until the statute of limitations has expired. See the Code of Iowa, Chapter 802.
 3. Exceptionally Cleared –
 - (a) Property will be held for one year after the case status is classified as exceptionally cleared.
 - (b) An exception is noted for sex abuse cases classified as open, suspended, or exceptionally cleared where an alleged victim of sexual abuse has made a report, but declines cooperate with the prosecution or for some other reason the case has not moved forward:
 - (1) When the victim is under eighteen (18) years of age at the time of the assault, the sexual abuse evidence kit and any other evidence shall be kept in property/evidence storage indefinitely or until meeting the requirements of Iowa Code 709.10 and Iowa Code 802.2.
 - (2) In cases where the victim of a sexual assault is eighteen (18) years old or older, the property in a sexual assault case shall be held indefinitely unless meeting the requirements of 709.10 and Iowa Code 802.2.
 - (3) All requirements of Iowa Code 709.10 shall be met by the department for all property related to a sexual assault case to include sexual assault kit tracking within the designated system, required timelines, notification to victims prior to disposal, and written county attorney approval for destruction.
 - (c) All sexual abuse evidence kits shall be submitted to the DCI laboratory or other approved laboratory for analysis regardless of the status of the case. If there is overwhelming evidence a sexual assault did not occur, the Investigation Division Commander or designee may determine a sexual assault kit should not be submitted for analysis. If the sexual assault kit is not submitted for analysis, the investigator shall note the decision in their final supplemental report.
- C. In death investigations involving homicide or suspicious circumstances, the property from the case shall be held indefinitely or until county attorney and supervisor approval to dispose is obtained. In death investigations involving natural causes, suicides, and accidental death, evidence shall be

held for one year. All photographic media (e.g. negatives, digital photographs, video etc.) shall be held indefinitely.

- D. Found property or property turned over to the department for destruction shall be held for ninety (90) days after receipt.
- E. Property that has been confiscated shall be handled as follows:
 - 1. Disposed of any time after the property is determined to have no evidentiary value.
 - 2. Property held for safekeeping shall be disposed of thirty (30) days after receipt.
- F. Any property may be released to the owner prior to the above time periods for the following reasons:
 - 1. When approval is granted by the prosecuting attorney's office with jurisdiction over the matter. In such cases the property will be photographed prior to its release.
 - 2. When the property no longer has relevance as evidence as determined by the case officer, a supervisor, and the appropriate prosecuting attorney (if applicable).
 - 3. When the property is unusual in value, size, or is potentially hazardous, such that the property cannot be safely stored at the Urbandale Police Facility building. Approval will be obtained from the appropriate prosecuting attorney and the item shall be photographed prior to its final disposition.
 - 4. When storage of the property will cause undue hardship for the owner of the property. Approval will be obtained from the appropriate prosecuting attorney and the item shall be photographed prior to its final disposition.

IX. Procedure: Review of Property

- A. When property has been held for the length of time specified above, the following steps shall occur prior to any disposition:
 - 1. Any property having a serial number will be queried through the IOWA/NCIC system to determine if the property has been entered as stolen.
 - 2. An ATF Gun Trace request will be sent on all firearms and a response received before disposition.
 - 3. The case file will be reviewed to determine:
 - a. All suspects have been arrested.
 - b. All criminal court proceedings including appeals are complete. Each defendant's court status will be verified with the county Clerk of Court and/or the prosecuting attorney.
 - c. Determine if any claims have been made for return of the property.
 - d. Determine if any forfeiture proceedings have been filed.
 - e. Determine if any civil proceedings have been filed.
 - f. Determine any ownership of the property.
- B. The review of property function shall be the responsibility of the property/evidence officer or designee.

- C. Prior to the final disposition of any property associated with a crime or incident that is classified as a felony, a supervisor from the Support Services Division (general criminal cases) or the Investigation Division (Drug related cases) shall confirm the status of the case and the ability to move forward with the disposal of the property ensuring all criminal and civil proceedings are completed and all statutory requirements are met. Documentation of the supervisory review shall be placed in the case file.

X. Procedure: Property Disposition

- A. Property that is no longer needed for legal proceedings and is not contraband will be disposed of as follows:
1. If the owner has been given notice at the time of the seizure and has not filed a claim for the property; the property will be considered abandoned. If the owner of the property is known, entitled to the property, and the property has some value as determined by the property/evidence officer, a second notice shall be sent to the owner stating their rights to the property as stated in Chapter 809, Section 5 of the Iowa Code.
 2. If the owner is not known, or the property is abandoned, or the owner declines to retrieve the property, the property may be destroyed, sold at auction, sold utilizing the city approved web based auction, or the item may be condemned to the department, another city agency, or other appropriate agencies in accordance with state law.
 3. If a court order exists relating to the disposal of property, the order shall be obeyed.
- B. Contraband shall be destroyed in accordance with all city, state and federal laws by burning, crushing, or shredding under the direction of the property/evidence officer or by forwarding to the appropriate agency for destruction. Two department employees must be present to verify the destruction of any property from the property/evidence control. The name of the verifying employee must be documented in the case file.
- C. All controlled substances shall be destroyed by obtaining a court order for destruction. Two department employees are required to be present during the destruction of controlled substances. Documentation with signatures of both employees, including the date of the destruction, shall be placed in the case file.
- D. No firearm(s) will be released to a convicted felon. A family member or designee must take possession of a firearm belonging to a convicted felon, or juvenile. If a person appears to be an imminent danger to themselves or others, the department shall seek legal assistance in preventing or restricting the release of a weapon to the person.
- E. When the department is in control of found property with no connection to a criminal case, department personnel seizing the item or property/evidence personnel shall make reasonable efforts to identify and notify the owner, or other person entitled to possess the property. Department personnel or the property/evidence personnel shall return the

property after such person provides reasonable and satisfactory proof of ownership or right to possession.

- F. There are situations where an individual turns in found property or money to the department and the individual expresses an interest in claiming the property due to the identity and/or the location of the owner entitled to possession is unable to be ascertained. The person finding the item(s) shall be advised of the procedure set forth to claim the property as stated in chapter 556.F11 of the Code of Iowa.
 - G. If no owner is located for found property within the allotted time period and the finding party does not file a claim for return of the property, the property will be disposed by one of the following methods:
 - 1. Sold at auction or by approved bidding procedures.
 - 2. Condemned for use by a city or state agency.
 - 3. Destroyed.
 - H. Property that is being held for safekeeping shall be returned to the owner. The owner shall be notified as stated in Chapter 809, Section 5 of the Code of Iowa. If the owner declines to retrieve the property, the property may be destroyed, sold at auction, or the item may be donated to the department, a city agency, or other appropriate agency in accordance with state law.
 - I. The final disposition of all property shall be documented and placed in the main case file. The Support Services Division shall be responsible for any property designated to be sold at auction including all relevant documentation detailing the sale.
 - J. All property set aside for destruction will be rendered unserviceable by damaging, crushing shredding or disabling the property whenever possible. It shall then be placed in the department's trash disposal containers.
 - K. Any property condemned to the city for city use will be documented on a supplemental report and placed in the main case file.
 - L. Any employee or the immediate family member of an employee of the Urbandale Police Department shall be prohibited from purchasing either directly or indirectly any property that has been forfeited to the department due to a criminal investigation. This shall include any property forfeited to other law enforcement agencies where the Urbandale Police Department was involved (i.e. joint investigation) or to any investigative task forces in which the department participates (e.g. Mid Iowa Narcotics Enforcement Task Force).
- XI. Procedure: Inspections and Audits**
- A. Semi-annually the commander of the Support Services Division or designee shall conduct an inspection to determine if agency policy and procedure in regards to the department's property and evidence control system is functioning properly. The inspection shall include but not be limited to:
 - 1. Accounting for secured keys.

2. Inspection of all secure areas for properly functioning equipment and security (e.g. locks, cameras, etc.).
 3. Inspection of case files to determine if proper documentation has been entered.
 4. Review of supplies.
 5. A report by the property/evidence officer detailing any concerns with items submitted by personnel such as packaging and proper documentation.
- B.** When property/evidence personnel are assigned to and/or transferred from the Support Services Division the Chief of Police shall order a complete audit of all high risk items. High risk items are defined as controlled substances, currency, firearms, and any other exceptional, valuable, or sensitive items contained within the secure room within the property evidence storage area. The audit shall also include a minimum of 10% of the remaining property items. If discrepancies are found, the Chief of Police may require a full audit of all property evidence items.

The audit shall be completed by a supervisor designated by the Chief of Police and the newly assigned property/evidence personnel. The outgoing property/evidence personnel may facilitate the audit. Upon completion, the assigned supervisor shall submit a full report to the Chief of Police.

- C.** An annual audit of property under the control of the department shall be conducted by personnel designated by the Chief of Police. The appointed auditor shall not have any responsibility for property/evidence control function for the department and may be personnel from an outside agency. The annual audit shall consist of a complete audit of all high risk items. High risk items are defined as controlled substances, currency, firearms, and any other exceptional, valuable, or sensitive items contained within the secure room within the property evidence storage area. The annual audit shall also include a minimum of 10% of the remaining property.
- D.** At least annually, the Chief of Police shall request an unannounced inspection of property storage areas. The unannounced inspections shall concentrate on cleanliness, proper supplies, security, and proper documentation as well as inspection of all secure areas for properly functioning equipment and security (e.g. locks, cameras, etc.). The inspection shall also include the audit of a few items of property/evidence for location and proper documentation.



Departmental General Order

To: All Officers
From: Chief Johansen
Re: Issuance and tracking of paper citations
Date: 01-15-2021
Departmental General Order #: 2021-01

The following procedures shall be followed for the issuance and tracking of traditional paper citations:

A. Issuance:

1. When needed, a Support Services Division supervisor shall issue a booklet of paper citations to an officer for use. The citations booklets issued shall be the lowest number available. Officers issuing citations shall do so in consecutive order from the smallest number to largest number in their booklet.
2. After a citation has been issued by an officer, it shall be submitted to their supervisor for review. Upon completion of the review, the citation shall be submitted to the secure storage drawer located across from the departmental mailboxes by the reviewing supervisor.
3. Only Support Services Division supervisors, specialist, technicians, shall have access to the secure storage drawer to retrieve the citations for entry into the records management system and transmission to court or the city clerk.

B. Tracking:

1. The Support Services Division shall log all citations booklets issued in the Departmental inventory system to include the number sequence issued to each officer.
2. Citation booklets not issued shall be maintained in a secure location accessible only by Support Services Division supervisors.
3. Support Services Division personnel shall maintain a log for each officer issued a citation booklet for the purpose of tracking and auditing citations issued. The log shall contain the citation numbers issued to each officer and indicate if they have been issued. If a citation is voided for any reason, it shall also be noted on the log.
4. Upon entry into the log, Support Services Division personnel shall ensure the citation is in sequential order. If it is not in order, staff shall notify their supervisor who will in turn notify the affected officer's supervisor. A memorandum shall be drafted by the officer to their supervisor explaining why the citation is not in sequential order. A copy of the memorandum will be supplied to the Support Services Division Supervisor. If further action or investigation is warranted, the Support Services Division supervisor shall notify the Support Services Division Commander.

C. Voiding a Citation Prior to issuance:

1. If a citation is voided prior to issuance, the officer shall write "VOID" in large letters across the face of the citation. The officer will then add his initials and identification number.
2. All copies of the citation will be submitted to the officer's supervisor along with a verbal explanation of the reason the citation was voided. If the supervisor is satisfied with the explanation, they shall write "approved" on the citation and add their initials and identification number. The voided citation shall be submitted to the secure storage drawer for tracking and audit purposes.
3. If the supervisor is not satisfied with the explanation, they should place the voided citation in a secure location and require the officer to submit a memorandum explaining the situation that lead to them voiding the citation. The supervisor shall review the memorandum with the Division Commander and determine if further investigation or disciplinary action is warranted.
4. At the conclusion of the investigation, the voided citation shall be submitted to the secure storage drawer for tracking and audit purposes.

D. Voiding a Citation After Issuance

1. The procedure for voiding the citation after issuance shall be the same procedure outlined above for non-issued citations except as follows:
 - a. Approval must come from the Chief of Police. The Chief's initials and identification number shall be placed on the citation in lieu of a supervisor.
 - b. Supervisors may also request a citation be voided; however, the issuing officer shall be notified of the reason for voiding.
 - c. If the issued citation has been transmitted to court or the city clerk, the issuing officer shall be responsible for ensuring the court or city clerk are notified the citation has been voided.
 - d. The issuing officer or a supervisor shall be responsible for notifying the cited party the citation has been voided.
 - e. A memorandum detailing the approval to void the citation and verification the court or city clerk as well as the cited party have been notified. All copies of the citation retained by the Department shall be submitted to the secure storage drawer for tracking and audit purposes.



Departmental General Order

To: All employees
From: Chief Johansen
Re: Police ride along program
Date: 01-15-2021
Departmental General Order #: 2021-02

The following order is to standardize the ride along program.

The Department will allow the following persons to participate in the ride along program:

- Interns
- Officer candidates on the current Civil Service certified hiring list with permission of the Chief of Police or a Division Commander (Maximum of two 4 hour periods).
- Citizen Police Academy participants during academy participation segment.
- WestCom employees.
- Sworn officer family members (16 year of age and older, immediate family, one member per quarter year).
- UPD civilian staff as required by a division commander or the Chief of Police.
- Special circumstances (Chief's pre-approval required, media, city personnel, other L.E., etc.)

If meeting one of the requirements above, the shift supervisor should be notified at least one day prior to the shift in which the ride along will occur.

Shift supervisors shall note rider information to include the category above and the officer requesting (if appropriate) on roll call sheet for tracking purposes and compliance to this order.

All persons participating shall sign a waiver prior to riding. Completed original forms will be forwarded to Support Services Division for filing in Laserfiche.

UPD reserves are not restricted by this policy.



Departmental General Order

To: All Officers
From: Chief Johansen
Re: Uniforms
Date: 06-20-2025
Departmental General Order #: 2025-01

This order will replace divisional general order 2023-01.

Officers will report for duty with clean and pressed uniforms. Uniforms shall be replaced as needed or if directed by a supervisor. Unless an exception is granted by the chief of police, sworn officers working in uniform shall be restricted to the uniforms listed below.

Division commanders may allow sworn officers to wear civilian style clothing as appropriate to their assignment. Division commanders shall issue orders clearly stating acceptable dress requirements for sworn and civilian personnel in their division.

All officers, regardless of assignment, shall maintain at least one class A long sleeve uniform for differing assignments and ceremonial activities.

Support Services will maintain a master list of uniform and equipment approved brands, model numbers, and styles. Officers will only purchase uniforms and equipment that is on the approved master list. The chief of police or his designee can approve variances to the master list.

Class A Uniform

- Navy blue polyester style short or long-sleeved shirt.
- Navy blue polyester style trouser with black stripe on the legs with two sap pockets.
- UPD shoulder patch on each sleeve.
- Long sleeve will have appropriate years of service hash mark (hash=4 years) on left sleeve.
- Issued metal badge worn on left chest.
- Name plate worn on right chest. A maximum of two insignia bars may be worn just above the name plate.
- Staff will wear appropriate insignia on the collars of the long and short sleeved shirts.
- Whistle chain is optional
- Black t-shirt shall be worn under the short-sleeved shirt.
- Black t-shirt or black mock turtleneck or turtleneck style shirt shall be worn under the long sleeved shirt. The turtleneck (mock) shall not have any markings (logos or lettering) on the neck that are visible. If there are markings, they must be the

same color as the turtleneck (black) or subdued colors so that they are not noticeable.

- Basketweave leather gear.
- Black leather boots or shoes.
- Black socks
- Tie: worn with long sleeved shirt. Unless an exception is granted by the chief of police or designee, officers shall wear long sleeve shirts with a tie and the winter hat during all events in which staff is wearing ceremonial uniforms.
- Summer hat with short sleeve shirt
- Winter hat with long sleeve shirt

Class B Uniform

- Navy blue or black short or long-sleeved polo shirts.
- Navy blue or black BDU style matching pants.
- UPD badge patch will be sewn on the left chest.
- Officer's name embroidered on the right chest.
- UPD shoulder patch on each sleeve.
- Black t-shirts shall be worn under the short or long-sleeved polo shirts.
- Black leather shoes or boots. Black athletic shoes shall be worn with Class B shorts.
- Black socks. ½ socks shall be worn with Class B shorts.
- UPD baseball cap can be worn with Class B uniform but is not required.
- Basketweave leather gear.
- Class B shorts are allowed to be worn May 1 to September 30.

Inclement weather

- All approved rain gear and cold weather clothing is listed on the master equipment list.
- Stocking caps shall be black in color and shall have no external markings or logos. Any variance to this must be approved by the Chief of Police or his designee.
- Ear bands may be worn in place of a stocking cap. The band must be black in color with no markings or logos.

Specialized or Collateral Duty Uniforms:

- Uniforms for these assignments will be determined by the Chief of Police and/or Patrol Commander.
- Bike Patrol uniforms will only be worn during bike patrol activities.

Uniform Vest Overlays:

- Uniform overlay approved brands and styles are listed on the master uniform list addendum.
- Uniform overlay for the Class A may utilize the officer's metal badge. The name plate can be metal or embroidered.

- Uniform overlay for the Class B should utilize the UPD badge patch and the officer's name should be embroidered on the right chest of the overlay.
- Department approved shirts and jackets that are specifically designed to be worn under the vest overlays due to only having department patches on the shoulders are not approved to be worn as a standalone uniform item.

Any equipment or uniform change to this departmental general order must be approved by the Chief of Police or designee.



Departmental General Order

To: All employees
From: Chief Johansen
Re: Use of NARCAN
Date: 03/25/2019
Departmental General Order #: 2019-01

I. General Order: The Urbandale Police Department shall train all sworn officers in the use of Naloxone (NARCAN) in order to reduce injuries and fatalities due to opioid related overdoses and exposures.

II. Definitions:

- A.** Opioids: Substances that produce a morphine-like effect. They are primarily used for pain relief including anesthesia. One type of opioid is Fentanyl. Fentanyl is similar to morphine but is much more potent. Fentanyl and its analogs are members of the class of drugs known as rapid-acting synthetic opioids that alleviate pain.
- B.** Naloxone (NARCAN): Medication used to counteract exposure from opioids, fentanyl, and its analogs.
- C.** Opiate-related overdose: An acute condition caused by excessive exposure to opioids causing fatal respiratory depression.

III. Procedure: Training

- A.** All sworn officers shall receive training in the use of NARCAN before administering the product.
- B.** Training shall include at minimum:
 - 1. Requesting medical assistance
 - 2. Victim assessment
 - 3. Proper administration of nasal NARCAN
 - 4. Monitoring of the victim
 - 5. Potential need for rescue breathing or CPR
- C.** All newly hired sworn officers shall receive the training as part of their field training program.
- D.** Retraining on the use of NARCAN shall occur every four (4) years.

IV. Procedure: Maintenance

- A.** The support services division shall be tasked with the maintenance of the NARCAN program to include the following:
 - 1. Maintaining adequate supply of NARCAN.
 - 2. Replacing used, lost, damaged, and expired doses of NARCAN.
 - 3. Training on the use of NARCAN for all sworn officers.
- B.** Two doses of NARCAN shall be carried in each patrol vehicle for use. The NARCAN shall be returned to the station for storage when the vehicle is not in use. This will ensure the NARCAN is not exposed to extreme temperatures or sunlight.

- C. Expired NARCAN shall be disposed of in accordance with state and federal guidelines.
- D. Support services personnel shall be notified any time NARCAN is utilized to ensure prompt replacement.

V. Procedure: Use

- A. Sworn officers that come in contact with a suspected opioid overdose or an accidental exposure victim shall request EMS and a supervisor respond to the scene as soon as possible.
- B. An assessment of the victim shall be conducted looking for the following symptoms:
 - 1. Signs of respiratory arrest to include shallow ineffective breathing. This may include deep snorting or gurgling.
 - 2. Bluish lips and/or fingertips
 - 3. Unresponsive to stimuli
 - 4. Pale or clammy skin
 - 5. Pinpoint pupils
- C. If the assessment concludes a possible opioid overdose, one dose of NARCAN nasal spray may be administered in the nostril of the victim.
- D. If NARCAN is administered, the victim will be constantly monitored to determine if follow up measures such as rescue breathing or CPR should be initiated. While awaiting EMS the victim should be placed in the recovery position (on their side).
- E. If the victim does not wake up , respond to touch, or does not seem to be breathing normally within two to three minutes of the first dose of NARCAN, an additional dose may be administered in the other nostril.
- F. Once revived, the victim may be in an agitated and combative state and may exhibit withdraw symptoms.
- G. Upon arrival, EMS personnel shall be informed NARCAN has been used and the approximate time(s) administered.
- H. Following an incident in which a victim receives NARCAN from a sworn officer, a detailed incident report shall be completed.

VI. Procedure: Canine

- A. NARCAN can be administered to a police canine if the animal is exposed and displaying symptoms of an accidental exposure that appear life threatening.
- B. After administration of the NARCAN, the police canine shall be transported directly to a veterinarian for further treatment and evaluation.
- C. A detailed incident report shall be completed.



Departmental General Order

To: All Employees
From: Chief Johansen
Re: Pink Patch Project uniform
Date: 05-08-2019
Departmental General Order #: 2018-03

In support of the Urbandale Police Protective and Benevolent Association's Pink Patch Project, officers are approved to wear an approved uniform shirt with specially designed pink patches developed by the UPPBA from October 1st through October 31st of each year. The decision to participate in this project will be the decision of each officer. Cost for officers to obtain uniform shirts with the pink patch shall be established by the UPPBA.

The UPPBA is authorized to sell the pink patches to the public as a means to raise money to support designated cancer charity/charities. Sales to the public may begin as soon as specific charity/charities are finalized by the UPPBA. The Pink Patch Project is solely funded by the UPPBA.



Departmental General Order

To: All personnel
From: Chief Johansen
Re: Notification to area schools
Date: 10-27-2022
Departmental General Order #: 2022-01 General Order

Critical incidents occurring near any school shall require supervisory personnel to request that WestCom notify the affected school(s). Based on the incident, the affected school(s) shall determine if they will initiate lockdown procedures and at what level. The below procedures shall be used to standardize when notification shall occur:

- Incidents occurring within an approximate 2-block radius of a school that may impact school safety **shall require notification** to the affected school(s). The 2-block radius may be increased at supervisor discretion based on the severity and mobility of the incident. Incidents requiring notification include but are not limited to the following:
 - Shots fired calls
 - Active shooter/active threats of violence
 - Domestic involving a weapon (actively involved – not just present)
 - Reports of a subject with a weapon
 - Any other critical incident that may impact school safety.
- Supervisors should error on the side of caution and notify the school(s) if they are unsure of the potential threat created by the situation encountered.
- Once the situation has been resolved or contained to a point there is no longer a potential threat to the school, supervisory personnel shall notify the school(s) via WestCom. School staff will determine when their lockdown ends.



Departmental General Order

To: All Officers
From: Chief Johansen
Re: UPD Procedure for OWI Blood Draw via MercyOne Des Moines
Date: 12/05/2024
Departmental General Order #:

Officers, who in the course of their impaired driving investigation, determine a blood sample needs to be collected either by implied consent or after obtaining a search warrant, shall utilize the following procedure in addition to complying with the OWI policy (Chapter 7 Section 61.1.9) of the Operations Manual.

Implied Consent requests for BLOOD specimen

Note: This route for specimen collection shall be limited to cases where the subject expresses full cooperation to provide a blood specimen as evidence, the investigating officers suspect drug impairment, **AND** the investigation is limited to OWI 1st or 2nd offense. Any refusal of an implied consent blood request **MUST** be followed with a request for an alternate specimen (breath or urine) before it can be considered a refusal under 321J.9.

Procedure:

1. Inform dispatch to contact MercyOne (either MercyOne Medical Center or MercyOne West) of intent to request a blood draw. Request parking instructions from hospital (i.e. ambulance sally port or general ER entrance).
2. Obtain a specimen collection kit from the evidence processing area.
3. Complete paper IDOT Implied Consent and Notice Form, ensuring suspect consents to blood.
4. After suspect consents, if not already notified by dispatch, notify "Charge Nurse" of officer's intent to obtain a blood specimen.
5. Allow MercyOne staff to offer/complete a medical screening exam (MSE) to identify emergency medical needs. The suspect can refuse this by signing a refusal of treatment plan. Note: Any medical treatment necessary, as determined by hospital staff, will take priority over blood draw.
 - a. Provide the specimen collection kit to hospital staff to collect the specimen. Note: Generally, officers will be allowed in the suspect's ED room; however, if deemed to be detrimental to suspect care,

officers may be requested by hospital staff to vacate the suspect's ED room. If asked to wait outside patient care area, officers shall remain in an area that prevents escape by the subject.

6. Officers will retain the specimen and maintain chain of custody under UPD Policy.

Search Warrants requests for BLOOD specimen with NO INJURY

Procedure:

1. Inform dispatch to contact MercyOne (either MercyOne Medical Center or MercyOne West) of intent to request a blood sample be obtained. Request parking instructions from hospital (i.e. ambulance sally port or general ER entrance).
2. Complete the search warrant application through existing process.
3. Obtain specimen collection kit from the evidence processing area.
4. If not already notified by dispatch, notify "Charge Nurse" of officer's intent to obtain a blood specimen.
5. Allow MercyOne staff to offer/complete medical screening exam (MSE) to identify emergency medical needs. The suspect can refuse this by signing a refusal of treatment plan. Note: Any medical treatment necessary, as determined by hospital staff, will take priority over blood draw.
6. Provide the specimen collection kit to hospital staff to collect the specimen.
 - a. Generally, officers will be allowed in the suspect's ED room; however, if deemed to be detrimental to suspect care, officers may be requested by hospital staff to vacate the suspect's ED room. If asked to wait outside patient care area, officers shall remain in an area that prevents escape by the subject.
 - b. If the ED nurse determines that the situation puts staff or the suspect at risk, the ED nurse will let the officer present know and the officer present can pursue next steps such as calling the medical examiner to obtain samples.
 - i. In most circumstances, per UPD OWI policy, a refusal affidavit would be completed, and force shall not be used to complete the collection using contingency phlebotomist(s).
7. Officers will retain specimen and maintain chain of custody under UPD Policy.

Search Warrants requests for BLOOD specimen for SERIOUS INJURY CRASH

Procedure:

1. Inform dispatch to contact the medical examiner nurse of intent to request a blood sample be obtained via search warrant at county jail with jurisdiction.
2. Complete the search warrant application through existing process.
3. Obtain a specimen collection kit from the evidence processing area.
4. Drive suspect to the county jail with jurisdiction.
5. Provide the specimen collection kit to the medical examiner nurse to collect specimen.
6. Officers will retain specimen and maintain chain of custody under UPD Policy.

MercyOne Des Moines POLICY:

MercyOne Des Moines Medical Center will assist law enforcement in obtaining blood samples to determine blood alcohol concentration/substances of abuse in the blood. If individuals are brought to the emergency department (ED), an ED provider will perform a medical screening exam on all patients, per the MercyOne Des Moines EMTALA policy. This ED Legal Blood Collection policy does not apply to those suspected of OWI and requesting a 2nd opinion legal blood draw by an independent laboratory.

The law enforcement officer will obtain consent from the patient for the blood draw, if the patient is able to consent, or note a search warrant has been obtained. MercyOne providers obtaining the blood draw will be given a blood draw kit for the collection by law enforcement. MercyOne is not responsible for testing or custody of the blood sample.

Any medical professional acting at the request of law enforcement, trained to draw blood – including but not limited to physician, physician's assistant, medical technologist, registered nurse, phlebotomist, lab assistant, medical laboratory technician (MLT), medical laboratory scientist (MLS), medical assistant, paramedic, or nurse – may collect the patient's blood (see State v. Green, 680 N.W.2d 370 (2004)).

Procedure – Emergency Department (ED) MSE:

1. The ED provider must perform a medical screening exam (MSE) and determine if the patient has an emergency medical

condition (EMC). For example, if the individual in custody was involved in a motor vehicle accident or may have sustained injury to themselves and presents to the ED, a MSE is warranted to determine if an EMC exists. The ED provider will perform any necessary tests or treatment as part of the MSE and applicable medical treatment. The medical treatment and evaluation of the patient will take priority over collection of blood alcohol samples.

2. If the individual refuses the MSE, they must sign a refusal of treatment form to be included in the patient's chart and inform law enforcement of this refusal. A patient can still consent to the blood draw (or a warrant may be presented) even if they have refused other medical treatment/exam.
3. The ED nurse will **NOT** delay medical treatment or care in the collecting of these samples. The ED nurse will not put ED staff or the patient at risk in the collection of these samples. If the ED nurse determines that the situation puts staff or the patient at risk, the ED nurse will let the officer present know and the officer present can pursue next steps such as calling the medical examiner to obtain samples.
4. If it does not interfere with patient care and at the direction of the ED nurse, law enforcement will be allowed to be present with patient while in the ED. If law enforcement is asked to wait outside patient care area, they shall remain in an area that prevents escape by the subject. Law enforcement should typically be present at the time the legal blood draw is conducted.

*If Mercy Hospital refuses to take the blood specimen, officers shall refrain from arguing or insisting the sample be taken. This is a voluntary process by Mercy and all efforts to remain in good standing shall be utilized by the officer. Upon refusal by Mercy staff to collect the sample, officers shall revert to contacting the Polk County Medical Examiner's Office for assistance in obtaining the sample. Any instances in which Mercy refuses to take a blood specimen shall be reported to the Patrol Division Commander.

MercyOne Procedure – Collection of samples using law enforcement kit:

The following procedures will be utilized by MercyOne staff:

The law enforcement officer will provide a blood draw collection kit and will complete a police officer's report and chain of custody paperwork (MercyOne staff are not responsible for this documentation). The law enforcement officer is responsible to obtain documented consent from the patient. If the patient refuses or is unable to consent, the officer must show the medical professional a warrant (or note the warrant is sealed and not sharable). The law enforcement officer will also complete all documents included in the testing kit.

1. The ED charge nurse will notify MercyOne phlebotomy (515-365-2000) that law enforcement is requesting a legal blood draw.
2. Phlebotomy will respond to the location of the patient and obtain the blood sample per lab protocol.
 - a. Identify patient using 2 patient identifiers per laboratory policy.
 - b. Draw the blood using standard venipuncture technique and utilizing the supplies provided in the kit supplied by law enforcement officer. The medical professional may substitute drawing supplies if needed but must use the blood tube(s) provided in the kit.
 - c. Law enforcement will complete their chain of custody paperwork.
 - d. The law enforcement officer will label, date, time, initial, and seal all tubes as instructed in the kit.
 - e. DO NOT process this sample in the MercyOne lab. The sample(s) go with law enforcement.



Divisional General Order

To: Patrol Division
From: Captain Stein
Re: Patrol Division: Duty Hours and Breaks
Date: 03-01-19
Divisional General Order #: 2019-01

This order will replace Patrol Division General Order: 2015-01

Reporting For Duty:

1. Patrol Division Hours:
 - a. 1st Watch: 0700-1900hrs
 - b. 2nd Watch: 1900-0700hrs

Roll Call:

1. Officers will receive their area assignment, vehicle assignment, intelligence information, traffic complaint areas, debrief of calls for service from prior shifts, and equipment assignments (body cameras, Tasers, radars etc.).
 - a. 1st Watch: Roll Call Time: 0700-0715hrs
 - b. 2nd Watch: Roll Call Time: 1900-1915hrs

Vehicle Preparation & Inspection:

1. Officers shall inspect and prepare their vehicles and equipment. The inspection and preparation should be completed in a timely manner. Any damages or deficiencies should be immediately reported to the shift supervisor.
 - a. 1st Watch: Vehicle Inspection & Preparation: 0715-0730hrs
 - b. 2nd Watch: Vehicle Inspection & Preparation: 1915-1930hrs

Ending Tour of Duty:

1. The Watch coming off their tour of duty can report back to the station at the following times:
 - a. 1st Watch: 1850hrs
 - b. 2nd Watch: 0650hrs

**** Sergeants or the Division Commander may occasionally alter these times due to roll call trainings, case work, body camera video downloading, etc.**

Time Clock:

1. All personnel, except for the Division Commander, will utilize the time clock system to record their hours. Additional hours will not be approved unless there is a "note" in the time clock system stating the reason for the additional hours.
2. Sergeants or the Division Commander will enter officer's time for out of the ordinary work hours to include training and special assignments. It is the responsibility of the individual officer to notify a Sergeant of their other than ordinary hours. The exception, is clocking in and out for off-duty jobs which will be entered by the officer.
3. The Division Commander or his designee will enter officer's court time in the time clock. Officers will have their subpoena stamped at court and then returned to the Division Commanders mailbox for entry. This should be done in a timely manner to be entered in the same time period as court. Phone hearing subpoenas will not require a court stamp.

Break Times and Types:

1. Patrol Division officers will coordinate with their Sergeants regarding break times. A minimum of two officers must be available during break times. During emergency situations an officer can be called off of their break to respond. Officers break durations are as follows:
 - a. Two (2) 15 minute breaks
 - b. One (1) 30 minute lunch break
2. Breaks are not allowed during the first and last hour of a shift.
3. Sworn officers may combine their break times unless told otherwise by their Sergeant or Division Commander.

Break Locations:

1. Patrol officers may take their break anywhere within the city limits of Urbandale.
2. Officers may seek approval from their Sergeant to take their break outside of the city limits of Urbandale but it will be no further than ½ mile.

Any deviation from this order must be approved by a Patrol Sergeant or the Patrol Division Commander.



Divisional General Order

To: Patrol Division
From: Captain Underwood
Re: Hit and Run Reports
Date: 05-29-2025
Divisional General Order #: 25-01

Effective June 16th, 2025, all officers assigned to the patrol division will create a UPD incident report **IN ADDITION TO** a Tracs accident report on all hit and run accidents.

When responding to a hit and run accident, officers will complete a Tracs Accident Report. Upon completion of the Tracs Report, officers will write a UPD Criminal Incident Report report using the following offense codes:

- 321.262-Vehicle Damage Only
- 321.263-Information and Aid-Leaving the Scene of an Accident
- 321.264-Striking Unattended Vehicle
- 321.265-Striking Fixtures on Roadway
- 321.266-Failing to Report Accident (several specifics on pick list)

In conjunction with and pursuant to departmental policy, officers will continue to investigation all hit and run reports while at the scene. After exhausting all investigative leads at the scene, the Criminal Incident Report will be assigned to the Accident Technical Investigator (TI) Team.



Divisional General Order

To: CID
From: Captain M. Logsdon
Re: Duty Hours and Breaks
Date: 01-06-23
Divisional General Order #: 2023-01

This order will replace CID Divisional Order 2016-01.

The Criminal Investigation Division (CID) duty hours are as follows:

- A. General Investigator: Monday through Friday 0800-1600hrs
- B. General Investigation Sergeant: Monday through Friday 0800-1600hrs
- C. Narcotic Investigator: Monday through Friday 0800-1600hrs
- D. Narcotic Sergeant: Monday through Friday 0800-1600hrs
- E. With supervisor approval: Hours can be adjusted/flexed to accommodate investigations, trainings, and special projects.
- F. General Investigators and the General Investigation Sergeant will utilize the time clock system daily to record their work hours. Any additional daily hours will not be approved unless there is a "note" stating the reason in the time clock system. CID Division Commander and Narcotics personnel do not need to use the time clock system on a daily basis.

All General CID personnel will coordinate their break times with the General Investigation Sergeant or CID Division Commander. All Narcotic personnel will coordinate their break times through their Narcotics Sergeant or Task Force Commander.

- A. Sworn Officers shall receive two (2) fifteen (15) minute breaks and one (1) thirty (30) minute paid lunch break.
- B. Sworn Officers may combine their break times unless told otherwise by the CID Division Commander or their respective Sergeant.
- C. CID personnel are not restricted on where breaks can be taken. Break times start upon leaving UPD or from the off-site work location you are leaving to take your break.



Divisional General Order

To: CID Personnel
From: Captain Matt Logsdon
Re: Dress Code
Date: 05-08-18
Divisional General Order #: 2018-01 CID GO

This order will replace 2013-01.

The following dress codes for the Criminal Investigation Division will be acceptable:

Business Casual: dress pants, "Dockers" style pants, "5.11" style pants, collared shirts (polo, casual, or dress), casual shoes, dress shoes, or duty style boots/shoes.

Business Professional: Blazer or suit jacket, suit pants, dress shirt, tie (not required but shall be worn for court trials), and dress shoes. Females can wear pant suits with dress shoes.

When your weapon is openly displayed on your person your badge will also be openly displayed (belt or hanging from neck).

Clothing must not have inappropriate logos (beer, cigarette, etc) or offensive language displayed on them.

When you are attending schools or trainings you are required to wear business casual attire. Trainings such as range, defensive tactics, and other trainings that require practical exercises will be exempt from wearing business casual.

Trial appearances for court require business professional attire or Class A uniform (optional). Business casual is allowed for non-trial court appearances and depositions.

Ceremony attendance can be uniform of the day (business casual or business professional), unless directed otherwise by the Chief of Police or his designee.

Detectives called out for follow-up during non-duty hours will be required to wear business casual.

C.S.I. personnel who are called out to process crime scenes are allowed to wear jeans, collared shirts, duty boots/shoes, or tennis shoes.

Detectives assigned to special assignments or task forces are exempt from the daily dress code. They will follow the dress code implemented by the supervisor of the special assignment or task force.

Detectives who are assigned to special assignments or task forces will be required to follow the dress code for schools, trainings, trial court, and ceremonies.

Temporary or medical exceptions to these requirements can be made with supervisor and commander approval.

The Chief of Police or his designee will have the final authority to determine if clothing is appropriate or not, when in question.



Divisional General Order

To: All Personnel
From: Captain Matt Logsdon and Captain Dave Disney
Re: Alcohol Tobacco Compliance Program
Date: 05-01-2017
Divisional General Order #: 2017-01

Alcohol Tobacco Compliance Check Procedures

The Department shall follow the procedures outlined by the Iowa Alcoholic Beverages Division (ABD) for routine and fair monitoring of Iowa retail establishments licensed to sell alcohol/tobacco products. The criminal investigation division commander or designee shall administer the program for the department.

Preparing for Compliance Checks

- The department shall coordinate the participation of minors and adults as informants to assist with the controlled-buy operations (compliance checks).
- Minors 16 and 17 years of age shall be utilized for tobacco compliance checks and adults 18-20 years of age shall be utilized for alcohol compliance checks.
- All informants shall be of good character.
- All informants shall have the appearance, demeanor, mannerisms and dress appropriate to their age group.
- All minors utilized as informants shall have a parent or guardian complete a Parent/Guardian Consent Form prior to the scheduled compliance check date. A copy of the consent form shall be provided to the parent/guardian.
- The officers involved in each case shall be available for testimony at hearings and district court proceedings at the request of the local/state prosecutor.
- A minimum of two officers shall conduct the compliance checks.
- At least one officer shall be in plain clothes and one in a uniform.
- A department confidential informant packet shall be completed on the informant assisting and submitted to CID Commander.
- All departmental policies and procedures governing the use of confidential informants as established in chapter 5 section 42.2.7(Confidential Informants) of the Operations Manual shall be followed.

Operational Briefing: Held Prior to Conducting Checks

- **Appearance:** The officer in charge shall approve the informant's appearance and a photo shall be taken of the informant prior to each day's compliance check. The informant's appearance shall not be changed after the photo.
- **Official Identification:** The officer shall verify the informant has proper, official identification showing date of birth. This shall be the only identification carried or presented throughout the course of the compliance check. A photocopy of the informant's ID shall be kept for department records.
- **Possessions:** The informant shall only have "buy" money provided by the department in their possession for the sole purpose of purchasing alcohol/tobacco. No other money shall be on their person. Officer shall check the informant and their possessions to ensure they have no additional money or any alcohol/tobacco in their possession.
- **Instructions:** The informant shall be instructed as follows:
 1. Go directly to the targeted merchandise to attempt to make the purchase.
 2. Speak only as necessary. At no time shall the informant try to persuade the licensee/clerk to complete the sale.
 3. If asked about age, the informant shall respond with how old they are.
 4. If asked for identification, the informant should present their identification to the licensee/clerk.
 5. If the licensee/clerk takes an informant's identification, the informant is not to argue and to should leave the store immediately. The officer will recover the informant's ID and congratulate the licensee for compliance.
 6. If a receipt of the purchase is offered, accept and maintain for evidence.
 7. Instruct the informant to attempt to get the name of the clerk (audio recorded)
- **Termination:** Any officer involved shall have the authority to terminate the operation at any time for safety reasons.
- **Officer Positioning:** When possible, the plain clothes officer shall be stationed either inside the store or at a point from which they can observe the sale. The officer shall not appear to be with the informant.

Reporting

- An incident report shall be completed for any violations occurring during a compliance check.
- Alcohol purchased during a compliance check shall be photographed and destroyed as stated in chapter 9 section 84.1.1(Property and Evidence Control) of the Operations Manual.
- Tobacco purchase during a compliance check and any original receipt (alcohol or tobacco) shall be placed in property/evidence control according to procedures stated in chapter 9 section 84.1.1(Property and Evidence Control) of the Operations Manual.

- After each retailer check, a compliance check form shall be completed. The completed forms shall be maintained by the sergeant assigned to administer the program. The completed form for tobacco compliance shall also be submitted to the ABD.
- Upon completion of a compliance check operation, the sergeant assigned shall provide a summary report detailing the operation to the following:
 1. Criminal Investigation Division Commander
 2. Chief of Police
 3. City Clerk
 4. City Attorney
 5. Iowa Alcoholic Beverages Division (Tobacco compliance only)
- Payment of the informant for services shall be by check issued by the city of Urbandale finance department after submission of the Alcohol-Tobacco Inspection Duty form.

Alcohol/Tobacco Compliance Fund

- The alcohol/tobacco compliance fund and any fund records shall be maintained in a secure location with only the criminal investigation division commander having access. The fund shall be administered by the criminal investigation division commander to ensure all funds are utilized for authorized expenditures for the alcohol/ tobacco compliance program. The criminal investigation division commander shall have the following responsibilities with respect to the department's Alcohol/Tobacco compliance fund:
 1. Maintenance of the fund in accordance with appropriate laws and internal controls.
 2. Proper disbursements and deposits.
 3. Quarterly audits as established by Chapter 2 Section 17.4.1 of the Operations Manual.
 4. Maintenance of all documentation of relevant fund transactions.
- The criminal investigation division commander shall make disbursements from the Alcohol/Tobacco compliance fund to the sergeant in charge of administering the program for the purchase of alcohol and/or tobacco during authorized compliance checks only. Disbursements for any other expenses are prohibited.
- The sergeant assigned to administer the alcohol/tobacco compliance checks shall request cash for use in the compliance checks from the patrol division commander relative to the anticipated compliance check date. No more than one hundred dollars (\$100) shall be distributed for an operation. Any cash dispensed shall be secured at all times.
- The appropriate portions of a departmental cash account receipt shall be completed prior to the issuance of any funds. The criminal investigation division commander will maintain the cash account receipt until the operation is completed and the required information on the receipt can be completed.

- The requested cash shall only be used to purchase alcohol/tobacco during the respective compliance checks.
- When able and appropriate, officers utilizing Alcohol/Tobacco compliance fund monies shall obtain a receipt from the person or business receiving the funds unless such action would jeopardize the operation.
- After the compliance checks have been completed, the sergeant shall return the unused cash with copies of any store receipts and compliance check forms showing a purchase to the criminal investigation division commander (original receipts for purchase shall be placed in evidence).
- The cash account form shall be completed and signed by both the patrol division commander and the alcohol/tobacco sergeant. The original cash account form will be maintained by the criminal investigation division commander and a copy shall be maintained in the respective compliance check records binder by the sergeant.
- All officers utilizing Alcohol/Tobacco compliance funds shall prepare a written report (CIR) accounting for all monies used from the fund as soon as practical. The written report with all supporting documentation shall be submitted to the appropriate supervisor for review and approval.
- The alcohol/tobacco compliance fund shall be maintained in compliance of the requirements governing cash accounts as stated in chapter 2 section 17.4.1(Accounting) of the Operations Manual including quarterly audits.
- All unexpended funds shall be returned to the Alcohol/Tobacco compliance fund as soon as practical. The funds that have been checked out for use shall be kept secure at all times and shall not be taken home by the officer. When unused funds are returned they shall be documented on the cash account receipt acknowledging their return.
- Grant money obtained to administer the program shall be controlled and audited by the city of Urbandale Finance Department. The grant money shall be maintained in a separate account specifically for use to administer the program. Any documentation required by the Finance Department for the purpose of auditing the account shall be provided by the criminal investigation division commander.
- When additional cash is needed to administer the compliance checks, the criminal investigation division commander shall request funds from the finance department. At no time will the cash account maintained at the department exceed \$200.00. .



Divisional General Order

To: Support Services
From: Capt. Stein
Re: Duty Hours, requests for time off
Date: 06-17-25
Divisional General Order: 2025-01

*This order will replace Support GO dated 01-09-23.

1. Police Department office hours shall be Monday through Friday from 0800 to 1700 hours, except on City recognized holidays.
2. Support Services personnel hours:
 - A. Administrative Specialist: 0730-1600
 - B. Administrative Technicians: 0800-1630 & 0830-1700 (weeks with a city observed holiday) (2 in each slot when at full staff, shift bid based on seniority if needed) or 0700-1730 with staggered days off.
 - C. Evidence Custodian: 0700-1630 (M-TH) & 0700-1100 (F)
 - D. Community Relations Officer: 0730-1530
 - E. Community Service Officer: 0730-1600
 - F. Sergeants: 0730-1530
3. All personnel will use the city time clock system to record their work hours. Any extra time will need a supervisor's approval before working said hours and a notation in the time clock system. All employees will account for their scheduled hours during the day. (8-hour shifts, then minimum of 8.0, etc.)
4. Breaks for personnel working in the records area/front counter will ensure at least one employee is always available (0800-1700). Personnel are not restricted on where they take their breaks, however, break times start upon leaving the records area. (1 hour total if combining break times)
5. When administrative technicians request the same time off and additional assistance to operate the front counter/perform duties cannot be obtained, the following rules shall apply:
 - A. If a time off request is submitted on or before the 20th of the month prior to the month of the request, time off will be granted by seniority as an employee of the police department.
 - B. If a time off request is submitted after the 20th of the month prior to the month of the request, time off will be granted by the earliest date/time submitted.
 - C. Exceptions may be made for special circumstance if sufficient notice is received.
 - D. The request process in the time clock will be used to determine submission dates and times.

Support Services Commander



Divisional General Order

To: Support Services Personnel
From: Capt. Stein
Re: Dress Code
Date: 08-01-25
Divisional General Order: 2025-02 Support GO

This order will replace any existing orders regarding Support Services dress code.

The following are the dress requirements for the Support Services Division:

Business Casual: Business casual attire is defined as a code of dress that blends business wear with a more relaxed style that maintains professionalism and is appropriate for an office environment. Dress pants, "chino" style pants, "5.11" style pants, collared shirts (polo, casual, or dress), casual shoes, dress shoes, or duty style boots/shoes. Also, blouses, dress pants, knee-length (minimum) skirts and dresses, sweaters, department logo fleece, casual shoes, dress shoes or heels. All shoes should be closed-toed.

Business Professional: Blazer or suit jacket, suit, or dress pants, dress shirt and dress shoes. Also, suits (pants or skirt), slacks, knee-length (minimum) dresses or skirts, blouses, and dress type closed-toe shoes.

Uniform: Class "A" and Class "B" uniforms will be clean and pressed. Uniforms shall be replaced as needed or directed by a supervisor. Uniforms shall adhere to Chief's General Order, 2025-01. Articles of uniform clothing are not to be worn with civilian attire, e.g. uniform jacket/coat.

Officers/employees assigned to CIT shall be allowed to wear a business casual or professional top with an Urbandale police logo, short or long sleeved, "5.11" style pants, slacks, or jeans. All footwear shall be closed toed, casual shoes, dress shoes, or duty style boots/shoes.

Officers assigned as SROs shall be in uniform a majority of the time. When not in uniform, SROs shall wear Urbandale police logo polo shirt, dress shirt or school district logo shirt, dress pants, "5.11" style pants, or slacks. All footwear should be closed-toed, casual shoes, dress shoes or duty style boots/shoes. Officers filling in for SROs will be in uniform.

Clothing should fit appropriately and not present a baggy or excessively tight appearance (e.g., 3XL shirt for a medium-sized employee).

Officers/employees preparing for or participating in community events such as NNO, Safety City, Trunk or Treat, and other events that require practical clothing will be exempt from the clothing requirements during that assignment but shall still dress appropriately for a work environment.

When attending training, meetings, and conferences outside the department or when the department is hosting outside entities for training, meetings, etc., business casual or uniform is required. Internal “employee only” trainings such as in-service, range, defensive tactics, and other trainings that require practical exercises will be exempt from the clothing requirements during that assignment but shall still dress appropriately for a work environment.

Officers instructing training or presenting material to an audience outside the department shall be in uniform, business professional, department polo or other than logo shirts but still professional with “5.11” style pants and duty style boots/shoes to present a professional appearance. Civilian employees shall wear a polo with a department logo or markings, dress pants, “chino” style pants, “5.11” style pants, slacks, casual shoes, dress shoes, or duty style boots/shoes.

When not in uniform and an officer’s weapon is openly displayed on their person, a badge will also be openly displayed (belt or hanging from neck).

Clothing must not have inappropriate logos (alcohol or tobacco), offense language, graphics, or outside business advertisements. Major clothing brand logos (Nike, Under Armor, etc.) are exempt.

Trial appearances for court require Class “A” uniform or business professional clothing. Class “B” uniform or business casual clothing is allowed for non-trial court appearances and depositions.

Officers/Employees may be exempt from clothing requirements on a designated “casual” day with division commander approval but must be appropriate for a professional work environment.

Non-uniform department issued logo jackets may be worn during inclement weather.

T-shirts and hooded sweatshirts are only to be worn on designated “casual” days approved by the division commander. Acceptable t-shirts and hooded sweatshirts will be UPD or t-shirts that promote our community events (NNO, COI, Run for the Badge, Justin Martin, CPA). Other t-shirts and hooded sweatshirts are not acceptable.

Ceremony attendance can be uniform of the day (business casual or uniform), unless directed by the Chief of Police or his designee.

Temporary or medical exceptions to the clothing requirements can be made with division commander approval.

When in question, the division commander or the Chief of Police will have the final authority to determine if clothing is appropriate.

CODE OF ETHICS

As a Law Enforcement Officer, my fundamental duty is to serve mankind; to safeguard lives and property, to protect the innocent against deception, the weak against oppression or intimidation, and the peaceful against violence or disorder; and to respect the Constitutional Rights of all men to liberty, equality, and justice.

I will keep my private life unsullied as an example to all; maintain courageous calm in the face of danger, scorn, or ridicule; develop self-restraint; and be constantly mindful of the welfare of others. Honest in thought and deed in both my personal and official life, I will be exemplary in obeying the laws of the land and the regulations of my department. Whatever I see or hear of a confidential nature or that is confided in me in my official capacity will be kept ever secret unless revelation is necessary in the performance of my duty.

I will never act officiously or permit personal feelings, prejudices, animosities or friendships to influence my decisions. With no compromise for crime and with relentless prosecution of criminals, I will enforce the law courteously and appropriately without fear of favor, malice, or ill will, never employing unnecessary force or violence and never accepting gratuities.

I recognized the badge of my office as a symbol of public faith, and I accept it as a public trust to be held so long as I am true to the ethics of police service. I will constantly strive to achieve these objectives and ideals, dedicating myself before God to my chosen profession- LAW ENFORCEMENT.

**DALLAS COUNTY
UNINCORPORATED**

GRIMES

JOHNSTON

**POLK COUNTY
UNINCORPORATED**

URBANDALE

CLIVE

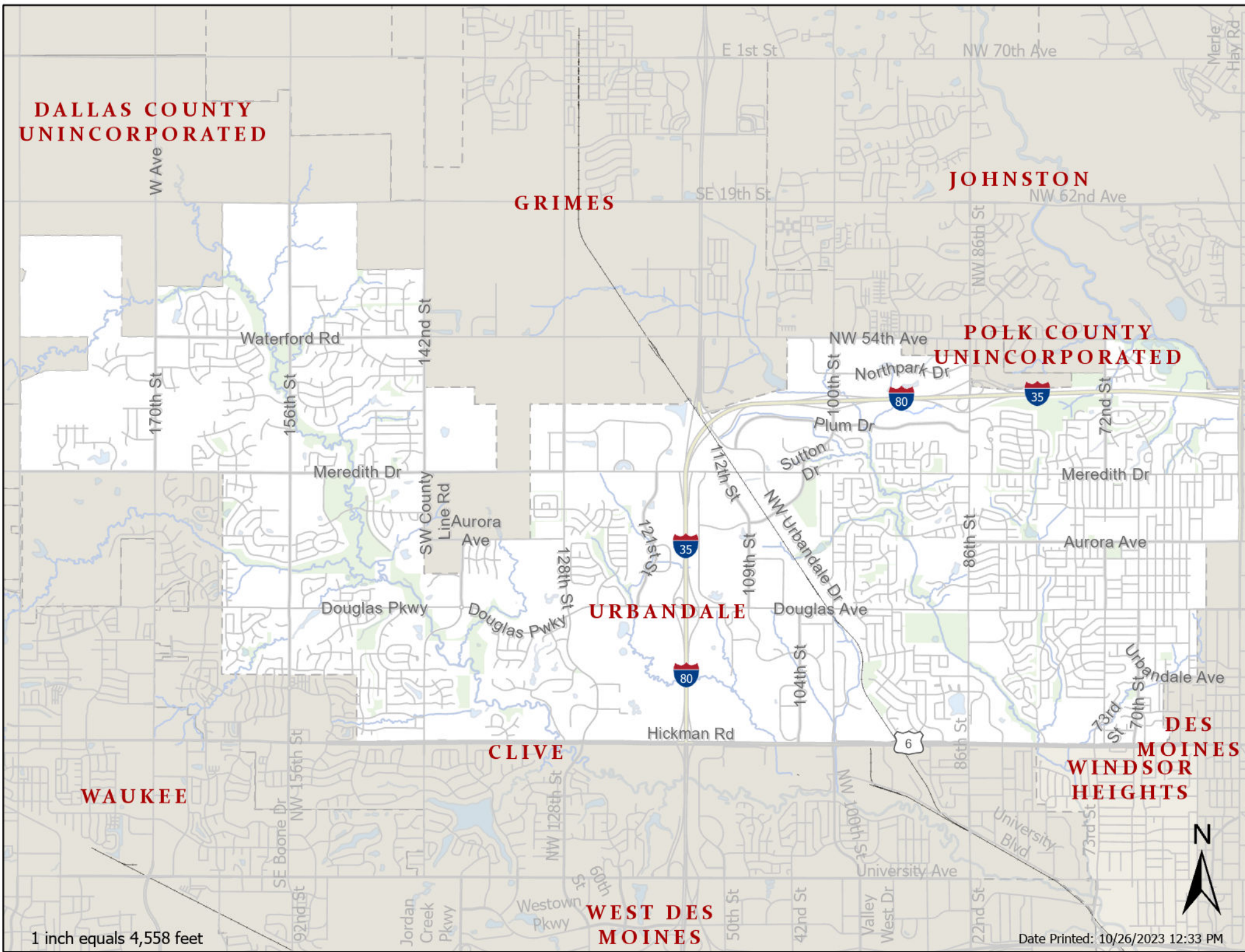
WAUKEE

**DES
MOINES
WINDSOR
HEIGHTS**

**WEST DES
MOINES**

1 inch equals 4,558 feet

Date Printed: 10/26/2023 12:33 PM





City of Urbandale Job Description

Job Title:	Chief of Police	Department:	Police
Supervisor:	City Manager	Civil Service	Entrance
Category:	X Exempt Non-exempt	Grade Level:	T
		Date Reviewed:	2024

Summary Description

Under the general direction of the City Manager, is responsible for the operation and performance of the Police Department including the Uniformed Patrol, Support Services, and Criminal Investigation Divisions. Provides advice, guidance, and policy recommendations to the City Manager, City Council, and City committees as it relates to Police Department matters. The job description is intended to represent only the key areas of responsibilities; specific position assignments will vary depending on the business needs of the department.

Routine Job Duties/Responsibilities

- Plans, organizes, directs and leads the overall operations and activities of the Police Department.
- Responds to concerns or questions and establishes and maintains effective working and professional relationships with City employees, municipal officials, commissions, committees, business and community groups, other city, county, state and federal departments/agencies, representatives of the media and the general public.
- Provides oversight and direction to the policies and procedures designed to increase the efficiency and effectiveness of departmental operations, to limit civil liabilities, and to address the public safety needs within the City.
- Oversees the financial aspects of the Police Department's operations, including accounting for department revenues and expenditures, preparing for the annual department budget and applying for appropriate grants and other outside funding opportunities. Oversees capital expenditures for equipment or facilities as needed. Assures that all operations of the Police Department are within authorized resources (i.e. budget and staff).
- Directs the development and implementation of strategic and long-range plans for the Police Department consistent with the City's long-range plans, including formulation of staffing plans and staff allocations.
- Directs the selection, orientation, training, performance management, wage administration, and discipline of employees in the Police Department in accordance with City policy.
- Assures fair and consistent treatment of all employees in the Police Department and that all employees comply with all City and departmental policies and procedures.
- Maintains the overall departmental direction of data gathering and report generation to meet established CALEA (the Commission on Accreditation of Law Enforcement Agencies) standards. Assures that all work performed in the Police Department meets the City's standards for customer service, accuracy, quality, and efficiency.
- Directs activities of the Police Department to assure that appropriate communication and coordination of efforts occurs with other units of the city.
- Assures that the Department's and City's mission, goals and objectives are fully supported and initiated.
- Ability to fulfill the job duties of a police captain, sergeant, and officer as necessary
- Performs other duties and responsibilities as assigned.

Periodic Job Duties/Responsibilities

- Attends meetings and represents the Police department including, but not limited to: City Council, intergovernmental agencies (such as, etc), civic, neighborhood and business groups.
- Facilitates CALEA assessment and inspection in four-year cycles for re-accreditation purposes. Responds to questions/inquiries from CALEA assessors regarding records, training, and law enforcement activities of department.

Job Standards

Must be able to pass a pre-employment offer: professional reference checks, drug screen, 411 physical, motor vehicle report and background with credit history check including polygraph and MMPI. Typical qualifications would be equivalent to:

- Education/Experience:**
- Bachelor's Degree in Criminal Justice, Public Administration or related field is required. Master's Degree is preferred.
 - Ten years of related work experience in Public Safety/Law Enforcement field; with five years in a management/supervisory capacity (rank of Sergeant or above).
 - Must be able to pass a pre-employment offer background check including credit history check.
 - Successful completion of the Civil Service testing process and Civil Service Commission appointment to the certified list is required.

- Skills:**
- Ability to organize, direct and coordinate a variety of projects and activities and staff including sworn officers and civilian employees
 - Strong leadership and management skills
 - Strong ethical, professional and service oriented leadership
 - Strong interpersonal skills
 - Ability to handle confidential information in a sensitive manner
 - Ability to coach subordinates in learning opportunities presented through performance management evaluation
 - Ability to take input from command staff and actively listen in evaluating suggested options for improved service delivery or operational efficiencies
 - Ability to work efficiently with no direct supervision
 - Excellent oral and written communication skills including critical thinking skills
 - Ability to synthesize various sources of information in order to draw conclusions and make difficult decisions under time constraints
 - Ability to use sound, independent judgment
 - Ability to perform essential duties at designated work site location at designated hours.

- Knowledge:**
- Extensive knowledge of and ability to apply law enforcement principles, practices, methods, including, but not limited to court procedures/practices, state/federal reporting.
 - Extensive knowledge of municipal, state and federal laws, codes or ordinances relating to municipal law enforcement
 - Good working knowledge of law enforcement operations, management, budgeting,

worker safety, labor relations, and related matters

- General knowledge of CALEA assessment techniques, standards, and benchmarks
- Proficiency with PCs and computer software and applications
- General knowledge of office equipment including, but not limited to: telephone, calculator, photo copier, and shredder

Licenses:

- Valid Iowa's Driver's License
- Iowa Police Officer Certification, or ability to obtain certification within twelve months of employment
- Iowa/NCIC certification within twelve months of employment
- All certifications required by the I.L.E.A.

Working Conditions:

- Long periods of sitting
- Intermittent standing and walking
- Ability to lift, carry, push, and pull up to 50 lbs. on occasion
- Frequent, talking, hearing, near sight acuity, concentration, judgment and writing ability
- All working conditions required of a police officer.

Physical Requirements:

- Ability to meet all physical standards for the job as specified by the Police Retirement System.
- Ability to perform physical functions of the job while wearing personal protective equipment.

Safety Hazards:

- Traffic hazards
- Electrical hazards
- Fire hazards
- Exposure to violent behavior
- Exposure to toxic/caustic chemicals
- Biohazards

Note: This job description should not be construed to imply that these requirements are the exclusive standards of the position. Incumbents will follow any other instructions, and perform any other related duties, as may be required. The employer has the right to revise this job description at any time. The job description is not to be construed as a contract for employment.



City of Urbandale Job Description

Job Title:	Police Captain	Department:	Police
Supervisor:	Police Chief	Civil Service	Promotional
Category:	X Exempt Non-exempt	Grade Level:	P
		Date Reviewed:	2024

Summary Description

Under the general direction of the Police Chief, assigns, directs and oversees the work of assigned unit(s) which may include specialized units. The job description is intended to represent only the key areas of responsibilities; specific position assignments will vary depending on the business needs of the department.

Routine Job Duties/Responsibilities

- Responsible for the management of sworn and civilian positions in the unit assigned, which includes, but is not limited to: Patrol, Criminal Investigations, or Support Services. Management includes, but is not limited to: development and training of assigned unit personnel; monitoring of staffing levels to ensure adequate coverage and to minimize overtime; etc.
- Investigates and/or responds to citizens' questions, concerns and/or complaints relating to the Police Department and determines the need for an internal investigation.
- Provides oversight and control over specific budget areas relating to assigned unit (e.g. overtime, supplies, equipment, etc.). Assists in the budgetary process as it related to the assigned unit, as requested.
- Establishes and maintains effective working relationships business and community groups, other law enforcement organizations, state and federal officials, other City departments, and/or representatives of the public as it relates to assigned unit.
- Interprets, analyzes, develops, and/or maintains applicable reports for assigned unit. This may include, but is not limited to: monthly reports, crime analysis, status of equipment availability, reports required for grants, etc.
- Keep apprised of current incidents and cases that are being investigated. Keep the Chief informed as needed.
- Directs the selection, orientation, training, performance management, wage administration, (Time Clock, Scheduling) and discipline of employees in the assigned unit in accordance with City and Police Department policy.
- Assures fair and consistent treatment of all employees in assigned unit and that all employees comply with all City and Department's policies and procedures.
- Handle minor union issues before a formal meeting with the Chief is requested.
- Assures that all work performed in the unit meets the City and Department's standards for customer service, accuracy, quality, and efficiency.
- Directs activities of the unit to assure that appropriate communication and coordination of efforts occurs with other units of the City and Department.
- Assures that the City and Department's mission, goals and objectives are fully supported and initiated.
- Performs other duties and responsibilities as assigned.
- Draft, review and recommend changes to the SOP and Rules and Regulations to the Chief of Police
- Ability to fulfill the job duties of a police sergeant and police officer as necessary.

Periodic Job Duties/Responsibilities

- Serves as Incident Commander of assigned unit at major incidents. Secures needed resources at the scene until relieved by a superior ranking officer.
- May assume the essential work of the Police Sergeant or Police Chief during his/her absence.
- Serves as the City/Department's representative at multi-jurisdictional meetings to discuss matters that affect the metro area police departments such as policy changes, training, dispatch center, task force, etc.
- Maintain and document accreditation compliance to include policy and procedure updates, training, and required periodic reporting.

Job Standards

Must be able to pass a pre-employment offer: professional reference checks, drug screen, 411 physical, motor vehicle report and background check including polygraph and MMPI. Typical qualifications would be equivalent to:

Education/Experience:

- A minimum of two (2) years of experience at the rank of police sergeant with the Urbandale Police Department. Time in grade will be determined from date of promotion to the close of the application period as stated in the promotional posting.
- Possession of a bachelor's degree with a minimum of 120 semester hours or equivalent from an accredited college or university is required. Preference will be given to those with a degree in criminal justice, public administration, or a related field.
- Successful completion of the Civil Service testing process and Civil Service Commission appointment to the certified list is required.

Skills:

- Ability to analyze situations and adopt a quick, effective, and reasonable course of action during stressful, emotional and/or physically taxing situations.
- Ability to take initiative with little direct supervision.
- Ability to write clear, accurate, factual, and concise reports.
- Ability to read, understand and interpret ordinances, laws and other operational procedures.
- Excellent critical thinking skills, including, but not limited to, the ability to: make observations and remember pertinent facts; question witnesses and obtain pertinent information.
- Excellent oral/interpersonal communication skills, including, but not limited to mediation of conflict; tact, diplomacy and professionalism when dealing with members of the public; empathy and sensitivity to victims of crime, etc.
- Ability to handle stressful, hostile, or irrational persons, whether due to physical or mental impairments, drugs/controlled substances or alcohol, or other factors
- Basic mathematical skills
- Ability to maintain intense concentration and alertness during stressful situation, particularly when preceded by extended periods of relative low stress or monotony.
- Excellent and safe driving techniques under emergency and non-emergency conditions
- Must be of good moral character.
- Excellent supervisory and management abilities
- Good training and instructional abilities
- Ability to perform essential duties at designated work site location at designated hours.

Knowledge:

- Proficiency with PC's, and various computer software applications
- Knowledge of state, federal, and city laws and ordinances
- Knowledge of City geography
- General knowledge of office equipment, including facsimile, photo copier, telephone, calculator, and shredder
- Knowledge of tools and equipment, including emergency equipment (i.e. AED, etc.), fire equipment, electronic equipment and firearms
- Proficiency with firearms and with physical defense techniques to defend self and others
- General knowledge of Human Resources laws and practices

- Knowledge of Police Department's Standard Operating Procedures and Rules and Regulations
- Knowledge of other city departments, their staff and supervisory personnel and what equipment they utilize/have in the event the PD needs such equipment in an emergency situation.
- Knowledge of who to call in the private sector in emergency situations for equipment/resources they have.

Licenses:

- Iowa NCIC Certification within 12 months of employment
- CPR First Aid
- Valid Iowa Driver's license
- Iowa police officer certification, or ability to obtain certification within twelve months of employment
- all certifications required by the I.L.E.A.

Working Conditions:

- Long periods of sitting
- Intermittent periods of standing and walking
- Ability to lift, carry, push, and pull up to 50 pounds
- Constant talking, hearing, smelling, near and far sight acuity, depth perception, color vision, field of vision, concentration, judgment, and writing ability
- Frequent stooping, reaching, handling, climbing, balancing, kneeling, crouching, crawling, dexterity, and feeling
- Constant exposure to weather, moving mechanical parts/hazards, and other environmental conditions
- Moderate exposure to extreme heat and/or cold, wet and/or humid conditions, noise intensity level, darkness/poor lighting, high, exposed places, confined spaces, dirt/dust, and odors
- Moderate use of protective footwear, ear wear, eye wear, hard hat, protective vests, and gloves
- Must be willing to use force, if necessary, to fulfill duties.
- All working conditions required of a police officer.

Physical Requirements:

- Ability to meet all physical standards for the job as specified by the Police Retirement System
- Ability to perform physical functions of the job while wearing personal protective equipment.

Safety Hazards:

- Traffic hazards
- Electrical hazards
- Fire hazards
- Exposure to violent behavior
- Exposure to toxic/caustic chemicals
- Biohazards

Note: This job description should not be construed to imply that these requirements are the exclusive standards of the position. Incumbents will follow any other instructions, and perform any other related duties, as may be required. The employer has the right to revise this job description at any time. The job description is not to be construed as a contract for employment.



City of Urbandale Job Description

Job Title:	Police Sergeant	Department:	Police
Supervisor:	Police Captain	Civil Service	Promotional
Category:	Exempt X Non-exempt	Grade Level:	M
		Date Reviewed:	2024

Summary Description

Under the general direction of the captain, supervises and directs employees assigned to a squad, small unit or specialized function. Maintains departmental equipment and supplies, interacts with citizens, provides case management, and performs administrative duties related to the position. The job description is intended to represent only the key areas of responsibilities; specific position assignments will vary depending on the business needs of the department.

Routine Job Duties/Responsibilities

Any of the following duties may be performed or assigned:

- Interprets and enforces municipal, city, state and federal laws within the jurisdiction of the City of Urbandale
- Reviews accident and arrest reports and other related paperwork and/or records to ensure accuracy and completeness. Prepares for and conducts briefings of criminal activities and related issues and outlines tactical approaches to the resolution of these cases.
- Provides case management for cases being investigated or prosecuted.
- Monitors, responds to, oversees and makes sure that calls for service are handled by the assigned officer appropriately.
- Assures proper maintenance of equipment assigned to unit, including firearms.
- Processes and responds to general public inquiries and concerns as requested. Takes police reports from the public as needed.
- Serves as public information officer for the department as directed.
- May be required to perform the essential job functions of a police officer.
- Responds to all major incidents and establishes incident command and securing needed resources at the scene until relieved by a superior ranking officer.
- Directs the selection, orientation, training, performance management, wage administration, and discipline of employees in the assigned unit in accordance with city and police department policy.
- Assures fair and consistent treatment of all employees in assigned unit and that all employees comply with all city and department's policies and procedures.
- Assures that all work performed in the unit meets the city and department's standards for customer service, accuracy, quality, and efficiency.
- Directs activities of the unit to assure that appropriate communication and coordination of efforts occurs with other units of the city and department.
- Assures that the city and department's mission, goals and objectives are fully supported and initiated.
- Performs other duties and responsibilities as assigned including supervision of specialized assignments and collateral duties including but not limited to field training, crash unit, canine, reserve officer program, Suburban Emergency Response Team, firearms, honor guard, CSI, July 4th committee, peer support, and bike patrol.
- Patrol scheduling of manpower, to include approval of vacation, holiday, sick time off.
- Initiate written report and investigate personnel complaints.

- Approve, copy and distribute all incident reports to different divisions.
- When assigned to the Mid Iowa narcotics Enforcement (MINE) Task Force:
- Provides oversight and supervision to detectives and employees assigned to unit.
- Provides oversight to all operations within the Task Force, coordinating with other law enforcement agencies as required.
- Establishes and maintains effective working relationships with other law enforcement agencies and/or organizations, state and federal officials and the Polk County Attorney's Office.
- Supervises the preparation of search warrants.
- Ability to fulfill the job duties of a police officer as necessary.
- Performs other duties and responsibilities as assigned.

Periodic Job Duties/Responsibilities

- May assume the essential work of the Police Captain during his/her absence.

Job Standards

Must be able to pass a pre-employment offer: professional reference checks, drug screen, 411 physical, motor vehicle report and background check including polygraph and MMPI. Typical qualifications would be equivalent to:

- Education/Experience:**
- A minimum of four (4) years of experience as a sworn officer with the Urbandale Police Department. Time in grade will be determined from hire date to the close of the application period as stated in the promotional posting.
 - A minimum of an associate degree with at least 60 semester hours or equivalent from an accredited college or university is required. Preference will be given to those with a degree in criminal justice, public administration, or a related field.
 - Successful completion of Civil Service testing process and Civil Service Commission appointment to the certified list is required.

- Skills:**
- Ability to handle confidential information in a sensitive manner.
 - Ability to analyze situations and adopt a quick, effective, and reasonable course of action during stressful, emotional and/or physically taxing situations.
 - Ability to take initiative with little direct supervision.
 - Ability to write clear, accurate, factual, and concise reports.
 - Ability to read, understand and interpret ordinances, laws, and other operational procedures.
 - Excellent critical thinking skills, including, but not limited to, the ability to: make observations and remember pertinent facts; question witnesses and obtain pertinent information.
 - Excellent oral/interpersonal communication skills, including, but not limited to mediation of conflict; tact, diplomacy and professionalism when dealing with members of the public; empathy and sensitivity to victims of crime, etc.
 - Ability to handle stressful, hostile or irrational persons, whether due to physical or mental impairments, drugs/controlled substances or alcohol, or other factors
 - Basic mathematical skills
 - Ability to maintain intense concentration and alertness during stressful situation, particularly when preceded by extended periods of relative low stress or monotony.
 - Excellent and safe driving techniques under emergency and non-emergency conditions
 - Must be of good moral character.
 - Excellent supervisory and management abilities

- Good training and instructional abilities
- Ability to perform essential duties at designated work site location at designated hours.

Knowledge:

- Proficiency with PC's, specifically mobile data units, and computer software and applications
- Knowledge of state, federal, and city laws and ordinances
- Knowledge of City geography
- General knowledge of office equipment, including facsimile, photo copier, telephone, calculator, and shredder
- Knowledge of tools and equipment, including emergency equipment (i.e. AED, etc.), fire equipment, electronic equipment and firearms
- Proficiency with firearms and with physical defense techniques to defend self and others.
- Basic knowledge of Human Resources laws and practices

Licenses:

- Iowa NCIC Certification within 12 months of employment.
- CPR First Aid
- Valid Iowa Driver's license
- Iowa police officer certification, or ability to obtain certification within twelve months of employment
- All certifications required by the I.L.E.A.

Working Conditions:

- Long periods of sitting
- Intermittent periods of standing and walking
- Ability to lift, carry, push, and pull up to 50 pounds.
- Constant talking, hearing, smelling, near and far sight acuity, depth perception, color vision, field of vision, concentration, judgment, and writing ability.
- Frequent stooping, reaching, handling, climbing, balancing, kneeling, crouching, crawling, dexterity, and feeling.
- Constant exposure to weather, moving mechanical parts/hazards, and other environmental conditions.
- Moderate exposure to extreme heat and/or cold, wet and/or humid conditions, noise intensity level, darkness/poor lighting, high, exposed places, confined spaces, dirt/dust, and odors
- Moderate use of protective footwear, ear wear, eye wear, hard hat, protective vests, and gloves
- Must be willing to use force, if necessary, to fulfill duties.
- All working conditions required of a police officer.

Physical Requirements:

- Ability to meet all physical standards for the job as specified by the Police Retirement System
- Ability to perform physical functions of the job while wearing personal protective equipment.

Safety Hazards:

- Traffic hazards
- Electrical hazards
- Fire hazards
- Exposure to violent behavior
- Exposure to toxic/caustic chemicals
- Biohazards

Note: This job description should not be construed to imply that these requirements are the exclusive standards of the position. Incumbents will follow any other instructions, and perform any other related duties, as may be required. The employer has the right to revise this job description at any time. The job description is not to be construed as a contract for employment.



City of Urbandale Job Description

Job Title:	Police Officer	Department:	Police Department
Supervisors:	Sergeant/Captain	Civil Service	Entrance
Category:	Exempt X Non-exempt	Grade Level:	Police Union Contract
		Date Reviewed:	2024

Summary Description

Under the general direction of the Sergeant/Captain, performs law enforcement and crime prevention services for the safety and protection of life and property in the Urbandale community. Preserves peace, order, safety, problem resolution and educates the Urbandale community. Also performs investigative work in preparation for arrests and/or criminal prosecution. The job description is intended to represent only the key areas of responsibilities; specific position assignments will vary depending on the business needs of the department.

Routine Job Duties/Responsibilities

- Interprets and enforces municipal, state, and federal regulations, codes, laws, and ordinances in assigned areas of the city.
- Responds to immediate calls for services in the answering of complaints, including handling “walk-in” complaints.
- Conducts uniformed preventative patrols in a 24 hour a day, seven day a week environment.
- Conducts preliminary investigations of crimes and completes appropriate reports, including, but not limited to: major crimes; traffic; theft; personal/familial and neighborhood disputes/assaults; intoxication; residential/commercial security alarms; etc.
- Prepares and completes supplementary reports related to complaints and investigations.
- Makes determination to arrest and processes arrested subject(s), which includes, but is not limited to: searching and/or seizing persons, vehicles, and/or property; collecting, preserving and processing evidence; interviewing victims/witnesses/suspects; transporting offenders; testifying in court proceedings; etc.
- Identifies and corrects safety hazards around public roadways, including, but not limited to: crash analysis, accident investigations; assisting stalled motorists or disabled vehicles; directing and controlling traffic; providing information on hazardous street conditions (e.g. non-working traffic signals, visibility during blizzards, flooded roadways, etc.), impounding vehicles, checking vehicle registration, issues traffic citations, etc.
- Acts as a partner with citizens, neighborhood groups, school systems, etc. in the resolution and identification of problems and/or for education etc., which may include, but is not limited to: referrals to other agencies; welfare checks; unlocking motor vehicles; education on law enforcement and crime prevention related topics, assisting with animal control related calls, ; Civil Code Enforcement, etc.
- Assists in emergency situations, including, but not limited to responding to Fire and EMS calls; watching and reporting on potentially severe weather conditions, etc.
- Inspects and maintains vehicle and all related law enforcement equipment.
- May be assigned to specialized police responsibilities and/or units, such as, but not limited to: Accident Investigation (AI); Field Training Officer; Firearms Instructor; Bike Patrol; Suburban Narcotics Unit and other assigned task forces; Suburban Emergency Response Team (SERT); etc.
- May provide direction and oversight to one or more Urbandale Police Reserve Officer(s).

- Establishes and maintains effective working relationships with other law enforcement agencies in matters relating to the apprehension of offenders and the investigation of offenses.
- Performs other duties and responsibilities as assigned.

Periodic Job Duties/Responsibilities

- Assists in receiving, searching, booking, fingerprinting, photographing and supervising prisoners
- Orders and maintains equipment and supplies.

Job Standards

Must be able to pass a pre-employment offer: professional reference checks, drug screen, 411 physical, motor vehicle report and background check including polygraph and MMPI. Typical qualifications would be equivalent to:

Education/Experience:

- High School Diploma or GED is required
- Preference may be given to candidates with at least an AA degree from an accredited college or university in diversified academic subjects or 2 years of active military service.
- Twenty years of age on or before application deadline date. Citizen of the United States at the time of application. No felony convictions or convictions for crimes involving moral turpitude.
- Uncorrected vision of not less than 20/100 in both eyes, corrected to 20/20.
- Successful completion of Civil Service testing process and Civil Service Commission appointment to the certified list is required

Skills:

- Ability to handle confidential information in a sensitive manner
- Ability to analyze situations and adopt a quick, effective, and reasonable course of action during stressful, emotional and/or physically taxing situations
- Ability to take initiative with little direct supervision
- Ability to write clear, accurate, factual, and concise reports
- Ability to read, understand and interpret ordinances, laws and other operational procedures
- Excellent critical thinking skills, including, but not limited to, the ability to: make observations and remember pertinent facts; question witnesses and obtain pertinent information
- Excellent oral/interpersonal communication skills, including, but not limited to: mediation of conflict; tact, diplomacy and professionalism when dealing with members of the public; empathy and sensitivity to victims of crime, etc.
- Ability to handle stressful, hostile, or irrational persons, whether due to physical or mental impairments, drugs/controlled substances or alcohol, or other factors
- Basic mathematical skills
- Ability to maintain intense concentration and alertness during stressful situation, particularly when preceded by extended periods of relative low stress or monotony.

- Excellent and safe driving techniques under emergency and non-emergency conditions
- Must be of good moral character
- Continuous visual effort, depth perception, color vision, hearing, and speaking abilities.
- Ability to perform essential duties at designated work site location at designated hours.

Knowledge:

- Proficiency with PC's, specifically mobile data units, and computer software and applications.
- Knowledge of state, federal, and city laws and ordinances
- Knowledge of City geography and municipal boundaries.
- General knowledge of office equipment, including facsimile, photo copier, telephone, calculator, and shredder
- Knowledge of tools and equipment, including emergency equipment (i.e. AED, etc.), fire equipment, electronic equipment and firearms
- Proficiency with firearms and with physical defense techniques to defend self and others

Licenses:

- Certification as an Iowa Police Officer within twelve months of employment
- NCIC Certification within twelve months of employment
- CPR/First Aid/AED certifications within twelve months of employment
- Valid Iowa Drivers' License
- All certifications required by the I.L.E.A.

Working Conditions:

- Long periods of sitting
- Intermittent periods of standing and walking
- Ability to lift, carry, push, and pull up to 50 pounds
- Constant talking, hearing, tasting/smelling, near and far sight acuity, depth perception, color vision, field of vision, concentration, judgment, and writing ability
- Frequent stooping, reaching, handling, climbing, balancing, kneeling, crouching, crawling, dexterity, and feeling
- Constant exposure to weather, moving mechanical parts/hazards, and other environmental conditions
- Moderate exposure to extreme heat and/or cold, wet and/or humid conditions, noise intensity level, darkness/poor lighting, high, exposed places, confined spaces, dirt/dust, and odors
- Moderate use of protective footwear, ear wear, eye wear, hard hat, protective vests, and gloves
- Must be willing to use force, if necessary, to fulfill duties.

Physical Requirements:

- Ability to meet all physical standards for the job as specified by the Police Retirement

System

- Ability to perform physical functions of the job while wearing personal protective equipment.

Safety Hazards

- Traffic hazards
- Electrical hazards
- Fire hazards
- Exposure to violent behavior
- Exposure to toxic/caustic chemicals
- Biohazards

Note: This job description should not be construed to imply that these requirements are the exclusive standards of the position. Incumbents will follow any other instructions, and perform any other related duties, as may be required. The employer has the right to revise this job description at any time. The job description is not to be construed as a contract for employment.



City of Urbandale

Job Description

Job Title:	Police Reserve Officer	Department:	Police
Supervisors:	Sergeant/Captain	Civil Service	N/A
Category:	Volunteer	Grade Level:	N/A
		Date Reviewed:	2024

Summary Description

The Urbandale reserve police officer is a volunteer law enforcement officer managed by the patrol division of the Urbandale Police Department. The reserve police officer is a highly dedicated and motivated individual who wants to serve the community by volunteering their time and effort through a law enforcement capacity. The primary purpose of the reserve police officer is to provide the community with an auxiliary unit of trained, competent police officers. Reserve police officers supplement department personnel and can be used in the event of an emergency when manpower is critical. The selection criteria to become a police reserve officer are the same as a full-time police officer. Reserve officers are required to perform to police standards, however, are volunteer part time and compensated according to city code. The job description is intended to represent only the key areas of responsibilities; specific position assignments will vary depending on the business needs of the department.

Routine Job Duties/Responsibilities

- Responds to calls for service regarding accidents, emergencies, crimes, threats, altercations and/or requests for aid.
- Interprets and enforces municipal, state, and federal regulations, codes, laws, and ordinances in assigned areas of the city.
- Provides information and assistance to the public and promotes good public relations.
- Interviews, interrogates and records statements from witnesses, suspects and victims.
- Identifies relevant facts and prepares written reports on incidents and cases assigned.
- Apprehends suspects by chasing suspects on foot, climbing over obstacles, physically subduing suspects and utilizing self-defense techniques.
- Interprets and enforces municipal, state and federal regulations, codes, laws, or ordinances, for the protection and education in assigned areas of the city.
- Assists in emergency situations, including, but not limited to responding to fire and EMS calls; watching and reporting on potentially severe weather conditions, etc. Administers first aid to injured persons.
- Inspects and maintains all related law enforcement equipment.
- Establishes and maintains effective working relationships with other law enforcement agencies in matters relating to the apprehension of offenders and the investigation of offenses.
- Testifies in court, marks and stores evidence, apprehends suspects, and makes arrests as prescribed by law.
- Assumes personal responsibility for ensuring the duties of the position are performed in a safe, efficient manner.
- Assures city and the department mission, goals and objectives are fully supported and initiated.
- Performs other duties and responsibilities as assigned.

Periodic Job Duties/Responsibilities

- Court appearance and testimony when required.
- Assists in receiving, searching, booking, fingerprinting, and photographing prisoners.
- Traffic and spectator control functions for special events.
- Assist during disasters; man-made, natural, civil disturbances, special threat situations, mass arrests or other emergency/unusual occurrences.

Job Standards

Participates and successfully passes the required state certification program for reserve police officers and department field training. Must meet established minimum volunteer hours each month. Must be able to pass a pre-employment offer: reference checks, physical and drug screen, motor vehicle report and background check. Typical qualifications would be equivalent to:

- Education/Experience:**
- High School Diploma or GED is required
 - Preference may be given to candidates with at least an AA degree from an accredited college or university in diversified academic subjects or 2 years of active military service.
 - Twenty years of age on or before application deadline date. Citizen of the United States at the time of application. No felony convictions or convictions for crimes involving moral turpitude.

- Skills:**
- Ability to handle confidential information in a sensitive manner
 - Ability to analyze situations and adopt a quick, effective, and reasonable course of action during stressful, emotional and/or physically taxing situations
 - Ability to take initiative with little direct supervision
 - Ability to write clear, accurate, factual, and concise reports
 - Ability to read, understand and interpret ordinances, laws and other operational procedures
 - Excellent critical thinking skills, including, but not limited to, the ability to: make observations and remember pertinent facts; question witnesses and obtain pertinent information
 - Excellent oral/interpersonal communication skills, including, but not limited to: mediation of conflict; tact, diplomacy and professionalism when dealing with members of the public; empathy and sensitivity to victims of crime, etc.
 - Ability to handle stressful, hostile, or irrational persons, whether due to physical or mental impairments, drugs/controlled substances or alcohol, or other factors
 - Basic mathematical skills
 - Ability to maintain intense concentration and alertness during stressful situation, particularly when preceded by extended periods of relative low stress or monotony.
 - Excellent and safe driving techniques under emergency and non-emergency conditions
 - Must be of good moral character
 - Ability to perform essential duties at designated work site location at designated hours.

- Knowledge:**
- Proficiency with PC's, specifically mobile data units, and computer software and

applications.

- Knowledge of state, federal, and city laws and ordinances
- Knowledge of City geography and municipal boundaries.
- General knowledge of office equipment, including facsimile, photo copier, telephone, calculator, and shredder
- Knowledge of tools and equipment, including emergency equipment (i.e. AED, etc.), fire equipment, electronic equipment and firearms
- Proficiency with firearms and with physical defense techniques to defend self and others

Licenses:

- Certification as an Iowa reserve police officer within twelve months of employment
- NCIC Certification within twelve months of employment
- CPR/First Aid/AED certifications within twelve months of employment
- Valid Iowa Drivers' License
- All certifications required by the I.L.E.A for a reserve police officer.

Working conditions:

- Long periods of sitting
- Intermittent periods of standing and walking
- Ability to lift, carry, push, and pull up to 50 pounds
- Constant talking, hearing, tasting/smelling, near and far sight acuity, depth perception, color vision, field of vision, concentration, judgment, and writing ability
- Frequent stooping, reaching, handling, climbing, balancing, kneeling, crouching, crawling, dexterity, and feeling
- Constant exposure to weather, moving mechanical parts/hazards, and other environmental conditions
- Moderate exposure to extreme heat and/or cold, wet and/or humid conditions, noise intensity level, darkness/poor lighting, high, exposed places, confined spaces, dirt/dust, and odors
- Moderate use of protective footwear, ear wear, eye wear, hard hat, protective vests, and gloves
- Must be willing to use force, if necessary, to fulfill duties.

Physical requirements:

- Ability to meet all physical standards of a full-time officer for the department.
- Ability to perform physical functions of the job while wearing personal protective equipment.

Safety hazards:

- Traffic Hazards
- Electrical hazards
- Fire Hazards
- Exposure to violent behavior
- Exposure to toxic/caustic chemicals
- Biohazards

Note: This job description should not be construed to imply that these requirements are the exclusive standards of the position. Incumbents will follow any other instructions, and perform any other related duties, as may be required. The employer has the right to revise this job description at any time. The job description is not to be

construed as a contract for employment.



City of Urbandale Job Description

Job Title:	Civilian Records Supervisor/Accreditation Manager	Department:	Police
Supervisors:	Captain	Civil Service	Promotional
Category:	X Exempt Non-exempt	Grade Level:	K
		Date:	2024

Summary Description

Supervises, plans and directs the operational and day-to-day functions of the civilian records staff in Support Services, including the maintenance and processing of all department records for legal processes, public information, and accreditation standards. Provides administrative support to the Chief of Police and Command Staff while maintaining a high level of confidentiality. This position is supervised by the Support Services Commander. The job description is intended to represent only the key areas of responsibilities; specific position assignments will vary depending on the business needs of the department.

Routine Job Duties/Responsibilities

- Supervises, manages and trains civilian personnel in the records section.
- Review records tasks and develops an efficient routine to complete operations.
- Implements all City and Department policies in the records section.
- Participates in the hiring of civilian records staff.
- Prepares annual performance evaluations for all civilian records personnel.
- Responsible for timeliness and efficiency of work in the records section.
- Ensures public information is available as requested and the release of such information is in compliance with local, state and federal regulations.
- Evaluate records equipment and supplies and recommends new purchases.
- Assist with preparation of work schedules and assignments.
- Ensure all statistical reports needed are completed in a timely manner.
- Serve as Terminal Agency Coordinator for NCIC computer system.
- Serve as the RMS/TRAC's Administrator for the Police Department.
- Serve as the UCR/NIBRS coordinator for the Police Department.
- Serve as the Power DMS Administrator for the Police Department.
- Represent the Police Department as the Accreditation Manager.
- Work with Command Staff to accomplish all C.A.L.E.A. needs.
- Participate in special projects as assigned
- Performs other duties as assigned

Job Standards

Must be able to pass a pre-employment offer: professional reference checks, drug screen, 411 physical, motor vehicle report and background check including credit history check.

Typical qualifications would be equivalent to:

Education/Experience:	• Associates degree from an accredited college or university required; Bachelor's Degree preferred • Five years' experience in office management with supervisory responsibilities. • Direct experience with customer service delivery preferred

Skills:

- Ability to coordinate and direct the work of others; ability to prepare accurate and comprehensive reports; ability to deal with customers tactfully and courteously; ability to communicate information clearly both verbally and in written form.
- Ability in organization development, team building, and group processes.
- Ability to work under pressure in a public area.
- Ability to distribute daily incoming material in a timely fashion.
- Ability to lead, motivate, train, organize, prioritize, supervise and evaluate the work of others.
- Ability to communicate effectively and maintain working relationships with other Police personnel, Court Officials, other law enforcement agencies and the public.
- Ability to prepare accurate and reliable reports containing findings, recommendations and conclusions.
- Ability to operate a personal computer using program applications appropriate to assigned duties and responsibilities.
- Ability to quickly learn and put to use new skills and knowledge brought about by rapidly changing information and/or technology.
- Ability to handle confidential information in a sensitive manner.
- Effective oral and written communication skills
- Excellent interpersonal/customer service skills.
- Excellent organizational skills.
- Ability to handle multiple priorities and direction from multiple department members.
- Work independently in the absence of supervision.
- Proficiency with PC's and computer software and applications, including word processing, email, spreadsheets, the internet, and databases.
- Independently prepare correspondence, reports, newsletters, and memoranda.
- Implement and maintain filing systems.
- Ability to perform essential duties at designated work site location at designated hours.

Knowledge:

- Various office equipment, which may include facsimile, photocopier, multi-line telephone, calculator, shredder, binding equipment, microfilm reader, Dictaphone, postage machine, digital paging system, two-way radio (portable and base), laminator.
- English usage, spelling, grammar and punctuation.
- General mathematics includes addition, subtraction, division, and multiplication.
- Modern office technology and equipment, including computers and related software applications.
- Customer service procedures and principles.
- Principles and procedures of record keeping.
- Principles of business letter writing and report preparation.
- General accounting methods and procedures.
- Applicable Federal, State and local codes, laws and regulations.
- Database entry and utilization.

Licenses:

- A valid driver's license
- Shall possess or have the ability to obtain a National Crime Information Certification (NCIC) as well as Terminal Agency Coordinator certification for the Department within 6 months.
- Shall possess or have the ability to obtain a State of Iowa Notary Public designation.

Working Conditions:

- Office environment.
- Long periods of sitting.
- Intermittent periods of standing and walking.
- Ability to lift, carry, push, pull up to 20 pounds.
- Constant talking, hearing, near and far sight acuity, field of vision, concentration handling, and dexterity.
- Frequent stooping, handling and writing ability.
- Intermittent balancing, kneeling, crouching, and reaching.

Safety Hazards

- None

Note: This job description should not be construed to imply that these requirements are the exclusive standards of the position. Incumbents will follow any other instructions, and perform any other related duties, as may be required. The employer has the right to revise this job description at any time. The job description is not to be construed as a contract for employment.



City of Urbandale Job Description

Job Title:	Administrative Specialist	Department:	Various
Supervisor:	Department Supervisor/Manager/Director	Civil Service	Entrance
Category:	Exempt X Non-exempt	Grade Level:	G
		Date:	2024

Summary Description

This is the third and top level in the administrative support series. Incumbents apply departmental policy and procedure in the conduct of administrative support functions within a department/division. Incumbent's data entry, verification and analysis; compilation of reports; creating and coordinating meeting agendas, minutes and arrangements; documenting meeting minutes and activities; and drafting original correspondence. Duties also include: providing customer service requiring interpretation of departmental information within procedures, referral, and tracking and follow-up of customer issues; processing forms and applications; tracking expenses and receivables; monitoring of budgets; and purchasing and maintaining an inventory of supplies. The job description is intended to represent only the key areas of responsibilities; specific position assignments will vary depending on the business needs of the department.

Routine Job Duties/Responsibilities

- Screens calls, visitors and mail; assists the public and other City staff in interpreting and applying City policies, procedures, codes and ordinances; research, responds to and tracks complaints and requests for information on regulations, procedures, systems and precedents relating to assigned responsibilities; determines appropriate dissemination of information.
- Maintains a calendar of activities, meetings and various events for assigned staff, coordinates meetings, activities, and conferences with other City departments, the public and outside agencies.
- Administers an assigned process or function; performs and verifies data entry; makes adjustments and updates; trains and monitors users; develops procedures for format and utilization of data; generates standard and ad hoc reports.
- Types, researches and proofreads a wide variety of standard and original reports, letters, memoranda, correspondence, newsletters, and charts; independently composes correspondence and newsletters; researches and develops forms related to assigned area of responsibility; monitors and updates department materials and manuals.
- Processes, verifies and reviews materials, applications, records and reports for completeness and conformance with established regulations and procedures; applies applicable policies and procedures in determining completeness of applications, records and reports; conducts research of files, records, and databases; provides information and forms to the public and employees; collects, processes and distributes appropriate information.
- Performs administrative support functions for a board or committee; takes meeting minutes; prepares and disseminates agendas and minutes of meetings; monitors and tracks related information; maintains related files and records; prepares related documentation on behalf of board or committee.
- Assists in the department budgeting processes; compiles annual budget requests; recommends expenditure requests for designated accounts; monitors accounts; processes and codes expenditure requests for designated accounts.
- Oversees an administrative process or program; develops and monitors process and procedures; tracks and compiles data for special projects and programs; collects and assembles data and background materials for a variety of reports; conducts surveys; ensures equipment, supplies, contracts, and related items are available and in compliance.
- Organizes and maintains filing systems; maintains records related to specific areas of assignment.
- Maintains department/area website and specific department software programs; develops and updates content; research, tracks and responds to website questions and inquires.
- Processes department accounting data including accounts payable, accounts receivable, purchasing and payroll; inputs corrections and updates; codes data; verifies data for accuracy and completeness; conducts inquire and completes report writing.
- Balances daily cash and completes daily and/or quarterly financial reports and deposits; verifies and corrects data for accuracy.
- Monitors that all work performed in the unit meets the City's standards for customer service, accuracy, quality, and efficiency.

- Assures that the City's mission, goals and objectives are fully supported and initiated.
- Performs other duties and responsibilities as assigned.

Job Standards

Must be able to pass a pre-employment offer: reference checks, drug screen, motor vehicle report and background and credit history check Any combination of education and experience providing the required skill and knowledge is qualifying.

Typical qualifications would be equivalent to:

Education/Experience:	• High School Diploma or equivalent. • Three years of administrative support and/or customer service experience.
Skills:	• Ability to handle confidential information in a sensitive manner. • Effective oral and written communication skills • Excellent interpersonal/customer service skills. • Excellent organizational skills. • Ability to handle multiple priorities and direction from multiple department members. • Work independently in the absence of supervision. • Proficiency with PC's and computer software and applications, including word processing, email, spreadsheets, the internet, and databases. • Type at a speed necessary for successful job performance. • Take and transcribe dictation, if required by the position, at a speed necessary for successful job performance. • Perform responsible and difficult administrative support work involving the use of independent judgment and personal initiative. • Independently prepare correspondence, reports, newsletters, and memoranda. • Implement and maintain filing systems. • Ability to perform essential duties at designated work site location at designated hours
Knowledge:	• Various office equipment, which may include facsimile, photocopier, multi-line telephone, calculator, shredder, binding equipment, microfilm reader, dictaphone, postage machine, digital paging system, two-way radio (portable and base), laminator. • English usage, spelling, grammar and punctuation. • General mathematics includes addition, subtraction, division, and multiplication. • Modern office technology and equipment, including computers and related software applications. • Customer service procedures and principles. • Principles and procedures of record keeping. • Principles of business letter writing and report preparation. • General accounting methods and procedures. • Applicable Federal, State and local codes, laws and regulations. • Database entry and utilization.
Licenses:	• A valid driver's license may be required depending on assignment. • Notary Public designation may be required depending on assignment.
Working Conditions:	• Office environment. • Long periods of sitting. • Intermittent periods of standing and walking. • Ability to lift, carry, push, pull up to 20 pounds. • Constant talking, hearing, near and far sight acuity, field of vision, concentration handling, and dexterity. • Frequent stooping, handling and writing ability. • Intermittent balancing, kneeling, crouching, and reaching.
Safety Hazards:	• None.

Note: This job description should not be construed to imply that these requirements are the exclusive standards of the position. Incumbents will follow any other instructions, and perform any other related duties, as may be required. The employer has the right to revise this job description at any time. The job description is not to be construed as a contract for employment.



City of Urbandale

Job Description

Job Title:	Evidence Technician	Department:	Police
Supervisors:	Sergeant/Captain	Civil Service	Entrance
Category:	Exempt X Non-exempt	Grade Level:	G
		Date Reviewed:	2024

Summary Description

Under the direction of Police Sergeant/Captain, provides a wide variety of non-sworn support and enforcement related functions for the public and police department staff. These services include but are not limited to, report writing, property and evidence control, video and photographic evidence management, fingerprinting, general maintenance functions, impounded vehicle processing, vehicle transportation, and other duties as assigned by management. The job description is intended to represent only the key areas of responsibilities; specific position assignments will vary depending on the business needs of the department.

Routine Job Duties/Responsibilities

- Performs customer service duties; answers the telephone; greets visitors; screens and routes telephone calls.
- Assists with Evidence and Property Room management, including filing, organizing, monitoring, and disposal of property. Assures quality controls to meet and exceed audit and inspections requirements of the property evidence control function.
- Prepares, manages, catalogs, duplicates, and stores all photographs and digital media.
- Prepares videos and photographs for court proceedings and open record requests to include redaction.
- Conducts fingerprinting as part of public assistance and various city of Urbandale employment applicants.
- Assists officers with impoundment of vehicles and collection of property under a variety of circumstances.
- Assures that all work performed in the unit meets the City's standards for customer service, accuracy, quality, and efficiency.
- Maintains, replaces, repairs, and purchases equipment. Recommends new equipment and technology purchases. Maintains evidence storage areas.
- Testifies in court related to custody and control of evidence and related areas.
- Evaluates court dispositions involving property and evidence to ensure a lawful disposition.
- Knowledgeable in state and federal law regarding evidence handling, custody, and control.
- Assures that the City's mission, goals, and objectives are fully supported and initiated.
- Manages evidentiary processes with the DCI crime lab and other laboratories as needed.
- Develops and distributes activity reports as required by supervisors.
- Prepares materials for various attorneys, investigations, and open records requests.
- Attends meetings, conferences, workshops and training sessions and reviews publications and audiovisual materials to become and remain current on the principles, practices and new developments in assigned work area.
- Performs other duties and responsibilities as assigned.

Job Standards

Must be able to pass a pre-employment offer: professional reference checks, drug screen, motor vehicle report,

and background check including a polygraph examination. Typical qualifications would be equivalent to:

- Education/Experience:**
- HS Diploma or GED and Three years' experience working with the public required
 - Preference may be given to candidates with at least an AA degree and/or 2 years of active military service.
 - Must be 20 years old.
- Skills:**
- Ability to handle confidential information in a sensitive manner.
 - Ability to gain proficiency in a variety of software programs to include Microsoft office suite, File on Q, Central Square records management, Gov Deals, DCI Beast, LaserFiche, WatchGuard, Versus 911, Iowa Courts Online, Adobe Premier Pro, Clear reporting, ATF e-trace, Iowa Track-kit, and others as required.
 - Ability to take initiative and work independently.
 - Ability to view graphic videos or photographs depicting acts of violence or other criminal behavior or the response to such acts.
 - Effective oral and written communication skills
 - Excellent interpersonal communication skills.
 - Ability to testify in criminal proceedings.
 - Ability to safely handle firearms.
 - Problem-solving ability
 - Excellent telephone techniques
 - Accurate mathematical skills
 - Sound judgment and decision-making abilities
 - Ability to concentrate in a diverse work setting
 - Must possess good organizational skills.
 - Ability to handle multiple priorities, good time management skills
 - Flexibility
 - Ability to work independently with limited supervision.
 - Type at a speed necessary for successful job performance.
 - Occasional handling emotionally distraught individuals while dealing with confidential and sensitive information.
 - Able to perform essential duties at designated work site location at designated hours.
- Knowledge:**
- Various office equipment, which may include facsimile, photo copier, multi-line telephone, calculator, shredder, binding equipment, two way radio (portable and base).
 - English usage, spelling, grammar and punctuation.
 - General mathematics including addition, subtraction, division, and multiplication.
 - Modern office technology and equipment, including computers and related software applications.
 - Reception and customer service procedures and principles.
 - Principles and procedures of record keeping.
 - Knowledge of established codes, ordinances and regulations or the ability to acquire the knowledge with the ability to read, analyze and interpret governmental regulations.
 - Knowledge of legal requirements for evidence handling and disposition.
 - Internal policy and procedure.
 - Knowledge of geography, streets and principal locations of the City
 - Ability to learn the operations and activities of assigned department or division.
- Licenses:**
- Valid Iowa Driver's License.

- Ability to be certified by Iowa/NCIC within 6 months of hire
- Notary Public designation may be required depending on assignment

Working Conditions:

- Long periods of standing and walking
- Ability to push and pull greater than 50 pounds
- Ability to lift and carry 21-50 pounds
- Intermittent balancing, stooping, crouching, crawling, feeling, near sight acuity, far sight acuity, and depth perception.
- Frequent climbing, kneeling, reaching, handling, dexterity, talking, hearing, smelling, color vision, field of vision, concentration, judgment, and writing ability.
- Moderate exposure to weather (including extreme cold, heat, wet and/or humidly), odors, and traffic hazards.
- May be required to work varying evenings, nights, and weekends as well as being called in during off hours to handle various situations.

Safety Hazards:

- Biohazards, exposure to toxic caustic chemicals.

Note: This job description should not be construed to imply that these requirements are the exclusive standards of the position. Incumbents will follow any other instructions, and perform any other related duties, as may be required. The employer has the right to revise this job description at any time. The job description is not to be construed as a contract for employment.



City of Urbandale Job Description

Job Title:	Administrative Technician	Department:	Various
Supervisor:	Department Supervisor/Manager/Director	Civil Service	Entrance
Category:	Exempt X Non-exempt	Grade Level:	E
		Date:	2024

Summary Description

This is the second level of the administrative support series. Basic knowledge of applicable laws, regulations, and departmental policies and procedures are required at this level. This level of the series may be used to describe ongoing work at this level or used as a second level for work of greater complexity and responsibility. Duties include: performing reception work providing organizational information and service to clients and visitors; filing and processing records and documents; performing and reviewing data entry and information; setting up work files; developing and maintaining tracking lists; scheduling facilities; taking and posting payments; processing mail; preparing forms and letters using established procedure; and maintaining an inventory of supplies and materials. The job description is intended to represent only the key areas of responsibilities; specific position assignments will vary depending on the business needs of the department.

Routine Job Duties/Responsibilities

- Performs reception and customer service duties; answers the telephone; greets visitors; screens and routes telephone calls; provides information on department or division operations and activities; accepts monies, documentation and information on behalf of the City and ensures documentation meets City requirements; provides information on City policies and procedures as required; follows up to ensure customer question or issue is responded to appropriately.
- Enters data into a computer from a variety of sources including accounting, payroll, standard statistical, activity and related documents; inputs corrections and updates; verifies data for accuracy and completeness; conducts inquiries; compiles information for reporting.
- Collects and processes over the counter or phone-in registrations, documentation and records for various City programs or permits; enters program information into automated system(s); verifies and determines applicability and acceptance of information; disseminates information and records in accordance with rules and regulations; tracks and issues licenses and permits.
- Types and proofreads a variety of routine and standard documents, lists, and forms including general correspondence, standard reports, newsletters, brochures and memoranda from rough draft, standard formats, or verbal instruction; makes routine updates to website information; prepares packets of information; disseminates information as appropriate.
- Participates in the maintenance of filing systems; sets up work files; reviews records for various information as requested; fulfills and documents customer requests including sensitive and confidential materials according to established procedures; scans, copies and files written and audiovisual materials.
- Processes the mail; receives, sorts, and distributes incoming and outgoing correspondence and packages.
- Schedules functions such as meetings, workshops, events, and training for assigned area; maintains function calendar; orders materials, supplies and refreshments; set-ups, arranges, and ensures facilities are cleaned.
- Assures that all work performed in the unit meets the City's standards for customer service, accuracy, quality, and efficiency.
- Assures that the City's mission, goals and objectives are fully supported and initiated.
- Performs other duties and responsibilities as assigned.

Job Standards

Must be able to pass a pre-employment offer: reference checks, drug screen, motor vehicle report and background and credit history check. Typical qualifications would be equivalent to:

- Education/Experience:**
- High School Diploma or equivalent.
 - One year of administrative support and/or customer service experience.
- Skills:**
- Ability to handle confidential information in a sensitive manner.
 - Effective oral and written communication skills
 - Excellent interpersonal/customer service skills.
 - Excellent organizational skills.
 - Ability to handle multiple priorities and direction from multiple department members.
 - Ability to work efficiently under general supervision.
 - Basic proficiency with PC's and computer software and applications, including word processing, email, spreadsheets, the internet, and databases.
 - Type at a speed necessary for successful job performance.
 - Ability to perform essential duties at designated work site location at designated hours.
- Knowledge:**
- Various office equipment, which may include facsimile, photocopier, multi-line telephone, calculator, shredder, binding equipment, microfilm reader, dictaphone, postage machine, digital paging system, two-way radio (portable and base), laminator.
 - English usage, spelling, grammar and punctuation.
 - General mathematics includes addition, subtraction, division, and multiplication.
 - Modern office technology and equipment, including computers and related software applications.
 - Reception and customer service procedures and principles.
 - Principles and procedures of record keeping.
 - Ability to learn the operations and activities of assigned department or division.
- Licenses:**
- A valid driver's license may be required depending on assignment.
 - Notary Public designation may be required depending on assignment.
- Working Conditions:**
- Office environment.
 - Long periods of sitting.
 - Intermittent periods of standing and walking.
 - Ability to lift, carry, push, pull up to 20 pounds.
 - Constant talking, hearing, near and far sight acuity, concentration handling, and dexterity.
 - Frequent stooping, handling and writing ability.
 - Intermittent balancing, kneeling, crouching, and reaching.
 - Long periods of computer usage, constant visual concentration
- Safety Hazards:**
- Occasional eye strain possible.

Note: This job description should not be construed to imply that these requirements are the exclusive standards of the position. Incumbents will follow any other instructions, and perform any other related duties, as may be required. The employer has the right to revise this job description at any time. The job description is not to be construed as a contract for employment.



City of Urbandale

Job Description

Job Title:	Community Service Officer	Department:	Police
Supervisors:	Sergeant/Captain	Civil Service	Entrance
Category:	Exempt X Non-exempt	Grade Level:	E
		Date Reviewed:	2024

Summary Description

Under the direction of Police Sergeant/Captain, provides a wide variety of non-sworn support related functions for the public and police department staff. These services include but are not limited to, report writing, inventory control, fingerprinting, vehicle and general maintenance functions, impounded vehicle processing, vehicle transportation, animal control and licensing services, community event planning and preparation, and other duties as assigned by management. The job description is intended to represent only the key areas of responsibilities; specific position assignments will vary depending on the business needs of the department.

Routine Job Duties/Responsibilities

- Performs customer service duties; answers the telephone; greets visitors; screens and routes telephone calls.
- Conducts fingerprinting as part of public assistance and various City of Urbandale employment applicants.
- When necessary, provides assistance regarding animal control and shelter maintenance to include but not limited to; the feeding and care of impounded and stray animals, cleaning the shelter as needed, filling in for sick or vacationing animal control officers, and responding to related animal control services.
- Assist with community crime prevention and outreach programs as directed to include planning, community and business outreach, set up and tear down of events.
- Assists patrol officers with the processing of impounded vehicles under a variety of circumstances.
- Assures all work performed in the unit meets the city's standards for customer service, accuracy, quality, and efficiency.
- Assures the City's mission, goals, and objectives are fully supported and initiated.
- Attends meetings, conferences, workshops and training sessions and reviews publications and audiovisual materials to become and remain current on the principles, practices, and new developments in assigned work area.
- Manages department inventory of all tangible assets.
- Performs other duties and responsibilities as assigned.

Periodic Job Duties/Responsibilities

- Front desk customer service

Job Standards

Must be able to pass a pre-employment offer: reference checks, drug screen, motor vehicle report and background check. Typical qualifications would be equivalent to:

- Education/Experience:**
- HS Diploma or GED and Three years' experience working with the public required
 - Preference may be given to candidates with at least an AA degree and/or 2 years of active military service.
- Skills:**
- Ability to handle confidential information in a sensitive manner
 - Ability to take initiative

- Effective oral and written communication skills
- Excellent interpersonal communication skills
- Problem-solving ability
- Excellent telephone techniques
- Accurate mathematical skills
- Sound judgment and decision-making abilities
- Ability to concentrate in a diverse work setting
- Must possess good organizational skills.
- Ability to handle multiple priorities, good time management skills
- Flexibility
- Ability to work independently with limited supervision.
- Type at a speed necessary for successful job performance.
- Ability to perform essential duties at designated work site location at designated hours.

Knowledge:

- Various office equipment, which may include facsimile, photo copier, multi-line telephone, calculator, shredder, binding equipment, two-way radio (portable and base).
- English usage, spelling, grammar and punctuation.
- General mathematics including addition, subtraction, division, and multiplication.
- Modern office technology and equipment, including computers and related software applications.
- Reception and customer service procedures and principles.
- Principles and procedures of record keeping.
- Knowledge of established codes, ordinances and regulations or the ability to acquire the knowledge with the ability to read, analyze and interpret governmental regulations.
- Knowledge of geography, streets and principal locations of the City
- Ability to learn the operations and activities of assigned department or division.

Licenses:

- Valid Iowa Driver's License.
- Ability to be certified by Iowa/NCIC within 6 months of hire
- Notary Public designation may be required depending on assignment.

Working Conditions:

- Long periods of standing and walking
- Ability to push and pull greater than 50 pounds
- Ability to lift and carry 21-50 pounds
- Intermittent balancing, stooping, crouching, crawling, feeling, near sight acuity, far sight acuity, and depth perception.
- Frequent climbing, kneeling, reaching, handling, dexterity, talking, hearing, smelling, color vision, field of vision, concentration, judgment, and writing ability.
- Moderate exposure to weather (including extreme cold, heat, wet and/or humidly), odors, and traffic hazards.
- May work varying evenings, nights, and weekends as well as being called in during off hours to handle various situations.

Safety Hazards:

- Traffic hazards
- Electrical hazards
- Fire hazards

- Exposure to toxic/caustic chemicals

Note: This job description should not be construed to imply that these requirements are the exclusive standards of the position. Incumbents will follow any other instructions, and perform any other related duties, as may be required. The employer has the right to revise this job description at any time. The job description is not to be construed as a contract for employment.



City of Urbandale Job Description

Job Title:	Mental Health Co-Responder	Department:	Police Department
Supervisor:	Sergeant/Captain	Civil Service	Entrance
Category:	Exempt X Non-exempt	Grade Level:	H
		Date:	2025

Summary Description

Under the general direction of the Sergeant/Captain, provides mental health related services based on law enforcement contracts and acts as liaison between the police department and various mental health providers, consumers and the community. This mental health responder will work closely with a CIT police officer in a co-responder model. Will provide crisis intervention, case management, resources and community conflict resolution by responding to calls involving persons that need assistance due to mental health concerns, community concerns, substance abuse, experiencing homelessness and those that need a resolution outside of the criminal justice path. The job description is intended to represent only the key areas of responsibilities; specific position assignments will vary depending on the business needs of the department.

Routine Job Duties/Responsibilities

- Respond to emergency calls or situations involving individuals experiencing mental health crises alongside law enforcement.
- Assess the mental health status of individuals in crisis and determine immediate needs, including potential risks to themselves or others.
- Provide emotional support and crisis de-escalation techniques to calm individuals in distress.
- Connect individuals to appropriate mental health services, such as psychiatric evaluations, inpatient care, outpatient therapy, or substance abuse treatment and complete follow-ups, as needed.
- Collaborate with local mental health professionals, hospitals, and social service agencies to facilitate timely care.
- Maintain accurate, confidential and timely records of interventions, assessments, and referrals made during each case.
- Maintains data as prescribed by the department, prepares computerized reports; develops and maintains tracking programs, as needed.
- Work in tandem with police officers to ensure an appropriate and coordinated response to individuals in crisis.
- Acts as a liaison with the mental health task force and other mental health agencies, assists in development, coordinating and implementing training to support the mental health service mission.
- Attend court proceedings, as needed, based on mental health protocols and legal requirements.
- Collaborate with clients to create individualized, strength-based treatment plans that address both mental health and housing stability, working toward long-term solutions.
- Stay current with mental health crisis intervention techniques, best practices, and legal or policy changes relevant to the role.
- Assures that the City's mission, goals and objectives are fully supported and initiated
- Performs other related duties and responsibilities as assigned.

Job Standards

Must be able to pass a pre-employment offer: reference checks, drug screen, motor vehicle report, background and credit history check Any combination of education and experience providing the required skill and knowledge is qualifying. Typical qualifications would be equivalent to:

Education/Experience:	• High School diploma or equivalent. • Bachelor's Degree in a human services-related field (including, not limited to psychology, social work, nursing and education) + Minimum of three years of experience in behavioral or mental health services. • OR AA Degree in a human services-related field (including, not limited to psychology, social work, nursing and education) + Minimum of five years of experience in behavioral or mental health services. Or without a BA degree or AA degree minimum of seven years of experience in behavioral or mental health services.
Skills:	• Ability to handle confidential information in a sensitive manner • Ability to analyze situations and adopt a quick, effective, and reasonable course of action during stressful, emotional and/or physically taxing situations • Ability to write clear, accurate, factual, and concise reports • Excellent critical thinking skills, including, but not limited to, the ability to: make observations and remember pertinent facts; question witnesses and obtain pertinent information • Excellent oral/interpersonal communication skills. • Ability to handle stressful, hostile, or irrational persons, whether due to physical or mental impairments. • Ability to maintain intense concentration and alertness during stressful situation, particularly when preceded by extended periods of relative low stress or monotony. • Must be of good moral character • Continuous visual effort, depth perception, color vision, hearing, and speaking abilities. • Ability to perform essential duties at designated work site location at designated hours.
Knowledge:	• Proficiency with PC's, specifically mobile data units, and computer software and applications. • Knowledge of City geography and municipal boundaries. • General knowledge of office equipment, including facsimile, photo copier, telephone, calculator, and shredder • Knowledge of tools and equipment, including emergency equipment (i.e. AED, etc.), fire equipment, electronic equipment
Licenses:	• Valid Iowa Drivers' License • CPR/First Aid/AED certifications within twelve months of employment
Working Conditions:	• Long periods of sitting • Intermittent periods of standing and walking • Ability to lift, carry, push, and pull up to 20 pounds • Constant talking, hearing, tasting/smelling, near and far sight acuity, depth perception, color vision, field of vision, concentration, judgment, and writing ability • Constant exposure to weather, moving mechanical parts/hazards, and other variety of on-scene response environmental conditions • Moderate use of protective footwear, ear wear, eye wear, hard hat, protective vests, and gloves.

Safety Hazards:

- Traffic hazards
- Electrical hazards
- Fire hazards
- Exposure to violent behavior
- Exposure to toxic/caustic chemicals
- Biohazards

Note: This job description should not be construed to imply that these requirements are the exclusive standards of the position. Incumbents will follow any other instructions, and perform any other related duties, as may be required. The employer has the right to revise this job description at any time. The job description is not to be construed as a contract for employment.



Criminal Justice Information Services (CJIS) Security Policy

Version 5.9

06/01/2020

CJISD-ITS-DOC-08140-5.9



Prepared by:
CJIS Information Security Officer

Approved by:
CJIS Advisory Policy Board

EXECUTIVE SUMMARY

Law enforcement needs timely and secure access to services that provide data wherever and whenever for stopping and reducing crime. In response to these needs, the Advisory Policy Board (APB) recommended to the Federal Bureau of Investigation (FBI) that the Criminal Justice Information Services (CJIS) Division authorize the expansion of the existing security management structure in 1998. Administered through a shared management philosophy, the CJIS Security Policy contains information security requirements, guidelines, and agreements reflecting the will of law enforcement and criminal justice agencies for protecting the sources, transmission, storage, and generation of Criminal Justice Information (CJI). The Federal Information Security Management Act of 2002 provides further legal basis for the APB approved management, operational, and technical security requirements mandated to protect CJI and by extension the hardware, software and infrastructure required to enable the services provided by the criminal justice community.

The essential premise of the CJIS Security Policy is to provide appropriate controls to protect the full lifecycle of CJI, whether at rest or in transit. The CJIS Security Policy provides guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of CJI. This Policy applies to every individual—contractor, private entity, noncriminal justice agency representative, or member of a criminal justice entity—with access to, or who operate in support of, criminal justice services and information.

The CJIS Security Policy integrates presidential directives, federal laws, FBI directives and the criminal justice community's APB decisions along with nationally recognized guidance from the National Institute of Standards and Technology. The Policy is presented at both strategic and tactical levels and is periodically updated to reflect the security requirements of evolving business models. The Policy features modular sections enabling more frequent updates to address emerging threats and new security measures. The provided security criteria assists agencies with designing and implementing systems to meet a uniform level of risk and security protection while enabling agencies the latitude to institute more stringent security requirements and controls based on their business model and local needs.

The CJIS Security Policy strengthens the partnership between the FBI and CJIS Systems Agencies (CSA), including, in those states with separate authorities, the State Identification Bureaus (SIB). Further, as use of criminal history record information for noncriminal justice purposes continues to expand, the CJIS Security Policy becomes increasingly important in guiding the National Crime Prevention and Privacy Compact Council and State Compact Officers in the secure exchange of criminal justice records.

The Policy describes the vision and captures the security concepts that set the policies, protections, roles, and responsibilities with minimal impact from changes in technology. The Policy empowers CSAs with the insight and ability to tune their security programs according to their risks, needs, budgets, and resource constraints while remaining compliant with the baseline level of security set forth in this Policy. The CJIS Security Policy provides a secure framework of laws, standards, and elements of published and vetted policies for accomplishing the mission across the broad spectrum of the criminal justice and noncriminal justice communities.

CHANGE MANAGEMENT

Revision	Change Description	Created/Changed by	Date	Approved By
5	Policy Rewrite	Security Policy Working Group	2/9/2011	See Signature Page
5.1	Incorporate Calendar Year 2011 APB approved changes and administrative changes	CJIS ISO Program Office	7/13/2012	APB & Compact Council
5.2	Incorporate Calendar Year 2012 APB approved changes and administrative changes	CJIS ISO Program Office	8/9/2013	APB & Compact Council
5.3	Incorporate Calendar Year 2013 APB approved changes and administrative changes	CJIS ISO Program Office	8/4/2014	APB & Compact Council
5.4	Incorporate Calendar Year 2014 APB approved changes and administrative changes	CJIS ISO Program Office	10/6/2015	APB & Compact Council
5.5	Incorporate Calendar Year 2015 APB approved changes and administrative changes	CJIS ISO Program Office	6/1/2016	APB & Compact Council
5.6	Incorporate Calendar Year 2016 APB approved changes and administrative changes	CJIS ISO Program Office	6/5/2017	APB & Compact Council
5.7	Incorporate Calendar Year 2017 APB approved changes and administrative changes	CJIS ISO Program Office	08/16/2018	APB & Compact Council
5.8	Incorporate Calendar Year 2018 APB approved changes and administrative changes	CJIS ISO Program Office	06/01/2019	APB & Compact Council
5.9	Incorporate Calendar Year 2019 APB approved changes and administrative changes	CJIS ISO Program Office	06/01/2020	APB & Compact Council

SUMMARY OF CHANGES

Version 5.9

APB Approved Changes

1. **Section 5.13.2 Mobile Device Management (MDM):** add clarifying language, Fall 2019, APB#18, SA#3, Mobile Device Management (MDM) Requirements in the *CJIS Security Policy*.
2. **Appendix H, Security Addendum:** add example of contract addendum, Fall 2019, APB#18, SA#7, Audit of Vendor Contracts with Authorized Criminal Justice Agencies (CJAs).
3. **NOTE:** There were no Spring 2019 APB actions.

Administrative Changes¹

1. **Section 5.6.2.2.2 Advanced Authentication Decision Tree:** updated the tree description to account for direct and indirect access to CJI.
2. **Figures 9 and 10:** updated both figures to account for direct and indirect access to CJI.

KEY TO APB APPROVED CHANGES (e.g. “Fall 2013, APB#11, SA#6, add language, Future CSP for Mobile Devices”):

Fall 2013 – Advisory Policy Board cycle and year

APB# – Advisory Policy Board Topic number

SA# – Security and Access Subcommittee Topic number

Summary of change

Topic title

¹ Administrative changes are vetted through the Security and Access Subcommittee and not the entire APB process.

TABLE OF CONTENTS

Executive Summary	i
Change Management	ii
Summary of Changes	iii
Table of Contents	iv
List of Figures	ix
1 Introduction	1
1.1 Purpose	1
1.2 Scope	1
1.3 Relationship to Local Security Policy and Other Policies	1
1.4 Terminology Used in This Document	2
1.5 Distribution of the CJIS Security Policy	2
2 CJIS Security Policy Approach	3
2.1 CJIS Security Policy Vision Statement	3
2.2 Architecture Independent	3
2.3 Risk Versus Realism	3
3 Roles and Responsibilities	4
3.1 Shared Management Philosophy	4
3.2 Roles and Responsibilities for Agencies and Parties	4
3.2.1 CJIS Systems Agencies (CSA)	5
3.2.2 CJIS Systems Officer (CSO)	5
3.2.3 Terminal Agency Coordinator (TAC)	6
3.2.4 Criminal Justice Agency (CJA)	6
3.2.5 Noncriminal Justice Agency (NCJA)	6
3.2.6 Contracting Government Agency (CGA)	7
3.2.7 Agency Coordinator (AC)	7
3.2.8 CJIS Systems Agency Information Security Officer (CSA ISO)	7
3.2.9 Local Agency Security Officer (LASO)	8
3.2.10 FBI CJIS Division Information Security Officer (FBI CJIS ISO)	8
3.2.11 Repository Manager	9
3.2.12 Compact Officer	9
4 Criminal Justice Information and Personally Identifiable Information	10
4.1 Criminal Justice Information (CJI)	10
4.1.1 Criminal History Record Information (CHRI)	10
4.2 Access, Use and Dissemination of Criminal History Record Information (CHRI), NCIC Restricted Files Information, and NCIC Non-Restricted Files Information	11
4.2.1 Proper Access, Use, and Dissemination of CHRI	11
4.2.2 Proper Access, Use, and Dissemination of NCIC Restricted Files Information	11
4.2.3 Proper Access, Use, and Dissemination of NCIC Non-Restricted Files Information	11
4.2.3.1 For Official Purposes	11
4.2.3.2 For Other Authorized Purposes	12
4.2.3.3 CSO Authority in Other Circumstances	12
4.2.4 Storage	12
4.2.5 Justification and Penalties	12

4.2.5.1	Justification	12
4.2.5.2	Penalties	12
4.3	Personally Identifiable Information (PII).....	12
5	Policy and Implementation	14
5.1	Policy Area 1: Information Exchange Agreements	15
5.1.1	Information Exchange	15
5.1.1.1	Information Handling.....	15
5.1.1.2	State and Federal Agency User Agreements	15
5.1.1.3	Criminal Justice Agency User Agreements	16
5.1.1.4	Interagency and Management Control Agreements	16
5.1.1.5	Private Contractor User Agreements and CJIS Security Addendum.....	16
5.1.1.6	Agency User Agreements	17
5.1.1.7	Outsourcing Standards for Channelers	17
5.1.1.8	Outsourcing Standards for Non-Channelers	18
5.1.2	Monitoring, Review, and Delivery of Services	18
5.1.2.1	Managing Changes to Service Providers	18
5.1.3	Secondary Dissemination.....	18
5.1.4	Secondary Dissemination of Non-CHRI CJI	18
5.2	Policy Area 2: Security Awareness Training.....	20
5.2.1	Basic Security Awareness Training	20
5.2.1.1	Level One Security Awareness Training	20
5.2.1.2	Level Two Security Awareness Training	20
5.2.1.3	Level Three Security Awareness Training	21
5.2.1.4	Level Four Security Awareness Training	21
5.2.2	LASO Training.....	22
5.2.3	Security Training Records.....	22
5.3	Policy Area 3: Incident Response	24
5.3.1	Reporting Security Events.....	24
5.3.1.1	Reporting Structure and Responsibilities.....	24
5.3.1.1.1	FBI CJIS Division Responsibilities	24
5.3.1.1.2	CSA ISO Responsibilities.....	24
5.3.2	Management of Security Incidents.....	25
5.3.2.1	Incident Handling.....	25
5.3.2.2	Collection of Evidence.....	25
5.3.3	Incident Response Training.....	25
5.3.4	Incident Monitoring.....	25
5.4	Policy Area 4: Auditing and Accountability.....	27
5.4.1	Auditable Events and Content (Information Systems).....	27
5.4.1.1	Events.....	27
5.4.1.1.1	Content.....	28
5.4.2	Response to Audit Processing Failures	28
5.4.3	Audit Monitoring, Analysis, and Reporting.....	28
5.4.4	Time Stamps.....	28
5.4.5	Protection of Audit Information	28
5.4.6	Audit Record Retention.....	28
5.4.7	Logging NCIC and III Transactions.....	29

5.5	Policy Area 5: Access Control.....	30
5.5.1	Account Management	30
5.5.2	Access Enforcement.....	30
5.5.2.1	Least Privilege	31
5.5.2.2	System Access Control	31
5.5.2.3	Access Control Criteria.....	31
5.5.2.4	Access Control Mechanisms.....	31
5.5.3	Unsuccessful Login Attempts	32
5.5.4	System Use Notification.....	32
5.5.5	Session Lock	32
5.5.6	Remote Access	33
5.5.6.1	Personally Owned Information Systems.....	33
5.5.6.2	Publicly Accessible Computers	33
5.6	Policy Area 6: Identification and Authentication	35
5.6.1	Identification Policy and Procedures.....	35
5.6.1.1	Use of Originating Agency Identifiers in Transactions and Information Exchanges	35
5.6.2	Authentication Policy and Procedures	35
5.6.2.1	Standard Authenticators.....	36
5.6.2.1.1	Password	36
5.6.2.1.2	Personal Identification Number (PIN)	38
5.6.2.1.3	One-time Passwords (OTP)	38
5.6.2.2	Advanced Authentication.....	38
5.6.2.2.1	Advanced Authentication Policy and Rationale	39
5.6.2.2.2	Advanced Authentication Decision Tree	39
5.6.3	Identifier and Authenticator Management	41
5.6.3.1	Identifier Management.....	41
5.6.3.2	Authenticator Management.....	42
5.6.4	Assertions	42
5.7	Policy Area 7: Configuration Management	48
5.7.1	Access Restrictions for Changes	48
5.7.1.1	Least Functionality.....	48
5.7.1.2	Network Diagram.....	48
5.7.2	Security of Configuration Documentation	48
5.8	Policy Area 8: Media Protection.....	49
5.8.1	Media Storage and Access	49
5.8.2	Media Transport	49
5.8.2.1	Digital Media during Transport	49
5.8.2.2	Physical Media in Transit	49
5.8.3	Digital Media Sanitization and Disposal.....	49
5.8.4	Disposal of Physical Media.....	49
5.9	Policy Area 9: Physical Protection	51
5.9.1	Physically Secure Location	51
5.9.1.1	Security Perimeter.....	51
5.9.1.2	Physical Access Authorizations.....	51
5.9.1.3	Physical Access Control	51

5.9.1.4	Access Control for Transmission Medium	51
5.9.1.5	Access Control for Display Medium	51
5.9.1.6	Monitoring Physical Access	52
5.9.1.7	Visitor Control	52
5.9.1.8	Delivery and Removal	52
5.9.2	Controlled Area	52
5.10	Policy Area 10: System and Communications Protection and Information Integrity	53
5.10.1	Information Flow Enforcement	53
5.10.1.1	Boundary Protection	53
5.10.1.2	Encryption	54
5.10.1.2.1	Encryption for CJI in Transit	54
5.10.1.2.2	Encryption for CJI at Rest	55
5.10.1.2.3	Public Key Infrastructure (PKI) Technology	55
5.10.1.3	Intrusion Detection Tools and Techniques	55
5.10.1.4	Voice over Internet Protocol	56
5.10.1.5	Cloud Computing	56
5.10.2	Facsimile Transmission of CJI	57
5.10.3	Partitioning and Virtualization	57
5.10.3.1	Partitioning	57
5.10.3.2	Virtualization	58
5.10.4	System and Information Integrity Policy and Procedures	58
5.10.4.1	Patch Management	58
5.10.4.2	Malicious Code Protection	59
5.10.4.3	Spam and Spyware Protection	59
5.10.4.4	Security Alerts and Advisories	59
5.10.4.5	Information Input Restrictions	60
5.11	Policy Area 11: Formal Audits	61
5.11.1	Audits by the FBI CJIS Division	61
5.11.1.1	Triennial Compliance Audits by the FBI CJIS Division	61
5.11.1.2	Triennial Security Audits by the FBI CJIS Division	61
5.11.2	Audits by the CSA	61
5.11.3	Special Security Inquiries and Audits	62
5.11.4	Compliance Subcommittees	62
5.12	Policy Area 12: Personnel Security	63
5.12.1	Personnel Screening Requirements for Individuals Requiring Unescorted Access to Unencrypted CJI	63
5.12.2	Personnel Termination	64
5.12.3	Personnel Transfer	64
5.12.4	Personnel Sanctions	64
5.13	Policy Area 13: Mobile Devices	66
5.13.1	Wireless Communications Technologies	66
5.13.1.1	802.11 Wireless Protocols	66
5.13.1.2	Cellular Devices	67
5.13.1.2.1	Cellular Service Abroad	68
5.13.1.2.2	Voice Transmissions Over Cellular Devices	68
5.13.1.3	Bluetooth	68

5.13.1.4 Mobile Hotspots.....	68
5.13.2 Mobile Device Management (MDM)	69
5.13.3 Wireless Device Risk Mitigations	69
5.13.4 System Integrity	70
5.13.4.1 Patching/Updates	70
5.13.4.2 Malicious Code Protection.....	70
5.13.4.3 Personal Firewall	70
5.13.5 Incident Response	71
5.13.6 Access Control	71
5.13.7 Identification and Authentication.....	71
5.13.7.1 Local Device Authentication	71
5.13.7.2 Advanced Authentication.....	72
5.13.7.2.1 Compensating Controls.....	72
5.13.7.3 Device Certificates.....	72
Appendices.....	A-1
Appendix A Terms and Definitions	A-1
Appendix B Acronyms.....	B-1
Appendix C Network Topology Diagrams	C-1
Appendix D Sample Information Exchange Agreements	D-1
D.1 CJIS User Agreement	D-1
D.2 Management Control Agreement.....	D-9
D.3 Noncriminal Justice Agency Agreement & Memorandum of Understanding.....	D-10
D.4 Interagency Connection Agreement	D-16
Appendix E Security Forums and Organizational Entities.....	E-1
Appendix F Sample Forms.....	F-1
F.1 Security Incident Response Form	F-2
Appendix G Best practices.....	G-1
G.1 Virtualization	G-1
G.2 Voice over Internet Protocol.....	G-4
G.3 Cloud Computing.....	G-15
G.4 Mobile Appendix	G-32
G.5 Administrator Accounts for Least Privilege and Separation of Duties.....	G-53
G.6 Encryption.....	G-66
G.7 Incident Response	G-76
G.8 Secure Coding.....	G-89
Appendix H Security Addendum	H-1
Appendix I References.....	I-1
Appendix J Noncriminal Justice Agency Supplemental Guidance	J-1
Appendix K Criminal Justice Agency Supplemental Guidance	K-1

LIST OF FIGURES

Figure 1 – Overview Diagram of Strategic Functions and Policy Components	4
Figure 2 – Dissemination of restricted and non-restricted NCIC data.....	13
Figure 3 – Information Exchange Agreements Implemented by a Local Police Department	19
Figure 4 – Security Awareness Training Use Cases	22
Figure 5 – Incident Response Process Initiated by an Incident in a Local Police Department	26
Figure 6 – Local Police Department's Use of Audit Logs	29
Figure 7 – A Local Police Department's Access Controls	34
Figure 8 – Advanced Authentication Use Cases.....	42
Figure 9 – Authentication Decision for Known Location	46
Figure 10 – Authentication Decision for Unknown Location	47
Figure 11 – A Local Police Department's Configuration Management Controls	48
Figure 12 – A Local Police Department's Media Management Policies.....	50
Figure 13 – A Local Police Department's Physical Protection Measures.....	52
Figure 14 – System and Communications Protection and Information Integrity Use Cases.....	60
Figure 15 – The Audit of a Local Police Department.....	62
Figure 16 – A Local Police Department's Personnel Security Controls	64

1 INTRODUCTION

This section details the purpose of this document, its scope, relationship to other information security policies, and its distribution constraints.

1.1 Purpose

The CJIS Security Policy provides Criminal Justice Agencies (CJA) and Noncriminal Justice Agencies (NCJA) with a minimum set of security requirements for access to Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Division systems and information and to protect and safeguard Criminal Justice Information (CJI). This minimum standard of security requirements ensures continuity of information protection. The essential premise of the CJIS Security Policy is to provide the appropriate controls to protect CJI, from creation through dissemination; whether at rest or in transit.

The CJIS Security Policy integrates presidential directives, federal laws, FBI directives, the criminal justice community's Advisory Policy Board (APB) decisions along with nationally recognized guidance from the National Institute of Standards and Technology (NIST) and the National Crime Prevention and Privacy Compact Council (Compact Council).

1.2 Scope

At the consent of the advisory process, and taking into consideration federal law and state statutes, the CJIS Security Policy applies to all entities with access to, or who operate in support of, FBI CJIS Division's services and information. The CJIS Security Policy provides minimum security requirements associated with the creation, viewing, modification, transmission, dissemination, storage, or destruction of CJI.

Entities engaged in the interstate exchange of CJI data for noncriminal justice purposes are also governed by the standards and rules promulgated by the Compact Council.

1.3 Relationship to Local Security Policy and Other Policies

The CJIS Security Policy may be used as the sole security policy for the agency. The local agency may complement the CJIS Security Policy with a local policy, or the agency may develop their own stand-alone security policy; however, the CJIS Security Policy shall always be the minimum standard and local policy may augment, or increase the standards, but shall not detract from the CJIS Security Policy standards.

The agency shall develop, disseminate, and maintain formal, documented procedures to facilitate the implementation of the CJIS Security Policy and, where applicable, the local security policy. The policies and procedures shall be consistent with applicable laws, executive orders, directives, policies, regulations, standards, and guidance. Procedures developed for CJIS Security Policy areas can be developed for the security program in general, and for a particular information system, when required.

This document is a compendium of applicable policies in providing guidance on the minimum security controls and requirements needed to access FBI CJIS information and services. These policies include presidential directives, federal laws, FBI directives and the criminal justice community's APB decisions. State, local, and Tribal CJA may implement more stringent policies

and requirements. Appendix I contains the references while Appendix E lists the security forums and organizational entities referenced in this document.

1.4 Terminology Used in This Document

The following terms are used interchangeably throughout this document:

- **Agency and Organization:** The two terms in this document refer to any entity that submits or receives information, by any means, to/from FBI CJIS systems or services.
- **Information and Data:** Both terms refer to CJI.
- **System, Information System, Service, or named applications like NCIC:** all refer to connections to the FBI's criminal justice information repositories and the equipment used to establish said connections.
- **References/Citations/Directives:** Appendix I contains all of the references used in this Policy and may contain additional sources that could apply to any section.

Appendix A and B provide an extensive list of the terms and acronyms.

1.5 Distribution of the CJIS Security Policy

The CJIS Security Policy, version 5.0 and later, is a publically available document and may be posted and shared without restrictions.

2 CJIS SECURITY POLICY APPROACH

The CJIS Security Policy represents the shared responsibility between FBI CJIS, CJIS Systems Agency (CSA), and the State Identification Bureaus (SIB) of the lawful use and appropriate protection of CJI. The Policy provides a baseline of security requirements for current and planned services and sets a minimum standard for new initiatives.

2.1 CJIS Security Policy Vision Statement

The executive summary of this document describes the vision in terms of business needs for confidentiality, integrity, and availability of information. The APB collaborates with the FBI CJIS Division to ensure that the Policy remains updated to meet evolving business, technology and security needs.

2.2 Architecture Independent

Due to advancing technology and evolving business models, the FBI CJIS Division is transitioning from legacy stovepipe systems and moving toward a flexible services approach. Systems such as National Crime Information Center (NCIC), National Instant Criminal Background Check System (NICS), and Next Generation Identification (NGI) will continue to evolve and may no longer retain their current system platforms, hardware, or program name. However, the data and services provided by these systems will remain stable.

The CJIS Security Policy looks at the data (information), services, and protection controls that apply regardless of the implementation architecture. Architectural independence is not intended to lessen the importance of systems, but provide for the replacement of one technology with another while ensuring the controls required to protect the information remain constant. This objective and conceptual focus on security policy areas provide the guidance and standards while avoiding the impact of the constantly changing landscape of technical innovations. The architectural independence of the Policy provides agencies with the flexibility for tuning their information security infrastructure and policies to reflect their own environments.

2.3 Risk Versus Realism

Every “shall” statement contained within the CJIS Security Policy has been scrutinized for risk versus the reality of resource constraints and real-world application. The purpose of the CJIS Security Policy is to establish the minimum security requirements; therefore, individual agencies are encouraged to implement additional controls to address agency specific risks. Each agency faces risk unique to that agency. It is quite possible that several agencies could encounter the same type of risk however depending on resources would mitigate that risk differently. In that light, a risk-based approach can be used when implementing requirements.

3 ROLES AND RESPONSIBILITIES

3.1 Shared Management Philosophy

In the scope of information security, the FBI CJIS Division employs a shared management philosophy with federal, state, local, and tribal law enforcement agencies. Although an advisory policy board for the NCIC has existed since 1969, the Director of the FBI established the CJIS APB in March 1994 to enable appropriate input and recommend policy with respect to CJIS services. Through the APB and its Subcommittees and Working Groups, consideration is given to the needs of the criminal justice and law enforcement community regarding public policy, statutory and privacy aspects, as well as national security relative to CJIS systems and information. The APB represents federal, state, local, and tribal law enforcement and criminal justice agencies throughout the United States, its territories, and Canada.

The FBI has a similar relationship with the Compact Council, which governs the interstate exchange of criminal history records for noncriminal justice purposes. The Compact Council is mandated by federal law to promulgate rules and procedures for the use of the Interstate Identification Index (III) for noncriminal justice purposes. To meet that responsibility, the Compact Council depends on the CJIS Security Policy as the definitive source for standards defining the security and privacy of records exchanged with noncriminal justice practitioners.

3.2 Roles and Responsibilities for Agencies and Parties

It is the responsibility of all agencies covered under this Policy to ensure the protection of CJI between the FBI CJIS Division and its user community. The following figure provides an abstract representation of the strategic functions and roles such as governance and operations.

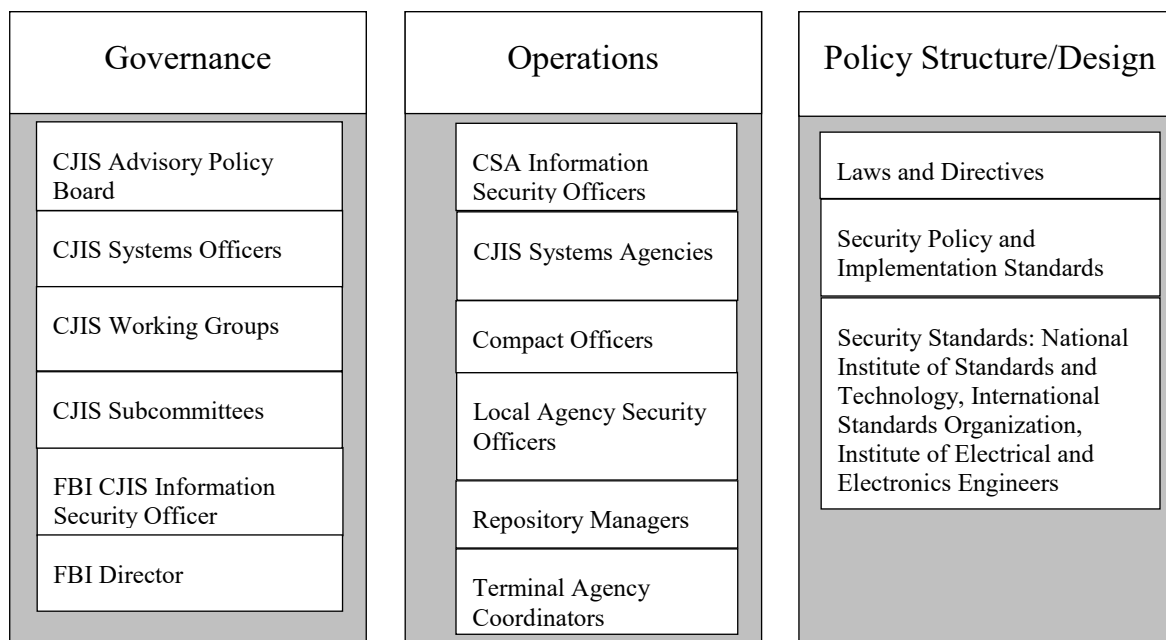


Figure 1 – Overview Diagram of Strategic Functions and Policy Components

This section provides a description of the following entities and roles:

1. CJIS Systems Agency.
2. CJIS Systems Officer.
3. Terminal Agency Coordinator.
4. Criminal Justice Agency.
5. Noncriminal Justice Agency.
6. Contracting Government Agency.
7. Agency Coordinator.
8. CJIS Systems Agency Information Security Officer.
9. Local Agency Security Officer.
10. FBI CJIS Division Information Security Officer.
11. Repository Manager.
12. Compact Officer.

3.2.1 CJIS Systems Agencies (CSA)

The CSA is responsible for establishing and administering an information technology security program throughout the CSA's user community, to include the local levels. The head of each CSA shall appoint a CJIS Systems Officer (CSO). The CSA may impose more stringent protection measures than outlined in this document. Such decisions shall be documented and kept current.

3.2.2 CJIS Systems Officer (CSO)

The CSO is an individual located within the CSA responsible for the administration of the CJIS network for the CSA. Pursuant to the Bylaws for the CJIS Advisory Policy Board and Working Groups, the role of CSO shall not be outsourced. The CSO may delegate responsibilities to subordinate agencies. The CSO shall set, maintain, and enforce the following:

1. Standards for the selection, supervision, and separation of personnel who have access to CJI.
2. Policy governing the operation of computers, access devices, circuits, hubs, routers, firewalls, and other components that comprise and support a telecommunications network and related CJIS systems used to process, store, or transmit CJI, guaranteeing the priority, confidentiality, integrity, and availability of service needed by the criminal justice community.
 - a. Ensure appropriate use, enforce system discipline, and ensure CJIS Division operating procedures are followed by all users of the respective services and information.
 - b. Ensure state/federal agency compliance with policies approved by the APB and adopted by the FBI.

- c. Ensure the appointment of the CSA ISO and determine the extent of authority to the CSA ISO.
 - d. Ensure the designation of a Terminal Agency Coordinator (TAC) within each agency with devices accessing CJIS systems.
 - e. Ensure each agency having access to CJI has someone designated as the Local Agency Security Officer (LASO).
 - f. Ensure each LASO receives enhanced security awareness training (ref. Section 5.2).
 - g. Approve access to FBI CJIS systems.
 - h. Assume ultimate responsibility for managing the security of CJIS systems within their state and/or agency.
 - i. Perform other related duties outlined by the user agreements with the FBI CJIS Division.
3. Outsourcing of Criminal Justice Functions
- a. Responsibility for the management of the approved security requirements shall remain with the CJA. Security control includes the authority to enforce the standards for the selection, supervision, and separation of personnel who have access to CJI; set and enforce policy governing the operation of computers, circuits, and telecommunications terminals used to process, store, or transmit CJI; and to guarantee the priority service needed by the criminal justice community.
 - b. Responsibility for the management control of network security shall remain with the CJA. Management control of network security includes the authority to enforce the standards for the selection, supervision, and separation of personnel who have access to CJI; set and enforce policy governing the operation of circuits and network equipment used to transmit CJI; and to guarantee the priority service as determined by the criminal justice community.

3.2.3 Terminal Agency Coordinator (TAC)

The TAC serves as the point-of-contact at the local agency for matters relating to CJIS information access. The TAC administers CJIS systems programs within the local agency and oversees the agency's compliance with CJIS systems policies.

3.2.4 Criminal Justice Agency (CJA)

A CJA is defined as a court, a governmental agency, or any subunit of a governmental agency which performs the administration of criminal justice pursuant to a statute or executive order and which allocates a substantial part of its annual budget to the administration of criminal justice. State and federal Inspectors General Offices are included.

3.2.5 Noncriminal Justice Agency (NCJA)

A NCJA is defined (for the purposes of access to CJI) as an entity or any subunit thereof that provides services primarily for purposes other than the administration of criminal justice.

3.2.6 Contracting Government Agency (CGA)

A CGA is a government agency, whether a CJA or a NCJA, that enters into an agreement with a private contractor subject to the CJIS Security Addendum. The CGA entering into an agreement with a contractor shall appoint an agency coordinator.

3.2.7 Agency Coordinator (AC)

An AC is a staff member of the CGA who manages the agreement between the Contractor and agency. The AC shall be responsible for the supervision and integrity of the system, training and continuing education of employees and operators, scheduling of initial training and testing, and certification testing and all required reports by NCIC. The AC shall:

1. Understand the communications, records capabilities, and needs of the Contractor which is accessing federal and state records through or because of its relationship with the CGA.
2. Participate in related meetings and provide input and comments for system improvement.
3. Receive information from the CGA (e.g., system updates) and disseminate it to appropriate Contractor employees.
4. Maintain and update manuals applicable to the effectuation of the agreement, and provide them to the Contractor.
5. Maintain up-to-date records of Contractor's employees who access the system, including name, date of birth, social security number, date fingerprint card(s) submitted, date security clearance issued, and date initially trained, tested, certified or recertified (if applicable).
6. Train or ensure the training of Contractor personnel. If Contractor personnel access NCIC, schedule the operators for testing or a certification exam with the CSA staff, or AC staff with permission from the CSA staff. Schedule new operators for the certification exam within six (6) months of assignment. Schedule certified operators for biennial re-certification testing within thirty (30) days prior to the expiration of certification. Schedule operators for other mandated class.
7. The AC will not permit an untrained/untested or non-certified Contractor employee to access CJI or systems supporting CJI where access to CJI can be gained.
8. Where appropriate, ensure compliance by the Contractor with NCIC validation requirements.
9. Provide completed applicant fingerprint cards on each Contractor employee who accesses the system to the CGA (or, where appropriate, CSA) for criminal background investigation prior to such employee accessing the system.
10. Any other responsibility for the AC promulgated by the FBI.

3.2.8 CJIS Systems Agency Information Security Officer (CSA ISO)

The CSA ISO shall:

1. Serve as the security point of contact (POC) to the FBI CJIS Division ISO.

2. Document technical compliance with the CJIS Security Policy with the goal to assure the confidentiality, integrity, and availability of criminal justice information to the user community throughout the CSA's user community, to include the local level.
3. Document and provide assistance for implementing the security-related controls for the Interface Agency and its users.
4. Establish a security incident response and reporting procedure to discover, investigate, document, and report to the CSA, the affected criminal justice agency, and the FBI CJIS Division ISO major incidents that significantly endanger the security or integrity of CJI.

3.2.9 Local Agency Security Officer (LASO)

Each LASO shall:

1. Identify who is using the CSA approved hardware, software, and firmware and ensure no unauthorized individuals or processes have access to the same.
2. Identify and document how the equipment is connected to the state system.
3. Ensure that personnel security screening procedures are being followed as stated in this Policy.
4. Ensure the approved and appropriate security measures are in place and working as expected.
5. Support policy compliance and ensure the CSA ISO is promptly informed of security incidents.

3.2.10 FBI CJIS Division Information Security Officer (FBI CJIS ISO)

The FBI CJIS ISO shall:

1. Maintain the CJIS Security Policy.
2. Disseminate the FBI Director approved CJIS Security Policy.
3. Serve as a liaison with the CSA's ISO and with other personnel across the CJIS community and in this regard provide technical guidance as to the intent and implementation of operational and technical policy issues.
4. Serve as a point-of-contact (POC) for computer incident notification and distribution of security alerts to the CSOs and ISOs.
5. Assist with developing audit compliance guidelines as well as identifying and reconciling security-related issues.
6. Develop and participate in information security training programs for the CSOs and ISOs, and provide a means by which to acquire feedback to measure the effectiveness and success of such training.
7. Maintain a security policy resource center (SPRC) on FBI.gov and keep the CSOs and ISOs updated on pertinent information.

3.2.11 Repository Manager

The State Identification Bureau (SIB) Chief, i.e. Repository Manager or Chief Administrator, is the designated manager of the agency having oversight responsibility for a state's fingerprint identification services. If both state fingerprint identification services and CJIS systems control are managed within the same state agency, the SIB Chief and CSO may be the same person.

3.2.12 Compact Officer

Pursuant to the National Crime Prevention and Privacy Compact, each party state shall appoint a Compact Officer who shall ensure that Compact provisions and rules, procedures, and standards established by the Compact Council are complied with in their respective state.

4 CRIMINAL JUSTICE INFORMATION AND PERSONALLY IDENTIFIABLE INFORMATION

4.1 Criminal Justice Information (CJI)

Criminal Justice Information is the term used to refer to all of the FBI CJIS provided data necessary for law enforcement and civil agencies to perform their missions including, but not limited to biometric, identity history, biographic, property, and case/incident history data. The following categories of CJI describe the various data sets housed by the FBI CJIS architecture:

1. Biometric Data—data derived from one or more intrinsic physical or behavioral traits of humans typically for the purpose of uniquely identifying individuals from within a population. Used to identify individuals, to include: fingerprints, palm prints, iris scans, and facial recognition data.
2. Identity History Data—textual data that corresponds with an individual’s biometric data, providing a history of criminal and/or civil events for the identified individual.
3. Biographic Data—information about individuals associated with a unique case, and not necessarily connected to identity data. Biographic data does not provide a history of an individual, only information related to a unique case.
4. Property Data—information about vehicles and property associated with crime when accompanied by any personally identifiable information (PII).
5. Case/Incident History—information about the history of criminal incidents.

The following type of data are exempt from the protection levels required for CJI: transaction control type numbers (e.g., ORI, NIC, UCN, etc.) when not accompanied by information that reveals CJI or PII.

The intent of the CJIS Security Policy is to ensure the protection of the aforementioned CJI until the information is: released to the public via authorized dissemination (e.g. within a court system; presented in crime reports data; released in the interest of public safety); purged or destroyed in accordance with applicable record retention rules. CJI introduced into the court system pursuant to a judicial proceeding that can be released to the public via a public records request is not subject to the CJIS Security Policy.

4.1.1 Criminal History Record Information (CHRI)

Criminal History Record Information (CHRI), sometimes informally referred to as “restricted data”, is a subset of CJI. Due to its comparatively sensitive nature, additional controls are required for the access, use and dissemination of CHRI. In addition to the dissemination restrictions outlined below, Title 28, Part 20, Code of Federal Regulations (CFR), defines CHRI and provides the regulatory guidance for dissemination of CHRI. While the CJIS Security Policy attempts to be architecturally independent, the III and the NCIC are specifically identified in Title 28, Part 20, CFR, and the NCIC Operating Manual, as associated with CHRI.

4.2 Access, Use and Dissemination of Criminal History Record Information (CHRI), NCIC Restricted Files Information, and NCIC Non-Restricted Files Information

This section describes the requirements for the access, use and dissemination of CHRI, NCIC restricted files information, and NCIC non-restricted files information.

4.2.1 Proper Access, Use, and Dissemination of CHRI

Information obtained from the III is considered CHRI. Rules governing the access, use, and dissemination of CHRI are found in Title 28, Part 20, CFR. The III shall be accessed only for an authorized purpose. Further, CHRI shall only be used for an authorized purpose consistent with the purpose for which III was accessed. Dissemination to another agency is authorized if (a) the other agency is an Authorized Recipient of such information and is being serviced by the accessing agency, or (b) the other agency is performing personnel and appointment functions for criminal justice employment applicants.

4.2.2 Proper Access, Use, and Dissemination of NCIC Restricted Files Information

The NCIC hosts restricted files and non-restricted files. NCIC restricted files are distinguished from NCIC non-restricted files by the policies governing their access and use. Proper access to, use, and dissemination of data from restricted files shall be consistent with the access, use, and dissemination policies concerning the III described in Title 28, Part 20, CFR, and the NCIC Operating Manual. The restricted files, which shall be protected as CHRI, are as follows:

1. Gang Files
2. Known or Appropriately Suspected Terrorist Files
3. Supervised Release Files
4. National Sex Offender Registry Files
5. Historical Protection Order Files of the NCIC
6. Identity Theft Files
7. Protective Interest Files
8. Person With Information (PWI) data in the Missing Person Files
9. Violent Person File
10. NICS Denied Transactions File

The remaining NCIC files are considered non-restricted files.

4.2.3 Proper Access, Use, and Dissemination of NCIC Non-Restricted Files Information

4.2.3.1 For Official Purposes

NCIC non-restricted files are those not listed as restricted files in Section 4.2.2. NCIC non-restricted files information may be accessed and used for any authorized purpose consistent with

the inquiring agency's responsibility. Information obtained may be disseminated to (a) other government agencies or (b) private entities authorized by law to receive such information for any purpose consistent with their responsibilities.

4.2.3.2 For Other Authorized Purposes

NCIC non-restricted files may be accessed for other purposes consistent with the resources of the inquiring agency; however, requests for bulk data are discouraged. Information derived from NCIC non-restricted files for other than law enforcement purposes can be used by authorized criminal justice personnel only to confirm the status of a person or property (i.e., wanted or stolen). An inquiring agency is authorized to charge a nominal administrative fee for such service. Non-restricted files information shall not be disseminated commercially.

A response to a NCIC person inquiry may include NCIC restricted files information as well as NCIC non-restricted files information. Agencies shall not disseminate restricted files information for purposes other than law enforcement.

4.2.3.3 CSO Authority in Other Circumstances

If no federal, state or local law or policy prohibition exists, the CSO may exercise discretion to approve or deny dissemination of NCIC non-restricted file information.

4.2.4 Storage

When CHRI is stored, agencies shall establish appropriate administrative, technical and physical safeguards to ensure the security and confidentiality of the information. These records shall be stored for extended periods only when they are key elements for the integrity and/or utility of case files and/or criminal record files. See Section 5.9 for physical security controls.

4.2.5 Justification and Penalties

4.2.5.1 Justification

In addition to the use of purpose codes and logging information, all users shall provide a reason for all III inquiries whenever requested by NCIC System Managers, CSAs, local agency administrators, or their representatives.

4.2.5.2 Penalties

Improper access, use or dissemination of CHRI and NCIC Non-Restricted Files information is serious and may result in administrative sanctions including, but not limited to, termination of services and state and federal criminal penalties.

4.3 Personally Identifiable Information (PII)

For the purposes of this document, PII is information which can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name. Any FBI CJIS provided data maintained by an agency, including but not limited to, education, financial transactions, medical history, and criminal or employment history may include PII. A criminal history record for

example inherently contains PII as would a Law Enforcement National Data Exchange (N-DEx) case file.

PII shall be extracted from CJI for the purpose of official business only. Agencies shall develop policies, based on state and local privacy rules, to ensure appropriate controls are applied when handling PII extracted from CJI. Due to the expansive nature of PII, this Policy does not specify auditing, logging, or personnel security requirements associated with the life cycle of PII.

Figure 2 – Dissemination of restricted and non-restricted NCIC data

A citizen of Springfield went to the Springfield Police Department to request whether his new neighbor, who had been acting suspiciously, had an outstanding warrant. The Springfield Police Department ran an NCIC persons inquiry, which produced a response that included a Wanted Person File (non-restricted file) record and a Known or Appropriately Suspected Terrorist File (restricted file) record. The Springfield Police Department advised the citizen of the outstanding warrant, but did not disclose any information concerning the subject being a known or appropriately suspected terrorist.

5 POLICY AND IMPLEMENTATION

The policy areas focus upon the data and services that the FBI CJIS Division exchanges and provides to the criminal justice community and its partners. Each policy area provides both strategic reasoning and tactical implementation requirements and standards.

While the major theme of the policy areas is concerned with electronic exchange directly with the FBI, it is understood that further dissemination of CJI to Authorized Recipients by various means (hard copy, e-mail, web posting, etc.) constitutes a significant portion of CJI exchanges. Regardless of its form, use, or method of dissemination, CJI requires protection throughout its life.

Not every consumer of FBI CJIS services will encounter all of the policy areas therefore the circumstances of applicability are based on individual agency/entity configurations and usage. Use cases within each of the policy areas will help users relate the Policy to their own agency circumstances. The policy areas are:

- Policy Area 1—Information Exchange Agreements
- Policy Area 2—Security Awareness Training
- Policy Area 3—Incident Response
- Policy Area 4—Auditing and Accountability
- Policy Area 5—Access Control
- Policy Area 6—Identification and Authentication
- Policy Area 7—Configuration Management
- Policy Area 8—Media Protection
- Policy Area 9—Physical Protection
- Policy Area 10—Systems and Communications Protection and Information Integrity
- Policy Area 11—Formal Audits
- Policy Area 12—Personnel Security
- Policy Area 13—Mobile Devices

5.1 Policy Area 1: Information Exchange Agreements

The information shared through communication mediums shall be protected with appropriate security safeguards. The agreements established by entities sharing information across systems and communications mediums are vital to ensuring all parties fully understand and agree to a set of security standards.

5.1.1 Information Exchange

Before exchanging CJI, agencies shall put formal agreements in place that specify security controls. The exchange of information may take several forms including electronic mail, instant messages, web services, facsimile, hard copy, and information systems sending, receiving and storing CJI.

Information exchange agreements outline the roles, responsibilities, and data ownership between agencies and any external parties. Information exchange agreements for agencies sharing CJI data that is sent to and/or received from the FBI CJIS shall specify the security controls and conditions described in this document.

Information exchange agreements shall be supported by documentation committing both parties to the terms of information exchange. As described in subsequent sections, different agreements and policies apply, depending on whether the parties involved are CJAs or NCJAs. See Appendix D for examples of Information Exchange Agreements.

There may be instances, on an ad-hoc basis, where CJI is authorized for further dissemination to Authorized Recipients not covered by an information exchange agreement with the releasing agency. In these instances the dissemination of CJI is considered to be secondary dissemination. Law Enforcement and civil agencies shall have a local policy to validate a requestor of CJI as an authorized recipient before disseminating CJI. See Section 5.1.3 for secondary dissemination guidance.

5.1.1.1 Information Handling

Procedures for handling and storage of information shall be established to protect that information from unauthorized disclosure, alteration or misuse. Using the requirements in this Policy as a starting point, the procedures shall apply to the handling, processing, storing, and communication of CJI. These procedures apply to the exchange of CJI no matter the form of exchange.

The policies for information handling and protection also apply to using CJI shared with or received from FBI CJIS for noncriminal justice purposes. In general, a noncriminal justice purpose includes the use of criminal history records for purposes authorized by federal or state law other than purposes relating to the administration of criminal justice, including – but not limited to - employment suitability, licensing determinations, immigration and naturalization matters, and national security clearances.

5.1.1.2 State and Federal Agency User Agreements

Each CSA head or SIB Chief shall execute a signed written user agreement with the FBI CJIS Division stating their willingness to demonstrate conformity with this Policy before accessing and participating in CJIS records information programs. This agreement shall include the standards and sanctions governing utilization of CJIS systems. As coordinated through the particular CSA

or SIB Chief, each Interface Agency shall also allow the FBI to periodically test the ability to penetrate the FBI's network through the external network connection or system. All user agreements with the FBI CJIS Division shall be coordinated with the CSA head.

5.1.1.3 Criminal Justice Agency User Agreements

Any CJA receiving access to CJI shall enter into a signed written agreement with the appropriate signatory authority of the CSA providing the access. The written agreement shall specify the FBI CJIS systems and services to which the agency will have access, and the FBI CJIS Division policies to which the agency must adhere. These agreements shall include:

1. Audit.
2. Dissemination.
3. Hit confirmation.
4. Logging.
5. Quality Assurance (QA).
6. Screening (Pre-Employment).
7. Security.
8. Timeliness.
9. Training.
10. Use of the system.
11. Validation.

5.1.1.4 Interagency and Management Control Agreements

A NCJA (government) designated to perform criminal justice functions for a CJA shall be eligible for access to the CJI. Access shall be permitted when such designation is authorized pursuant to executive order, statute, regulation, or interagency agreement. The NCJA shall sign and execute a management control agreement (MCA) with the CJA, which stipulates management control of the criminal justice function remains solely with the CJA. The MCA may be a separate document or included with the language of an interagency agreement. An example of an NCJA (government) is a city information technology (IT) department.

5.1.1.5 Private Contractor User Agreements and CJIS Security Addendum

The CJIS Security Addendum is a uniform addendum to an agreement between the government agency and a private contractor, approved by the Attorney General of the United States, which specifically authorizes access to CHRI, limits the use of the information to the purposes for which it is provided, ensures the security and confidentiality of the information is consistent with existing regulations and the CJIS Security Policy, provides for sanctions, and contains such other provisions as the Attorney General may require.

Private contractors who perform criminal justice functions shall meet the same training and certification criteria required by governmental agencies performing a similar function, and shall be subject to the same extent of audit review as are local user agencies. All private contractors who perform criminal justice functions shall acknowledge, via signing of the CJIS Security

Addendum Certification page, and abide by all aspects of the CJIS Security Addendum. The CJIS Security Addendum is presented in Appendix H. Modifications to the CJIS Security Addendum shall be enacted only by the FBI.

1. Private contractors designated to perform criminal justice functions for a CJA shall be eligible for access to CJI. Access shall be permitted pursuant to an agreement which specifically identifies the agency's purpose and scope of providing services for the administration of criminal justice. The agreement between the CJA and the private contractor shall incorporate the CJIS Security Addendum approved by the Director of the FBI, acting for the U.S. Attorney General, as referenced in Title 28 CFR 20.33 (a)(7).
2. Private contractors designated to perform criminal justice functions on behalf of a NCJA (government) shall be eligible for access to CJI. Access shall be permitted pursuant to an agreement which specifically identifies the agency's purpose and scope of providing services for the administration of criminal justice. The agreement between the NCJA and the private contractor shall incorporate the CJIS Security Addendum approved by the Director of the FBI, acting for the U.S. Attorney General, as referenced in Title 28 CFR 20.33 (a)(7).

5.1.1.6 Agency User Agreements

A NCJA (public) designated to request civil fingerprint-based background checks, with the full consent of the individual to whom a background check is taking place, for noncriminal justice functions, shall be eligible for access to CJI. Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General. A NCJA (public) receiving access to CJI shall enter into a signed written agreement with the appropriate signatory authority of the CSA/SIB providing the access. An example of a NCJA (public) is a county school board.

A NCJA (private) designated to request civil fingerprint-based background checks, with the full consent of the individual to whom a background check is taking place, for noncriminal justice functions, shall be eligible for access to CJI. Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General. A NCJA (private) receiving access to CJI shall enter into a signed written agreement with the appropriate signatory authority of the CSA, SIB, or authorized agency providing the access. An example of a NCJA (private) is a local bank.

All NCJAs accessing CJI shall be subject to all pertinent areas of the CJIS Security Policy (see Appendix J for supplemental guidance). Each NCJA that directly accesses FBI CJI shall also allow the FBI to periodically test the ability to penetrate the FBI's network through the external network connection or system.

5.1.1.7 Outsourcing Standards for Channelers

Channelers designated to request civil fingerprint-based background checks or noncriminal justice ancillary functions on behalf of a NCJA (public) or NCJA (private) for noncriminal justice functions shall be eligible for access to CJI. Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General. All Channelers accessing CJI shall be subject to the terms and conditions described in the Compact

Council Security and Management Control Outsourcing Standard. Each Channeler that directly accesses CJI shall also allow the FBI to conduct periodic penetration testing.

Channelers leveraging CJI to perform civil functions on behalf of an Authorized Recipient shall meet the same training and certification criteria required by governmental agencies performing a similar function, and shall be subject to the same extent of audit review as are local user agencies.

5.1.1.8 Outsourcing Standards for Non-Channelers

Contractors designated to perform noncriminal justice ancillary functions on behalf of a NCJA (public) or NCJA (private) for noncriminal justice functions shall be eligible for access to CJI. Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General. All contractors accessing CJI shall be subject to the terms and conditions described in the Compact Council Outsourcing Standard for Non-Channelers. Contractors leveraging CJI to perform civil functions on behalf of an Authorized Recipient shall meet the same training and certification criteria required by governmental agencies performing a similar function, and shall be subject to the same extent of audit review as are local user agencies.

5.1.2 Monitoring, Review, and Delivery of Services

As specified in the interagency agreements, MCAs, and contractual agreements with private contractors, the services, reports and records provided by the service provider shall be regularly monitored and reviewed. The CJA, authorized agency, or FBI shall maintain sufficient overall control and visibility into all security aspects to include, but not limited to, identification of vulnerabilities and information security incident reporting/response. The incident reporting/response process used by the service provider shall conform to the incident reporting/response specifications provided in this Policy.

5.1.2.1 Managing Changes to Service Providers

Any changes to services provided by a service provider shall be managed by the CJA, authorized agency, or FBI. This includes provision of services, changes to existing services, and new services. Evaluation of the risks to the agency shall be undertaken based on the criticality of the data, system, and the impact of the change.

5.1.3 Secondary Dissemination

If CHRI is released to another authorized agency, and that agency was not part of the releasing agency's primary information exchange agreement(s), the releasing agency shall log such dissemination.

5.1.4 Secondary Dissemination of Non-CHRI CJI

If CJI does not contain CHRI and is not part of an information exchange agreement then it does not need to be logged. Dissemination shall conform to the local policy validating the requestor of the CJI as an employee and/or contractor of a law enforcement agency or civil agency requiring the CJI to perform their mission or a member of the public receiving CJI via authorized dissemination.

Figure 3 – Information Exchange Agreements Implemented by a Local Police Department

A local police department executed a Memorandum of Understanding (MOU) for the interface with their state CSA. The local police department also executed an MOU (which included an MCA) with the county information technology (IT) department for the day-to-day operations of their criminal-justice infrastructure. The county IT department, in turn, outsourced operations to a local vendor who signed the CJIS Security Addendum.

5.2 Policy Area 2: Security Awareness Training

Security training is key to the human element of information security. All users with authorized access to CJI should be made aware of their individual responsibilities and expected behavior when accessing CJI and the systems which process CJI. LASOs require enhanced training on the specific duties and responsibilities of those positions and the impact those positions have on the overall security of information systems.

5.2.1 Basic Security Awareness Training

Basic security awareness training shall be required within six months of initial assignment, and biennially thereafter, for all personnel who have access to CJI to include all personnel who have unescorted access to a physically secure location. The CSO/SIB Chief may accept the documentation of the completion of security awareness training from another agency. Accepting such documentation from another agency means that the accepting agency assumes the risk that the training may not meet a particular requirement or process required by federal, state, or local laws.

A significant number of topics can be mentioned and briefly discussed in any awareness session or campaign. To help further the development and implementation of individual agency security awareness training programs the following baseline guidance is provided.

5.2.1.1 Level One Security Awareness Training

At a minimum, the following topics shall be addressed as baseline security awareness training for all personnel who have unescorted access to a physically secure location:

1. Individual responsibilities and expected behavior with regard to being in the vicinity of CJI usage and/or terminals.
2. Implications of noncompliance.
3. Incident response (Identify points of contact and individual actions).
4. Visitor control and physical access to spaces—discuss applicable physical security policy and procedures, e.g., challenge strangers, report unusual activity, etc.

5.2.1.2 Level Two Security Awareness Training

In addition to 5.2.1.1 above, the following topics, at a minimum, shall be addressed as baseline security awareness training for all authorized personnel with access to CJI:

1. Media protection.
2. Protect information subject to confidentiality concerns — hardcopy through destruction.
3. Proper handling and marking of CJI.
4. Threats, vulnerabilities, and risks associated with handling of CJI.
5. Social engineering.
6. Dissemination and destruction.

5.2.1.3 Level Three Security Awareness Training

In addition to 5.2.1.1 and 5.2.1.2 above, the following topics, at a minimum, shall be addressed as baseline security awareness training for all authorized personnel with both physical and logical access to CJJ:

1. Rules that describe responsibilities and expected behavior with regard to information system usage.
2. Password usage and management—including creation, frequency of changes, and protection.
3. Protection from viruses, worms, Trojan horses, and other malicious code.
4. Unknown e-mail/attachments.
5. Web usage—allowed versus prohibited; monitoring of user activity.
6. Spam.
7. Physical Security—increases in risks to systems and data.
8. Handheld device security issues—address both physical and wireless security issues.
9. Use of encryption and the transmission of sensitive/confidential information over the Internet—address agency policy, procedures, and technical contact for assistance.
10. Laptop security—address both physical and information security issues.
11. Personally owned equipment and software—state whether allowed or not (e.g., copyrights).
12. Access control issues—address least privilege and separation of duties.
13. Individual accountability—explain what this means in the agency.
14. Use of acknowledgement statements—passwords, access to systems and data, personal use and gain.
15. Desktop security—discuss use of screensavers, restricting visitors' view of information on screen (mitigating “shoulder surfing”), battery backup devices, allowed access to systems.
16. Protect information subject to confidentiality concerns—in systems, archived, on backup media, and until destroyed.
17. Threats, vulnerabilities, and risks associated with accessing CJIS Service systems and services.

5.2.1.4 Level Four Security Awareness Training

In addition to 5.2.1.1, 5.2.1.2, and 5.1.2.3 above, the following topics at a minimum shall be addressed as baseline security awareness training for all Information Technology personnel (system administrators, security administrators, network administrators, etc.):

1. Protection from viruses, worms, Trojan horses, and other malicious code—scanning, updating definitions.
2. Data backup and storage—centralized or decentralized approach.

3. Timely application of system patches—part of configuration management.
4. Access control measures.
5. Network infrastructure protection measures.

5.2.2 LASO Training

LASO training shall be required prior to assuming duties but no later than six months after initial assignment, and annually thereafter.

At a minimum, the following topics shall be addressed as enhanced security awareness training for a LASO:

1. The roles and responsibilities listed in CJIS Security Policy Section 3.2.9.
2. Additional state/local/tribal/federal agency LASO roles and responsibilities.
3. Summary of audit findings from previous state audits of local agencies.
4. Findings from the last FBI CJIS Division audit of the CSA.
5. Most recent changes to the CJIS Security Policy.

5.2.3 Security Training Records

Records of individual basic security awareness training and specific information system security training shall be documented, kept current, and maintained by the CSO/SIB Chief/Compact Officer. Maintenance of training records can be delegated to the local level.

Figure 4 – Security Awareness Training Use Cases

Use Case 1 - Security Awareness Training Program Implementation by a Local Police Department

A local police department with a staff of 20 sworn criminal justice professionals and 15 support personnel worked with a vendor to develop role-specific security-awareness training, and required all staff to complete this training upon assignment and every two years thereafter. The local police department scheduled the sworn law-enforcement training to coincide with their NCIC certification training. The vendor maintained the training records for the police department's entire staff, and provided reporting to the department to help it ensure compliance with the CJIS Security Policy.

Use Case 2 - Level One Security Awareness Training

A local police department hires custodial staff that will have physical access throughout the PD (a physically secure location) after normal business hours to clean the facility. These personnel have unescorted access to a physically secure location and therefore must be given the baseline security awareness training on all the topics identified in CSP Section 5.2.1.1 Level One Security Awareness Training.

Use Case 3 – Level Two Security Awareness Training

A school district maintains a locked file cabinet with hard copies of background check results of all teachers and employees which may include CJI (CHRI). Only authorized personnel who have the

ability to open the cabinet are required to be given the baseline security awareness training on all the topics identified in CSP Sections 5.2.1.1 and 5.2.1.2.

Use Case 4 – Level Three Security Awareness Training

A County Sheriff's Office has employed a number of dispatchers. Part of the function of these dispatchers is to run CJI queries at the request of the Sheriff and deputies. As part of their daily duties, the dispatchers have access to CJI both logically (running queries) and physically (printed copies of reports containing CJI). These dispatchers are entrusted with direct access to CJI and are therefore required to be given the baseline security awareness training on all the topics identified in CSP Sections 5.2.1.1, 5.2.1.2, and 5.2.1.3.

Use Case 5 – Level Four Security Awareness Training

The State Police has hired a number of system and network administrator personnel to help bolster security of the state network. Part of their daily duties may include creating accounts for new personnel, implementing security patches for existing systems, creating backups of existing systems, and implementing access controls throughout the network. These administrators have privileged access to CJI and CJI-processing systems, and are therefore required to be given the baseline security awareness training on all the topics identified in CSP Sections 5.2.1.1, 5.2.1.2, 5.2.1.3, and 5.2.1.4.

5.3 Policy Area 3: Incident Response

The security risk of both accidental and malicious attacks against government and private agencies, remains persistent in both physical and logical environments. To ensure protection of CJI, agencies shall: (i) establish operational incident handling procedures that include adequate preparation, detection, analysis, containment, recovery, and user response activities; (ii) track, document, and report incidents to appropriate agency officials and/or authorities.

ISOs have been identified as the POC on security-related issues for their respective agencies and shall ensure LASOs institute the CSA incident response reporting procedures at the local level. Appendix F contains a sample incident notification letter for use when communicating the details of a CJI-related incident to the FBI CJIS ISO.

Refer to Section 5.13.5 for additional incident response requirements related to mobile devices used to access CJI.

5.3.1 Reporting Security Events

The agency shall promptly report incident information to appropriate authorities. Security events, including identified weaknesses associated with the event, shall be communicated in a manner allowing timely corrective action to be taken. Formal event reporting and escalation procedures shall be in place. Wherever feasible, the agency shall employ automated mechanisms to assist in the reporting of security incidents. All employees, contractors and third party users shall be made aware of the procedures for reporting the different types of event and weakness that might have an impact on the security of agency assets and are required to report any security events and weaknesses as quickly as possible to the designated point of contact.

5.3.1.1 Reporting Structure and Responsibilities

5.3.1.1.1 FBI CJIS Division Responsibilities

The FBI CJIS Division shall:

1. Manage and maintain the CJIS Division's Computer Security Incident Response Capability (CSIRC).
2. Serve as a central clearinghouse for all reported intrusion incidents, security alerts, bulletins, and other security-related material.
3. Ensure additional resources for all incidents affecting FBI CJIS Division controlled systems as needed.
4. Disseminate prompt advisories of system threats and operating system vulnerabilities via the security policy resource center on FBI.gov, to include but not limited to: Product Security Bulletins, Virus Bulletins, and Security Clips.
5. Track all reported incidents and/or trends.
6. Monitor the resolution of all incidents.

5.3.1.1.2 CSA ISO Responsibilities

The CSA ISO shall:

1. Assign individuals in each state, federal, and international law enforcement organization to be the primary point of contact for interfacing with the FBI CJIS Division concerning incident handling and response.
2. Identify individuals who are responsible for reporting incidents within their area of responsibility.
3. Collect incident information from those individuals for coordination and sharing among other organizations that may or may not be affected by the incident.
4. Develop, implement, and maintain internal incident response procedures and coordinate those procedures with other organizations that may or may not be affected.
5. Collect and disseminate all incident-related information received from the Department of Justice (DOJ), FBI CJIS Division, and other entities to the appropriate local law enforcement POCs within their area.
6. Act as a single POC for their jurisdictional area for requesting incident response assistance.

5.3.2 Management of Security Incidents

A consistent and effective approach shall be applied to the management of security incidents. Responsibilities and procedures shall be in place to handle security events and weaknesses effectively once they have been reported.

5.3.2.1 Incident Handling

The agency shall implement an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery. Wherever feasible, the agency shall employ automated mechanisms to support the incident handling process.

Incident-related information can be obtained from a variety of sources including, but not limited to, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports. The agency should incorporate the lessons learned from ongoing incident handling activities into the incident response procedures and implement the procedures accordingly.

5.3.2.2 Collection of Evidence

Where a follow-up action against a person or agency after an information security incident involves legal action (either civil or criminal), evidence shall be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s).

5.3.3 Incident Response Training

The agency shall ensure general incident response roles responsibilities are included as part of required security awareness training.

5.3.4 Incident Monitoring

The agency shall track and document security incidents on an ongoing basis. The CSA ISO shall maintain completed security incident reporting forms until the subsequent FBI triennial audit or until legal action (if warranted) is complete; whichever time-frame is greater.

Figure 5 – Incident Response Process Initiated by an Incident in a Local Police Department

A state ISO received a notification from a local police department that suspicious network activity from a known botnet was detected on their network. The state ISO began the process of collecting all pertinent information about this incident, e.g. incident date/time, points-of-contact, systems affected, nature of the incident, actions taken, etc. and requested that the local police department confirm that their malware signatures were up to date. The state ISO contacted both the FBI CJIS ISO and state CSO to relay the preliminary details of this incident. The FBI CJIS ISO instructed the involved parties to continue their investigation and to submit an incident response form once all the information had been gathered. The FBI CJIS ISO contacted the lead for the FBI CSIRC to inform them that an incident response form was forthcoming. The state ISO gathered the remainder of the information from the local police department and submitted a completed incident response form to the FBI CJIS ISO who subsequently provided it to the FBI CSIRC. The FBI CSIRC notified the Department of Justice Computer Incident Response Team (DOJCIRT). The state ISO continued to monitor the situation, passing relevant details to the FBI CJIS ISO, ultimately determining that the botnet was eliminated from the local police department's infrastructure. Subsequent investigations determined that the botnet was restricted to the department's administrative infrastructure and thus no CJI was compromised.

5.4 Policy Area 4: Auditing and Accountability

Agencies shall implement audit and accountability controls to increase the probability of authorized users conforming to a prescribed pattern of behavior. Agencies shall carefully assess the inventory of components that compose their information systems to determine which security controls are applicable to the various components.

Auditing controls are typically applied to the components of an information system that provide auditing capability (servers, etc.) and would not necessarily be applied to every user-level workstation within the agency. As technology advances, more powerful and diverse functionality can be found in such devices as personal digital assistants and cellular telephones, which may require the application of security controls in accordance with an agency assessment of risk.

Refer to Section 5.13.6 for additional audit requirements related to mobile devices used to access CJI.

5.4.1 Auditable Events and Content (Information Systems)

The agency's information system shall generate audit records for defined events. These defined events include identifying significant events which need to be audited as relevant to the security of the information system. The agency shall specify which information system components carry out auditing activities. Auditing activity can affect information system performance and this issue must be considered as a separate factor during the acquisition of information systems.

The agency's information system shall produce, at the application and/or operating system level, audit records containing sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events. The agency shall periodically review and update the list of agency-defined auditable events. In the event an agency does not use an automated system, manual recording of activities shall still take place.

5.4.1.1 Events

The following events shall be logged:

1. Successful and unsuccessful system log-on attempts.
2. Successful and unsuccessful attempts to use:
 - a. access permission on a user account, file, directory or other system resource;
 - b. create permission on a user account, file, directory or other system resource;
 - c. write permission on a user account, file, directory or other system resource;
 - d. delete permission on a user account, file, directory or other system resource;
 - e. change permission on a user account, file, directory or other system resource.
3. Successful and unsuccessful attempts to change account passwords.
4. Successful and unsuccessful actions by privileged accounts (i.e. root, Oracle, DBA, admin, etc.).
5. Successful and unsuccessful attempts for users to:
 - a. access the audit log file;

- b. modify the audit log file;
- c. destroy the audit log file.

5.4.1.1.1 Content

The following content shall be included with every audited event:

1. Date and time of the event.
2. The component of the information system (e.g., software component, hardware component) where the event occurred.
3. Type of event.
4. User/subject identity.
5. Outcome (success or failure) of the event.

5.4.2 Response to Audit Processing Failures

The agency's information system shall provide alerts to appropriate agency officials in the event of an audit processing failure. Audit processing failures include, for example: software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.

5.4.3 Audit Monitoring, Analysis, and Reporting

The responsible management official shall designate an individual or position to review/analyze information system audit records for indications of inappropriate or unusual activity, investigate suspicious activity or suspected violations, to report findings to appropriate officials, and to take necessary actions. Audit review/analysis shall be conducted at a minimum once a week. The frequency of review/analysis should be increased when the volume of an agency's processing indicates an elevated need for audit review. The agency shall increase the level of audit monitoring and analysis activity within the information system whenever there is an indication of increased risk to agency operations, agency assets, or individuals based on law enforcement information, intelligence information, or other credible sources of information.

5.4.4 Time Stamps

The agency's information system shall provide time stamps for use in audit record generation. The time stamps shall include the date and time values generated by the internal system clocks in the audit records. The agency shall synchronize internal information system clocks on an annual basis.

5.4.5 Protection of Audit Information

The agency's information system shall protect audit information and audit tools from modification, deletion and unauthorized access.

5.4.6 Audit Record Retention

The agency shall retain audit records for at least one (1) year. Once the minimum retention time period has passed, the agency shall continue to retain audit records until it is determined they are no longer needed for administrative, legal, audit, or other operational purposes. This includes, for

example, retention and availability of audit records relative to Freedom of Information Act (FOIA) requests, subpoena, and law enforcement actions.

5.4.7 Logging NCIC and III Transactions

A log shall be maintained for a minimum of one (1) year on all NCIC and III transactions. The III portion of the log shall clearly identify both the operator and the authorized receiving agency. III logs shall also clearly identify the requester and the secondary recipient. The identification on the log shall take the form of a unique identifier that shall remain unique to the individual requester and to the secondary recipient throughout the minimum one year retention period.

Figure 6 – Local Police Department's Use of Audit Logs

A state CSO contacted a local police department regarding potentially inappropriate use of CHRI that was retrieved using the local department's ORI. The state CSO requested all relevant information from the police department to reconcile state NCIC and III logs against local police department logs. The police department provided the combination of their CJI processing application's logs with relevant operating system and network infrastructure logs to help verify the identity of the users conducting these queries. The review of these logs substantiated the CSO's suspicion.

5.5 Policy Area 5: Access Control

Access control provides the planning and implementation of mechanisms to restrict reading, writing, processing and transmission of CJIS information and the modification of information systems, applications, services and communication configurations allowing access to CJIS information.

Refer to Section 5.13.6 for additional access control requirements related to mobile devices used to access CJIS.

5.5.1 Account Management

The agency shall manage information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The agency shall validate information system accounts at least annually and shall document the validation process. The validation and documentation of accounts can be delegated to local agencies.

Account management includes the identification of account types (i.e., individual, group, and system), establishment of conditions for group membership, and assignment of associated authorizations. The agency shall identify authorized users of the information system and specify access rights/privileges. The agency shall grant access to the information system based on:

1. Valid need-to-know/need-to-share that is determined by assigned official duties.
2. Satisfaction of all personnel security criteria.

The agency responsible for account creation shall be notified when:

1. A user's information system usage or need-to-know or need-to-share changes.
2. A user is terminated or transferred or associated accounts are removed, disabled, or otherwise secured.

5.5.2 Access Enforcement

The information system shall enforce assigned authorizations for controlling access to the system and contained information. The information system controls shall restrict access to privileged functions (deployed in hardware, software, and firmware) and security-relevant information to explicitly authorized personnel.

Explicitly authorized personnel include, for example, security administrators, system and network administrators, and other privileged users with access to system control, monitoring, or administration functions (e.g., system administrators, information system security officers, maintainers, system programmers).

Access control policies (e.g., identity-based policies, role-based policies, rule-based policies) and associated access enforcement mechanisms (e.g., access control lists, access control matrices, cryptography) shall be employed by agencies to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, domains) in the information system.

5.5.2.1 Least Privilege

The agency shall approve individual access privileges and shall enforce physical and logical access restrictions associated with changes to the information system; and generate, retain, and review records reflecting all such changes. The agency shall enforce the most restrictive set of rights/privileges or access needed by users for the performance of specified tasks. The agency shall implement least privilege based on specific duties, operations, or information systems as necessary to mitigate risk to CJI. This limits access to CJI to only authorized personnel with the need and the right to know.

Logs of access privilege changes shall be maintained for a minimum of one year or at least equal to the agency's record retention policy – whichever is greater.

5.5.2.2 System Access Control

Access control mechanisms to enable access to CJI shall be restricted by object (e.g., data set, volumes, files, records) including the ability to read, write, or delete the objects. Access controls shall be in place and operational for all IT systems to:

1. Prevent multiple concurrent active sessions for one user identification, for those applications accessing CJI, unless the agency grants authority based upon operational business needs. Agencies shall document the parameters of the operational business needs for multiple concurrent active sessions.
2. Ensure that only authorized personnel can add, change, or remove component devices, dial-up connections, and remove or alter programs.

5.5.2.3 Access Control Criteria

Agencies shall control access to CJI based on one or more of the following:

1. Job assignment or function (i.e., the role) of the user seeking access.
2. Physical location.
3. Logical location.
4. Network addresses (e.g., users from sites within a given agency may be permitted greater access than those from outside).
5. Time-of-day and day-of-week/month restrictions.

5.5.2.4 Access Control Mechanisms

When setting up access controls, agencies shall use one or more of the following mechanisms:

1. Access Control Lists (ACLs). ACLs are a register of users (including groups, machines, processes) who have been given permission to use a particular object (system resource) and the types of access they have been permitted.
2. Resource Restrictions. Access to specific functions is restricted by never allowing users to request information, functions, or other resources for which they do not have access. Three major types of resource restrictions are: menus, database views, and network devices.

3. Encryption. Encrypted information can only be decrypted, and therefore read, by those possessing the appropriate cryptographic key. While encryption can provide strong access control, it is accompanied by the need for strong key management. Follow the guidance in Section 5.10.1.2 for encryption requirements if encryption of stored information is employed as an access enforcement mechanism.
4. Application Level. In addition to controlling access at the information system level, access enforcement mechanisms are employed at the application level to provide increased information security for the agency.

5.5.3 Unsuccessful Login Attempts

Where technically feasible, the system shall enforce a limit of no more than 5 consecutive invalid access attempts by a user (attempting to access CJI or systems with access to CJI). The system shall automatically lock the account/node for a 10 minute time period unless released by an administrator.

5.5.4 System Use Notification

The information system shall display an approved system use notification message, before granting access, informing potential users of various usages and monitoring rules. The system use notification message shall, at a minimum, provide the following information:

1. The user is accessing a restricted information system.
2. System usage may be monitored, recorded, and subject to audit.
3. Unauthorized use of the system is prohibited and may be subject to criminal and/or civil penalties.
4. Use of the system indicates consent to monitoring and recording.

The system use notification message shall provide appropriate privacy and security notices (based on associated privacy and security policies or summaries) and remain on the screen until the user acknowledges the notification and takes explicit actions to log on to the information system.

Privacy and security policies shall be consistent with applicable laws, executive orders, directives, policies, regulations, standards, and guidance. System use notification messages can be implemented in the form of warning banners displayed when individuals log in to the information system. For publicly accessible systems:

1. the system use information is available and when appropriate, is displayed before granting access;
2. any references to monitoring, recording, or auditing are in keeping with privacy accommodations for such systems that generally prohibit those activities; and
3. the notice given to public users of the information system includes a description of the authorized uses of the system.

5.5.5 Session Lock

The information system shall prevent further access to the system by initiating a session lock after a maximum of 30 minutes of inactivity, and the session lock remains in effect until the user reestablishes access using appropriate identification and authentication procedures. Users shall

directly initiate session lock mechanisms to prevent inadvertent viewing when a device is unattended. A session lock is not a substitute for logging out of the information system. In the interest of safety, devices that are: (1) part of a criminal justice conveyance; or (2) used to perform dispatch functions and located within a physically secure location; or (3) terminals designated solely for the purpose of receiving alert notifications (i.e. receive only terminals or ROT) used within physically secure location facilities that remain staffed when in operation, are exempt from this requirement. Note: an example of a session lock is a screen saver with password.

5.5.6 Remote Access

The agency shall authorize, monitor, and control all methods of remote access to the information system. Remote access is any temporary access to an agency's information system by a user (or an information system) communicating temporarily through an external, non-agency-controlled network (e.g., the Internet).

The agency shall employ automated mechanisms to facilitate the monitoring and control of remote access methods. The agency shall control all remote accesses through managed access control points. The agency may permit remote access for privileged functions only for compelling operational needs but shall document the technical and administrative process for enabling remote access for privileged functions in the security plan for the information system.

Virtual escorting of privileged functions is permitted only when all the following conditions are met:

1. The session shall be monitored at all times by an authorized escort
2. The escort shall be familiar with the system/area in which the work is being performed.
3. The escort shall have the ability to end the session at any time.
4. The remote administrative personnel connection shall be via an encrypted (FIPS 140-2 certified) path.
5. The remote administrative personnel shall be identified prior to access and authenticated prior to or during the session. This authentication may be accomplished prior to the session via an Advanced Authentication (AA) solution or during the session via active teleconference with the escort throughout the session.

5.5.6.1 Personally Owned Information Systems

A personally owned information system shall not be authorized to access, process, store or transmit CJI unless the agency has established and documented the specific terms and conditions for personally owned information system usage. When personally owned mobile devices (i.e. bring your own device [BYOD]) are authorized, they shall be controlled in accordance with the requirements in Policy Area 13: Mobile Devices.

This control does not apply to the use of personally owned information systems to access agency's information systems and information that are intended for public access (e.g., an agency's public website that contains purely public information).

5.5.6.2 Publicly Accessible Computers

Publicly accessible computers shall not be used to access, process, store or transmit CJI. Publicly accessible computers include but are not limited to: hotel business center computers, convention center computers, public library computers, public kiosk computers, etc.

Figure 7 – A Local Police Department’s Access Controls

A local police department purchased a new computer-assisted dispatch (CAD) system that integrated with their state CSA’s CJI interfaces. In doing so, the police department employed least-privilege practices to ensure that its employees were only given those privileges needed to perform their jobs, and as such, excluding IT administrators, employees had only non-administrative privileges on all equipment they used. The police department also used ACLs in the operating systems to control access to the CAD client’s executables. The CAD system used internal role-based access controls to ensure only those users that needed access to CJI were given it. The police department performed annual audits of user accounts on all systems under their control including remote access mechanisms, operating systems, and the CAD system to ensure all accounts were in valid states. The police department implemented authentication-failure account lockouts, system use notification via login banners, and screen-saver passwords on all equipment that processes CJI.

5.6 Policy Area 6: Identification and Authentication

The agency shall identify information system users and processes acting on behalf of users and authenticate the identities of those users or processes as a prerequisite to allowing access to agency information systems or services.

5.6.1 Identification Policy and Procedures

Each person who is authorized to store, process, and/or transmit CJI shall be uniquely identified. A unique identification shall also be required for all persons who administer and maintain the system(s) that access CJI or networks leveraged for CJI transit. The unique identification can take the form of a full name, badge number, serial number, or other unique alphanumeric identifier. Agencies shall require users to identify themselves uniquely before the user is allowed to perform any actions on the system. Agencies shall ensure that all user IDs belong to currently authorized users. Identification data shall be kept current by adding new users and disabling and/or deleting former users.

5.6.1.1 Use of Originating Agency Identifiers in Transactions and Information Exchanges

An FBI authorized originating agency identifier (ORI) shall be used in each transaction on CJIS systems in order to identify the sending agency and to ensure the proper level of access for each transaction. The original identifier between the requesting agency and the CSA/SIB/Channeler shall be the ORI, and other agency identifiers, such as user identification or personal identifier, an access device mnemonic, or the Internet Protocol (IP) address.

Agencies may act as a servicing agency and perform transactions on behalf of authorized agencies requesting the service. Servicing agencies performing inquiry transactions on behalf of another agency may do so using the requesting agency's ORI. Servicing agencies may also use their own ORI to perform inquiry transactions on behalf of a requesting agency if the means and procedures are in place to provide an audit trail for the current specified retention period. Because the agency performing the transaction may not necessarily be the same as the agency requesting the transaction, the CSA/SIB/Channeler shall ensure that the ORI for each transaction can be traced, via audit trail, to the specific agency which is requesting the transaction.

Audit trails can be used to identify the requesting agency if there is a reason to inquire into the details surrounding why an agency ran an inquiry on a subject. Agencies assigned a P (limited access) ORI shall not use the full access ORI of another agency to conduct an inquiry transaction.

5.6.2 Authentication Policy and Procedures

Authentication refers to mechanisms or processes that verify users are valid once they are uniquely identified. The CSA/SIB may develop an authentication strategy which centralizes oversight but decentralizes the establishment and daily administration of the security measures for access to CJI.

Each individual's identity shall be authenticated at either the local agency, CSA, SIB or Channeler level. The authentication strategy shall be part of the agency's audit for policy compliance. The FBI CJIS Division shall identify and authenticate all individuals who establish direct web-based interactive sessions with FBI CJIS Services. The FBI CJIS Division shall authenticate the ORI of all message-based sessions between the FBI CJIS Division and its customer agencies but will not

further authenticate the user nor capture the unique identifier for the originating operator because this function is performed at the local agency, CSA, SIB or Channeler level.

5.6.2.1 Standard Authenticators

Authenticators are (the something you know, something you are, or something you have) part of the identification and authentication process. Examples of standard authenticators include passwords, hard or soft tokens, biometrics, one-time passwords (OTP) and personal identification numbers (PIN). Users shall not be allowed to use the same password or PIN in the same logon sequence.

5.6.2.1.1 Password

When agencies use a password as an authenticator for an individual's unique ID, they shall use the basic password standards in 5.6.2.1.1.1, OR follow the advanced password standards in 5.6.2.1.1.2.

NOTE: There is no option to combine or select particular options between the two separate lists below.

5.6.2.1.1.1 Basic Password Standards

When agencies elect to follow the basic password standards, passwords shall:

1. Be a minimum length of eight (8) characters on all systems.
2. Not be a dictionary word or proper name.
3. Not be the same as the Userid.
4. Expire within a maximum of 90 calendar days.
5. Not be identical to the previous ten (10) passwords.
6. Not be transmitted in the clear outside the secure location.
7. Not be displayed when entered.

5.6.2.1.1.2 Advanced Password Standards

When agencies elect to follow the advanced password standards, passwords shall:

1. Passwords shall be a minimum of twenty (20) characters in length with no additional complexity requirements imposed (e.g., ASCII characters, emojis, all keyboard characters, and spaces will be acceptable).
2. Password Verifiers shall not permit the use of a stored "hint" for forgotten passwords and/or prompt subscribers to use specific types of information (e.g., "What was the name of your first pet?") when choosing a password.
3. Verifiers shall maintain a list of "banned passwords" that contains values known to be commonly-used, expected, or compromised. For example, the list may include, but is not limited to:

- a. Passwords obtained from previous breach corpuses
 - b. Dictionary words
 - c. Repetitive or sequential characters (e.g. 'aaaaaa', '1234abcd')
 - d. Context-specific words, such as the name of the service, the username, and derivatives thereof
4. When processing requests to establish and change passwords, Verifiers shall compare the prospective passwords against the "banned passwords" list.
5. If the chosen password is found to be part of a "banned passwords" list, the Verifier shall:
 - a. Advise the subscriber that they need to select a different password,
 - b. Provide the reason for rejection, and
 - c. Require the subscriber to choose a different password.
6. Verifiers shall limit the number of failed authentication attempts that can be made as described in Section 5.5.3 Unsuccessful Login Attempts.
7. Verifiers shall force a password change if there is evidence of authenticator compromise or every 365 days from the last password change.
8. Verifiers shall use approved encryption and an authenticated protected channel when requesting passwords to protect against eavesdropping and Man-in-the-Middle (MitM) attacks.
9. Verifiers shall store passwords in a manner that is resistant to offline attacks by salting and hashing the password using a one-way key derivation function when stored.
 - a. The salt shall be at least 32 bits in length.
 - b. The salt shall be chosen arbitrarily so as to minimize salt value collisions among stored hashes.

Note: Key derivation functions take a password, a salt, and a cost factor as inputs then generate a password hash. Their purpose is to make each password guessing trial by an attacker who has obtained a password hash file expensive and therefore the cost of a guessing attack high or prohibitive.
10. For each subscriber, Verifiers shall protect stored salt and resulting hash values using a password or PIN.

5.6.2.1.2 Personal Identification Number (PIN)

When agencies implement the use of a PIN as a standard authenticator, the PIN attributes shall follow the guidance in section 5.6.2.1.1 (password). When agencies utilize a PIN in conjunction with a certificate or a token (e.g. key fob with rolling numbers) for the purpose of advanced authentication, agencies shall follow the PIN attributes described below. For example: A user certificate is installed on a smartphone for the purpose of advanced authentication (AA). As the user invokes that certificate, a PIN meeting the below attributes shall be used to access the certificate for the AA process.

1. Be a minimum of six (6) digits
2. Have no repeating digits (i.e., 112233)
3. Have no sequential patterns (i.e., 123456)
4. Not be the same as the Userid.
5. Expire within a maximum of 365 calendar days.
 - a. If a PIN is used to access a soft certificate which is the second factor of authentication, AND the first factor is a password that complies with the requirements in Section 5.6.2.1.1, then the 365 day expiration requirement can be waived by the CSO.
6. Not be identical to the previous three (3) PINs.
7. Not be transmitted in the clear outside the secure location.
8. Not be displayed when entered.

EXCEPTION: When a PIN is used for local device authentication, the only requirement is that it be a minimum of six (6) digits.

5.6.2.1.3 One-time Passwords (OTP)

One-time passwords are considered a “something you have” token for authentication. Examples include bingo cards, hard or soft tokens, and out-of-band tokens (i.e. OTP received via a text message).

When agencies implement the use of an OTP as an authenticator, the OTP shall meet the requirements described below.

1. Be a minimum of six (6) randomly generated characters
2. Be valid for a single session
3. If not used, expire within a maximum of five (5) minutes after issuance

5.6.2.2 Advanced Authentication

Advanced Authentication (AA) provides for additional security to the typical user identification and authentication of login ID and password, such as: biometric systems, user-based digital certificates (e.g. public key infrastructure (PKI)), smart cards, software tokens, hardware tokens, paper (inert) tokens, out-of-band authenticators (retrieved via a separate communication service channel – e.g., authenticator is sent on demand via text message, phone call, etc.), or “Risk-based Authentication” that includes a software token element comprised of a number of factors, such as

network information, user information, positive device identification (i.e. device forensics, user pattern analysis and user binding), user profiling, and high-risk challenge/response questions.

When user-based certificates are used for authentication purposes, they shall:

1. Be specific to an individual user and not to a particular device.
2. Prohibit multiple users from utilizing the same certificate.
3. Require the user to “activate” that certificate for each use in some manner (e.g., passphrase or user-specific PIN).

5.6.2.2.1 Advanced Authentication Policy and Rationale

The requirement to use or not use AA is dependent upon the physical, personnel, and technical security controls associated with the user location and whether CJI is accessed directly or indirectly. AA shall not be required for users requesting access to CJI from within the perimeter of a physically secure location (Section 5.9), when the technical security controls have been met (Sections 5.5 and 5.10), or when the user has no ability to conduct transactional activities on state and national repositories, applications, or services (i.e. indirect access). Conversely, if the technical security controls have not been met, AA shall be required even if the request for CJI originates from within a physically secure location. Section 5.6.2.2.2 provides agencies with a decision tree to help guide AA decisions. The CSO will make the final determination of whether access is considered indirect.

The intent of AA is to meet the standards of two-factor authentication. Two-factor authentication employs the use of two of the following three factors of authentication: something you know (e.g. password), something you have (e.g. hard token), something you are (e.g. biometric). The two authentication factors shall be unique (i.e. password/token or biometric/password but not password/password or token/token).

EXCEPTION:

AA shall be required when the requested service has built AA into its processes and requires a user to provide AA before granting access. **EXAMPLES:**

1. A user, irrespective of his/her location, accesses the LEEP portal. The LEEP has AA built into its services and requires AA prior to granting access. AA is required.
2. A user, irrespective of their location, accesses a State’s portal through which access to CJI is facilitated. The State Portal has AA built into its processes and requires AA prior to granting access. AA is required.

5.6.2.2.2 Advanced Authentication Decision Tree

The following AA Decision Tree, coupled with figures 9 and 10 below, assists decision makers in determining whether or not AA is required.

1. Is the access to CJI direct access or indirect access?
 - a. If access is direct, proceed to question 2.
 - b. If access is indirect, decision tree is completed. AA is not required.
2. Can request’s physical originating location be determined?

If either (a) or (b) below are true the answer to the above question is “yes”. Proceed to question 3.

- a. The IP address is attributed to a physical structure; or
- b. The mnemonic is attributed to a specific device assigned to a specific location that is a physical structure.

If neither (a) or (b) above are true then the answer is “no”. Skip to question number 5.

3. Does request originate from within a physically secure location as described in Section 5.9.1?

If either (a) or (b) below are true the answer to the above question is “yes”. Proceed to question 4.

- a. The IP address is attributed to a physically secure location; or
- b. If a mnemonic is used it is attributed to a specific device assigned to a specific physically secure location.

If neither (a) or (b) above are true then the answer is “no”. Decision tree completed. AA required.

4. Are all required technical controls implemented at this location or at the controlling agency?

If either (a) or (b) below are true the answer to the above question is “yes”. Decision tree completed. AA is not required.

- a. Appropriate technical controls listed in Sections 5.5 and 5.10 are implemented; or
- b. The controlling agency (i.e. parent agency or agency leveraged as conduit to CJI) extends its wide area network controls down to the requesting agency and the extended controls provide assurance equal or greater to the controls listed in Sections 5.5 and 5.10.

If neither (a) or (b) above are true then the answer is “no”. Decision tree completed. AA required.

5. Does request originate from an agency-controlled user device?

If either (a) or (b) below are true the answer to the above question is “yes”. Proceed to question 6.

- a. The static IP address or MAC address can be traced to registered device; or
- b. Certificates are issued to agency managed devices only and certificate exchange is allowed only between authentication server and agency issued devices.

If neither (a) or (b) above are true then the answer is “no”. Decision tree completed. AA required.

6. Is the agency managed user device associated with and located within a criminal justice conveyance?

If any of the (a), (b), or (c) statements below is true the answer to the above question is “yes”. Proceed to Figure 9 Step 4.

- a. The static IP address or MAC address is associated with a device associated with a criminal justice conveyance; or
- b. The certificate presented is associated with a device associated with a criminal justice conveyance; or
- c. The mnemonic presented is associated with a specific device assigned and that device is attributed to a criminal justice conveyance.

If none of the (a), (b), or (c) statements above are true then the answer is “no”. Proceed to question number 7.

7. Is the user device an agency-issued and controlled smartphone or tablet?

If both (a) and (b) below are true, the answer to the above question is “yes.” Proceed to question number 8.

- a. The law enforcement agency issued the device to an individual; and
- b. The device is subject to administrative management control of the issuing agency.

If either (a) or (b) above is false, then the answer is “no.” Decision tree completed. AA required.

8. Does the agency-issued smartphone or tablet have CSO-approved AA compensating controls implemented?

If (a) and (b) below are true, the answer to the above question is “yes.” Decision tree completed. AA is not required.

- a. An agency cannot meet a requirement due to legitimate technical or business constraints; and
- b. The CSO has given written approval permitting temporary AA compensating controls to be implemented in lieu of the required AA control measures.

If either (a) or (b) above is false then the answer is “no.” Decision tree completed. AA required.

5.6.3 Identifier and Authenticator Management

The agency shall establish identifier and authenticator management processes.

5.6.3.1 Identifier Management

In order to manage user identifiers, agencies shall:

1. Uniquely identify each user.
2. Verify the identity of each user.
3. Receive authorization to issue a user identifier from an appropriate agency official.
4. Issue the user identifier to the intended party.

5. Disable the user identifier after a specified period of inactivity.
6. Archive user identifiers.

5.6.3.2 Authenticator Management

In order to manage information system authenticators, agencies shall:

1. Define initial authenticator content.
2. Establish administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators.
3. Change default authenticators upon information system installation.
4. Change/refresh authenticators periodically.

Information system authenticators include, for example, tokens, user-based PKI certificates, biometrics, passwords, and key cards. Users shall take reasonable measures to safeguard authenticators including maintaining possession of their individual authenticators, not loaning or sharing authenticators with others, and immediately reporting lost or compromised authenticators.

5.6.4 Assertions

Identity providers can be leveraged to identify individuals and assert the individual's identity to a service or to a trusted broker who will in-turn assert the identity to a service. Assertion mechanisms used to communicate the results of a remote authentication to other parties shall be:

1. Digitally signed by a trusted entity (e.g., the identity provider).
2. Obtained directly from a trusted entity (e.g. trusted broker) using a protocol where the trusted entity authenticates to the relying party using a secure protocol (e.g. transport layer security [TLS]) that cryptographically authenticates the verifier and protects the assertion.

Assertions generated by a verifier shall expire after 12 hours and shall not be accepted thereafter by the relying party.

Figure 8 – Advanced Authentication Use Cases

Use Case 1 - A Local Police Department Authentication Control Scenario

During the course of an investigation, a detective attempts to access Criminal Justice Information (CJI) from a hotel room using an agency issued mobile broadband card. To gain access, the detective first establishes the remote session via a secure virtual private network (VPN) tunnel (satisfying the requirement for encryption). Upon connecting to the agency network, the detective is challenged for a username (identification), password ("something you know"), and a one-time password OTP ("something you have") from a hardware token to satisfy the requirement for advanced authentication. Once the detective's credentials are validated, his identity is asserted by the infrastructure to all authorized applications needed to complete his queries.

Use Case 2 – Use of a Smart Card

A user is issued a smart card that is loaded with user-specific digital certificates from a terminal within a controlled area. The user selects an application that will provide access to Criminal Justice Information (CJI) then enters the proper username (identification) and password (“something you know”). Once prompted, the user connects the smart card (“something you have”) to the terminal. The user is prompted to enter a personal identification number (PIN) to unlock the smart card. Once unlocked, the smart card sends the certificates to the authentication management server at the local agency where the combined username, password, and digital user certificates are validated. The user has satisfied the requirement for AA and is granted access to CJI.

Use Case 3 – Out of Band One-Time-Password (OTP) – Mobile phone-based

Using an agency- issued laptop, a user connects to the agency network via an agency-issued mobile broadband card and an encrypted virtual private network (VPN) tunnel. As part of an on-going investigation, the user initiates an application that will permit access to Criminal Justice Information (CJI). The user is prompted to enter a username (identification) and a password (“something you know”). Once that has been completed, a text message containing a one-time password (OTP) is sent via text message (out of band) to the user’s agency-issued cell phone. The user is challenged via the CJI application for that OTP. The user enters the OTP (“something you have”) then the username, password, and OTP are validated. The user has satisfied the requirement for AA and is granted access to CJI.

Use Case 4 – Improper Use of a One-Time-Password (OTP) – Laptop

Using an agency- issued laptop, a user connects to the agency network via an agency-issued mobile broadband card and an encrypted virtual private network (VPN) tunnel. As part of an on-going investigation, the user initiates an application that will permit access to Criminal Justice Information (CJI). The user is prompted to enter a username (identification) and a password (“something you know”). Once that has been completed, a one-time password (OTP) is sent to the user’s agency-issued laptop (in band) via pop-up message. The user is challenged via the CJI application for that OTP; however, the delivery of the OTP to the device that is being used to access CJI (in band) defeats the purpose of the second factor. This method does not satisfy the requirement for AA, and therefore the user should not be granted access to CJI. See the below explanation:

This method of receiving the necessary OTP (in band) does not guarantee the authenticity of the user’s identity because anyone launching the CJI application and entering a valid username/password combination is presented the OTP via a pop-up which is intend to be the second factor of authentication. This method makes the application accessible to anyone with knowledge of the valid username and password. Potentially, this is no more secure than using only a single factor of authentication.

Use Case 5 – Risk-based Authentication (RBA) Implementation

A user has moved office locations and requires email access (containing Criminal Justice Information) via an Outlook Web Access (OWA) client utilizes a risk-based authentication (RBA) solution. The user launches the OWA client and is prompted to enter a username (identification) and a password (“something you know”). The RBA detects this computer has not previously been used by the user, is not listed under the user’s profile, and then presents high-risk challenge/response question(s) which the user is prompted to answer. Once the questions have been verified as correct, the user is authenticated and granted access to the email. Meanwhile, the RBA logs and collects a number of device forensic information and captures the user pattern analysis to update the user’s profile. The CJIS Security Policy requirements for RBA have been satisfied.

Use Case 6 – Improper Risk-based Authentication (RBA) Implementation

A user has moved office locations and requires access to email containing Criminal Justice Information (CJI) via an Outlook Web Access (OWA) client utilizing a risk-based authentication (RBA) solution. The user launches the OWA client and is prompted to enter a username (identification) and a password (“something you know”). The RBA detects this computer has not previously been used by the user and is not listed under the user’s profile. The user is prompted to answer high-risk challenge/response questions for verification and authorization to access to the email; however, if the second authentication factor is to answer additional questions presented every time the user logs on, then this solution is referred to as a knowledge-based authentic on (KBA) solution. A KBA solution does not satisfy the requirement for AA, and therefore the user should not be granted access to CJI.

See the below explanation:

A KBA solution is not a viable advanced authentication (AA) solution per the CJIS Security Policy (CSP). The KBA asks questions and compares the answers to those stored within the user’s profile. A KBA is neither a CSP compliant two factor authentication solution, nor does it meet the CSP criteria of a risk-based authentication (RBA) solution which logs and collects a number of device forensic information and captures the user pattern analysis to update the user’s profile. Using this collected data, the RBA presents challenge/response questions when changes to the user’s profile are noted versus every time the user logs in.

Use Case 7 – Advanced Authentication Compensating Controls on Agency-Issued Smartphones

An authorized user is issued a smartphone that is administratively managed by the agency-installed mobile device management (MDM) solution to ensure device compliance with the CJIS Security Policy. The user initiates an email client on the smartphone that contains emails with CJI. The email client challenges the user to enter a username (identification) and a password (one factor: something you know) which are forwarded to the local agency for authentication. The smartphone lacks the technical capability to challenge the user for a second factor of authentication. This email client is used across the state agency so access is a necessity for the user’s job functions.

An audit by the CSA identifies the agency's use of the agency smartphone as not compliant with AA requirements due to the authorized user authenticating with only one factor instead of the required two factors.

Subsequently, the agency performs a risk assessment of their smartphone authentication solution and document a legitimate technical constraint due to the lack of technical solutions for smartphone-based two-factor authentication. The risk assessment identifies the following compensating controls that, when combined with the authorized user authenticating to the local agency with their password, meet the intent of the AA requirement by providing a similar level of security:

1. Enhance smartphone policy to enable possession of the smartphone to be considered a factor of authentication (i.e. something you have). Require authorized users to treat the smartphone as a controlled device and protect it as they would a personal credit card or an issued firearm to ensure only they will be in possession of the device
2. Move the email client used to authenticate with the local agency inside an encrypted, password-protected secure container on the smartphone ensuring only the authorized user can access the email application to authenticate.

The agency submits an AA compensating controls request to the CSO outlining the technical constraint identified by the risk assessment, what compensating controls will be employed, and the desired duration of the compensating controls.

The CSO approves the agency's request and provides documentation of the approval to the agency to maintain for audit purposes. The agency enacts the compensating controls and informs agency personnel they are permitted to access CJI via the agency-issued smartphone.

Figure 9 – Authentication Decision for Known Location

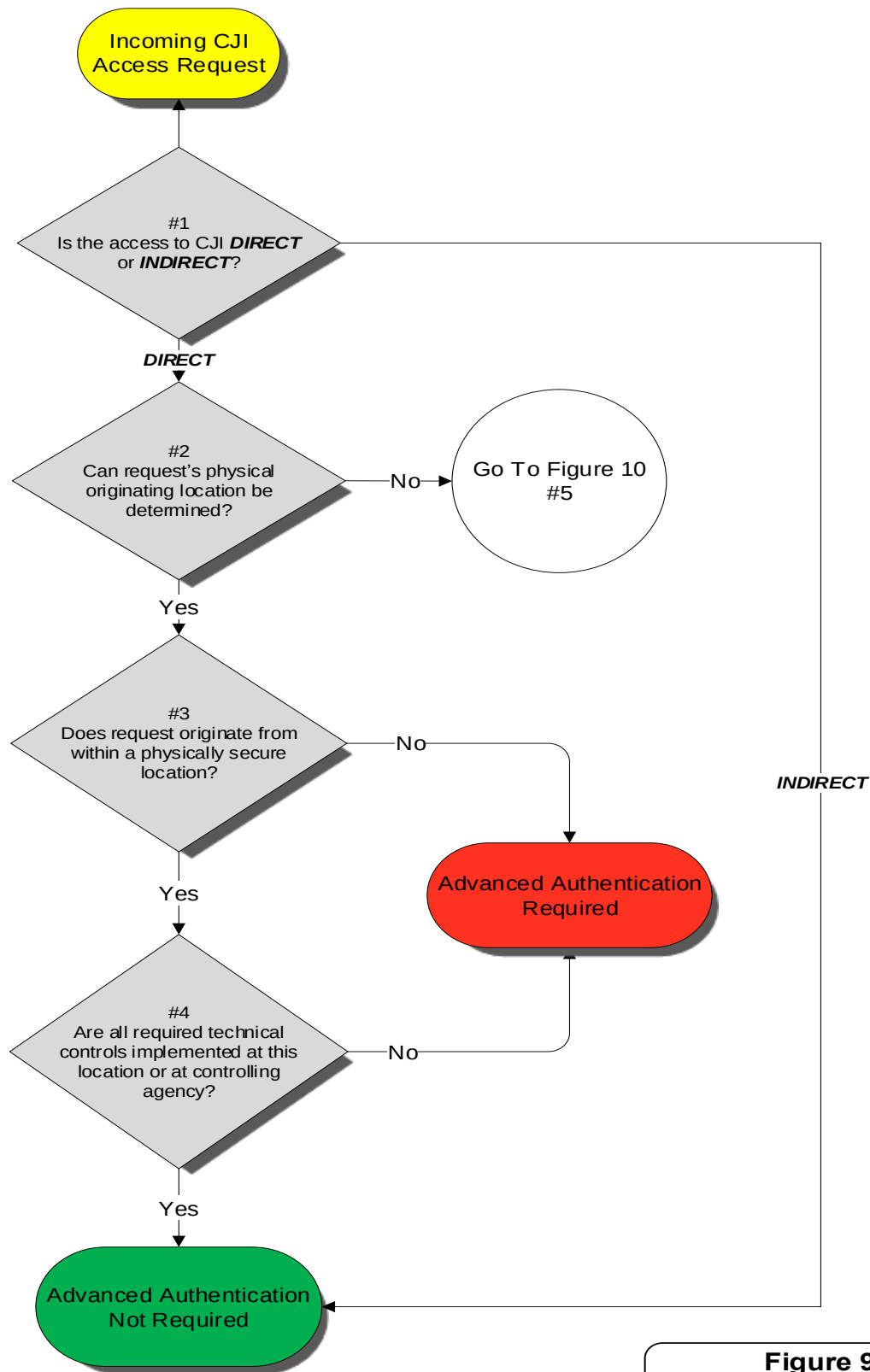


Figure 9		
	06/01/2020	

Figure 10 – Authentication Decision for Unknown Location

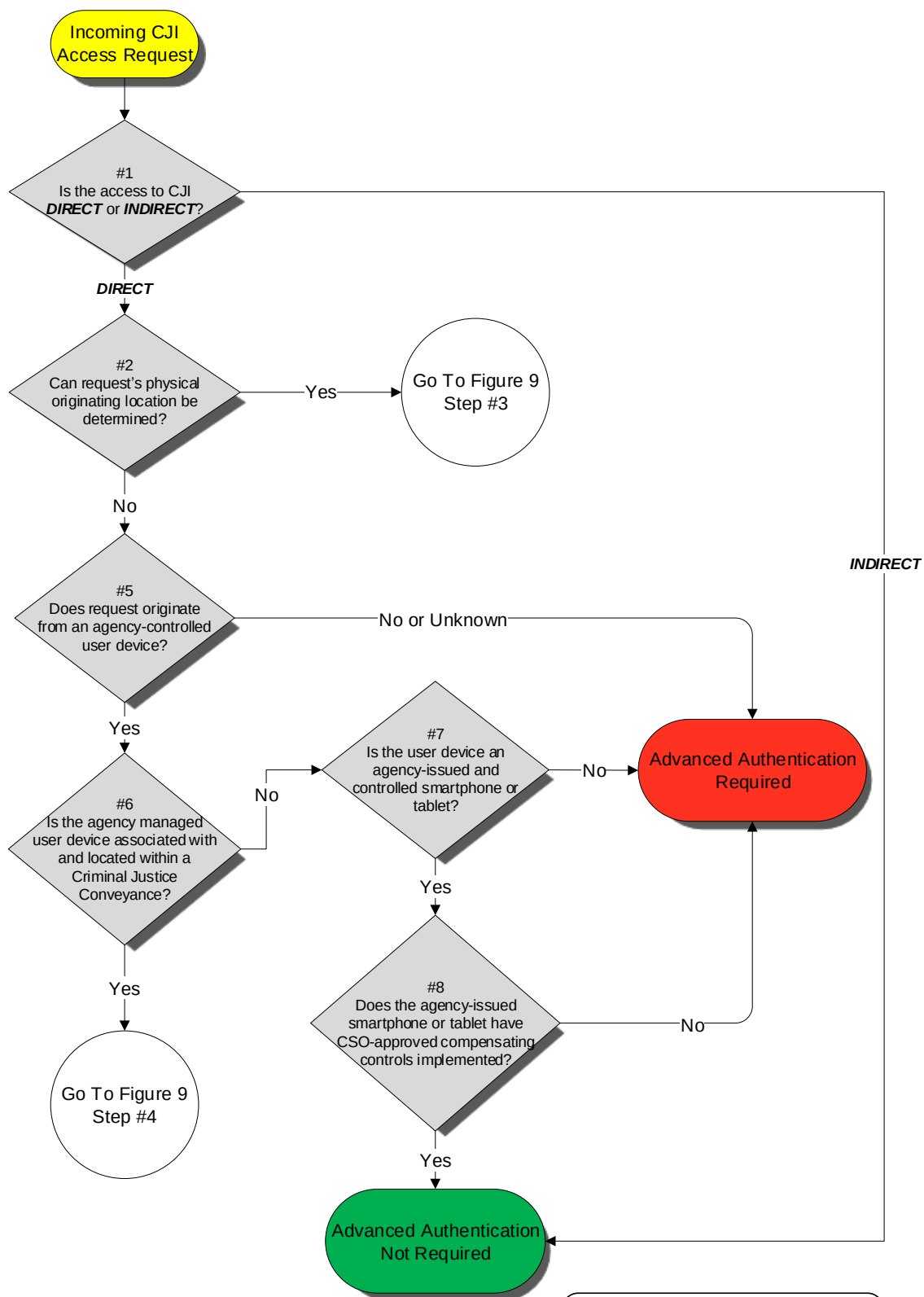


Figure 10		
	06/01/2020	

5.7 Policy Area 7: Configuration Management

5.7.1 Access Restrictions for Changes

Planned or unplanned changes to the hardware, software, and/or firmware components of the information system can have significant effects on the overall security of the system. The goal is to allow only qualified and authorized individuals access to information system components for purposes of initiating changes, including upgrades, and modifications. Section 5.5, Access Control, describes agency requirements for control of privileges and restrictions.

5.7.1.1 Least Functionality

The agency shall configure the application, service, or information system to provide only essential capabilities and shall specifically prohibit and/or restrict the use of specified functions, ports, protocols, and/or services.

5.7.1.2 Network Diagram

The agency shall ensure that a complete topological drawing depicting the interconnectivity of the agency network, to criminal justice information, systems and services is maintained in a current status. See Appendix C for sample network diagrams.

The network topological drawing shall include the following:

1. All communications paths, circuits, and other components used for the interconnection, beginning with the agency-owned system(s) and traversing through all interconnected systems to the agency end-point.
2. The logical location of all components (e.g., firewalls, routers, switches, hubs, servers, encryption devices, and computer workstations). Individual workstations (clients) do not have to be shown; the number of clients is sufficient.
3. “For Official Use Only” (FOUO) markings.
4. The agency name and date (day, month, and year) drawing was created or updated.

5.7.2 Security of Configuration Documentation

The system configuration documentation often contains sensitive details (e.g. descriptions of applications, processes, procedures, data structures, authorization processes, data flow, etc.) Agencies shall protect the system documentation from unauthorized access consistent with the provisions described in Section 5.5 Access Control.

Figure 11 – A Local Police Department’s Configuration Management Controls

A local police department decided to update their CAD system, and in doing so tracked all changes made to their infrastructure in a configuration management journal, updated their network topology documents to include all new components in their architecture, then marked all documentation as FOUO and stored them securely.

5.8 Policy Area 8: Media Protection

Media protection policy and procedures shall be documented and implemented to ensure that access to digital and physical media in all forms is restricted to authorized individuals. Procedures shall be defined for securely handling, transporting and storing media.

5.8.1 Media Storage and Access

The agency shall securely store digital and physical media within physically secure locations or controlled areas. The agency shall restrict access to digital and physical media to authorized individuals. If physical and personnel restrictions are not feasible then the data shall be encrypted per Section 5.10.1.2.

5.8.2 Media Transport

The agency shall protect and control digital and physical media during transport outside of controlled areas and restrict the activities associated with transport of such media to authorized personnel.

5.8.2.1 Digital Media during Transport

Controls shall be in place to protect digital media containing CJI while in transport (physically moved from one location to another) to help prevent compromise of the data. Encryption, as defined in Section 5.10.1.2 of this Policy, is the optimal control during transport; however, if encryption of the data isn't possible then each agency shall institute physical controls to ensure the security of the data.

5.8.2.2 Physical Media in Transit

The controls and security measures in this document also apply to CJI in physical (printed documents, printed imagery, etc.) form. Physical media shall be protected at the same level as the information would be protected in electronic form.

5.8.3 Digital Media Sanitization and Disposal

The agency shall sanitize, that is, overwrite at least three times or degauss digital media prior to disposal or release for reuse by unauthorized individuals. Inoperable digital media shall be destroyed (cut up, shredded, etc.). The agency shall maintain written documentation of the steps taken to sanitize or destroy electronic media. Agencies shall ensure the sanitization or destruction is witnessed or carried out by authorized personnel.

5.8.4 Disposal of Physical Media

Physical media shall be securely disposed of when no longer required, using formal procedures. Formal procedures for the secure disposal or destruction of physical media shall minimize the risk of sensitive information compromise by unauthorized individuals. Physical media shall be destroyed by shredding or incineration. Agencies shall ensure the disposal or destruction is witnessed or carried out by authorized personnel.

Figure 12 – A Local Police Department’s Media Management Policies

A local police department implemented a replacement CAD system that integrated to their state’s CSA and was authorized to process CJI. The police department contracted with an off-site media manager to store backups of their data in the contractor’s vaults, but the contractor was not authorized to process or store CJI. To ensure the confidentiality of the police department’s data while outside its perimeter, they encrypted all data going to the contractor with an encryption product that is FIPS 140-2 certified. The police department rotated and reused media through the contractor’s vaults periodically, and when it required destruction, the police department incinerated the media to irreversibly destroy any data on it.

5.9 Policy Area 9: Physical Protection

Physical protection policy and procedures shall be documented and implemented to ensure CJI and information system hardware, software, and media are physically protected through access control measures.

5.9.1 Physically Secure Location

A physically secure location is a facility, a criminal justice conveyance, or an area, a room, or a group of rooms within a facility with both the physical and personnel security controls sufficient to protect CJI and associated information systems. The physically secure location is subject to criminal justice agency management control; SIB control; FBI CJIS Security addendum; or a combination thereof.

Sections 5.9.1.1 – 5.9.1.8 describe the physical controls required in order to be considered a physically secure location, while Sections 5.2 and 5.12, respectively, describe the minimum security awareness training and personnel security controls required for unescorted access to a physically secure location. Sections 5.5, 5.6.2.2.1, and 5.10 describe the requirements for technical security controls required to access CJI from within the perimeter of a physically secure location without AA.

5.9.1.1 Security Perimeter

The perimeter of a physically secure location shall be prominently posted and separated from non-secure locations by physical controls. Security perimeters shall be defined, controlled and secured in a manner acceptable to the CSA or SIB.

5.9.1.2 Physical Access Authorizations

The agency shall develop and keep current a list of personnel with authorized access to the physically secure location (except for those areas within the permanent facility officially designated as publicly accessible) or shall issue credentials to authorized personnel.

5.9.1.3 Physical Access Control

The agency shall control all physical access points (except for those areas within the facility officially designated as publicly accessible) and shall verify individual access authorizations before granting access.

5.9.1.4 Access Control for Transmission Medium

The agency shall control physical access to information system distribution and transmission lines within the physically secure location.

5.9.1.5 Access Control for Display Medium

The agency shall control physical access to information system devices that display CJI and shall position information system devices in such a way as to prevent unauthorized individuals from accessing and viewing CJI.

5.9.1.6 Monitoring Physical Access

The agency shall monitor physical access to the information system to detect and respond to physical security incidents.

5.9.1.7 Visitor Control

The agency shall control physical access by authenticating visitors before authorizing escorted access to the physically secure location (except for those areas designated as publicly accessible). The agency shall escort visitors at all times and monitor visitor activity.

5.9.1.8 Delivery and Removal

The agency shall authorize and control information system-related items entering and exiting the physically secure location.

5.9.2 Controlled Area

If an agency cannot meet all of the controls required for establishing a physically secure location, but has an operational need to access or store CJI, the agency shall designate an area, a room, or a storage container, as a controlled area for the purpose of day-to-day CJI access or storage. The agency shall, at a minimum:

1. Limit access to the controlled area during CJI processing times to only those personnel authorized by the agency to access or view CJI.
2. Lock the area, room, or storage container when unattended.
3. Position information system devices and documents containing CJI in such a way as to prevent unauthorized individuals from access and view.
4. Follow the encryption requirements found in Section 5.10.1.2 for electronic storage (i.e. data “at rest”) of CJI.

Figure 13 – A Local Police Department's Physical Protection Measures

A local police department implemented a replacement CAD system that was authorized to process CJI over an encrypted VPN tunnel to the state's CSA. The police department established a physically separated wing within their precinct separated by locked doors, walls, and a monitored security system within which CJI was processed by criminal justice professionals. Only those persons with the appropriate authorizations were permitted within this wing unless accompanied by such a person. Within this secure wing the police department further segregated the back-office information systems' infrastructure within a separately controlled area restricted only to those authorized administrative personnel with a need to enter.

5.10 Policy Area 10: System and Communications Protection and Information Integrity

Examples of systems and communications safeguards range from boundary and transmission protection to securing an agency's virtualized environment. In addition, applications, services, or information systems must have the capability to ensure system integrity through the detection and protection against unauthorized changes to software and information. This section details the policy for protecting systems and communications infrastructures.

Refer to Section 5.13.4 for additional system integrity requirements related to mobile devices used to access CJI.

5.10.1 Information Flow Enforcement

The network infrastructure shall control the flow of information between interconnected systems. Information flow control regulates where information is allowed to travel within an information system and between information systems (as opposed to who is allowed to access the information) and without explicit regard to subsequent accesses to that information. In other words, controlling how data moves from one place to the next in a secure manner. Examples of controls that are better expressed as flow control than access control (see Section 5.5) are:

1. Prevent CJI from being transmitted unencrypted across the public network.
2. Block outside traffic that claims to be from within the agency.
3. Do not pass any web requests to the public network that are not from the internal web proxy.

Specific examples of flow control enforcement can be found in boundary protection devices (e.g. proxies, gateways, guards, encrypted tunnels, firewalls, and routers) that employ rule sets or establish configuration settings that restrict information system services or provide a packet filtering capability.

5.10.1.1 Boundary Protection

The agency shall:

1. Control access to networks processing CJI.
2. Monitor and control communications at the external boundary of the information system and at key internal boundaries within the system.
3. Ensure any connections to the Internet, other external networks, or information systems occur through controlled interfaces (e.g. proxies, gateways, routers, firewalls, encrypted tunnels). See Section 5.13.4.3 for guidance on personal firewalls.
4. Employ tools and techniques to monitor network events, detect attacks, and provide identification of unauthorized use.
5. Ensure the operational failure of the boundary protection mechanisms do not result in any unauthorized release of information outside of the information system boundary (i.e. the device "fails closed" vs. "fails open").

6. Allocate publicly accessible information system components (e.g. public Web servers) to separate sub networks with separate, network interfaces. Publicly accessible information systems residing on a virtual host shall follow the guidance in Section 5.10.3.2 to achieve separation.

5.10.1.2 Encryption

Encryption is a form of cryptology that applies a cryptographic operation to provide confidentiality of (sensitive) information. Decryption is the reversing of the cryptographic operation to convert the information back into a plaintext (readable) format. There are two main types of encryption: symmetric encryption and asymmetric encryption (also known as public key encryption). Hybrid encryption solutions do exist and use both asymmetric encryption for client/server certificate exchange – session integrity and symmetric encryption for bulk data encryption – data confidentiality.

5.10.1.2.1 Encryption for CJI in Transit

When CJI is transmitted outside the boundary of the physically secure location, the data shall be immediately protected via encryption. When encryption is employed, the cryptographic module used shall be FIPS 140-2 certified and use a symmetric cipher key strength of at least 128 bit strength to protect CJI.

NOTE: Subsequent versions of approved cryptographic modules that are under current review for FIPS 140-2 compliancy can be used in the interim until certification is complete.

EXCEPTIONS:

1. See Sections 5.13.1.2.2 and 5.10.2.
2. Encryption shall not be required if the transmission medium meets all of the following requirements:
 - a. The agency owns, operates, manages, or protects the medium.
 - b. Medium terminates within physically secure locations at both ends with no interconnections between.
 - c. Physical access to the medium is controlled by the agency using the requirements in Sections 5.9.1 and 5.12.
 - d. Protection includes safeguards (e.g., acoustic, electric, electromagnetic, and physical) and if feasible countermeasures (e.g., alarms, notifications) to permit its use for the transmission of unencrypted information through an area of lesser classification or control.
 - e. With prior approval of the CSO.

Examples:

- A campus is completely owned and controlled by a criminal justice agency (CJA)
 - If line-of-sight between buildings exists where a cable is buried, encryption is not required.

- A multi-story building is completely owned and controlled by a CJA – If floors are physically secure or cable runs through non-secure areas are protected, encryption is not required.
- A multi-story building is occupied by a mix of CJAs and non-CJAs – If floors are physically secure or cable runs through the non-secure areas are protected, encryption is not required.

5.10.1.2.2 Encryption for CJI at Rest

When CJI is at rest (i.e. stored digitally) outside the boundary of the physically secure location, the data shall be protected via encryption. When encryption is employed, agencies shall either encrypt CJI in accordance with the standard in Section 5.10.1.2.1 above, or use a symmetric cipher that is FIPS 197 certified (AES) and at least 256 bit strength.

1. When agencies implement encryption on CJI at rest, the passphrase used to unlock the cipher shall meet the following requirements:
 - a. Be at least 10 characters
 - b. Not be a dictionary word.
 - c. Include at least one (1) upper case letter, one (1) lower case letter, one (1) number, and one (1) special character.
 - d. Be changed when previously authorized personnel no longer require access.
2. Multiple files maintained in the same unencrypted folder shall have separate and distinct passphrases. A single passphrase may be used to encrypt an entire folder or disk containing multiple files. All audit requirements found in Section 5.4.1 Auditable Events and Content (Information Systems) shall be applied.

NOTE: Commonly available encryption tools often use a key to unlock the cipher to allow data access; this key is called a passphrase. While similar to a password, a passphrase is not used for user authentication. Additionally, the passphrase contains stringent character requirements making it more secure and thus providing a higher level of confidence that the passphrase will not be compromised.

5.10.1.2.3 Public Key Infrastructure (PKI) Technology

For agencies using public key infrastructure (PKI) technology, the agency shall develop and implement a certificate policy and certification practice statement for the issuance of public key certificates used in the information system. Registration to receive a public key certificate shall:

1. Include authorization by a supervisor or a responsible official.
2. Be accomplished by a secure process that verifies the identity of the certificate holder.
3. Ensure the certificate is issued to the intended party.

5.10.1.3 Intrusion Detection Tools and Techniques

Intrusion detection systems are deployed inside a network to monitor events against a known set of parameters (i.e. malicious activity or policy violations) and make notification to the system of any event which violates any of those parameters. They are passive in nature, listening and

monitoring network traffic. There are mainly two types of IDS; network-based IDS (NIDS) and host-based IDS (HIDS).

Intrusion prevention systems are an IDS with the capability to respond to detected intrusions. They are normally deployed at the perimeter of a network, scanning traffic. Like detection systems, protection systems compare scanned traffic to defined normal parameters but unlike detection systems are able to take some type of immediate action to mitigate, or prevent, an event.

Agencies shall:

1. Implement network-based and/or host-based intrusion detection or prevention tools.
2. Maintain current intrusion detection or prevention signatures.
3. Monitor inbound and outbound communications for unusual or unauthorized activities.
4. Send individual intrusion detection logs to a central logging facility where correlation and analysis will be accomplished as a system wide intrusion detection effort.
5. Review intrusion detection or prevention logs weekly or implement automated event notification.
6. Employ automated tools to support near-real-time analysis of events in support of detecting system-level attacks.

5.10.1.4 Voice over Internet Protocol

Voice over Internet Protocol (VoIP) has been embraced by organizations globally as an addition to, or replacement for, public switched telephone network (PSTN) and private branch exchange (PBX) telephone systems. The immediate benefits are lower costs than traditional telephone services and VoIP can be installed in-line with an organization's existing Internet Protocol (IP) services. Among VoIP's risks that have to be considered carefully are: myriad security concerns, cost issues associated with new networking hardware requirements, and overarching quality of service (QoS) factors.

In addition to the security controls described in this document, the following additional controls shall be implemented when an agency deploys VoIP within a network that contains unencrypted CJI:

1. Establish usage restrictions and implementation guidance for VoIP technologies.
2. Change the default administrative password on the IP phones and VoIP switches.
3. Utilize Virtual Local Area Network (VLAN) technology to segment VoIP traffic from data traffic.

Appendix G.2 outlines threats, vulnerabilities, mitigations, and NIST best practices for VoIP.

5.10.1.5 Cloud Computing

Organizations transitioning to a cloud environment are presented unique opportunities and challenges (e.g., purported cost savings and increased efficiencies versus a loss of control over the data). Reviewing the cloud computing white paper (Appendix G.3), the cloud assessment located within the security policy resource center on FBI.gov, NIST Special Publications (800-144, 800-

145, and 800-146), as well as the cloud provider's policies and capabilities will enable organizations to make informed decisions on whether or not the cloud provider can offer service that maintains compliance with the requirements of the CJIS Security Policy.

The storage of CJI, regardless of encryption status, shall only be permitted in cloud environments (e.g. government or third-party/commercial datacenters, etc.) which reside within the physical boundaries of APB-member country (i.e. U.S., U.S. territories, Indian Tribes, and Canada) and legal authority of an APB-member agency (i.e. U.S. – federal/state/territory, Indian Tribe, or the Royal Canadian Mounted Police (RCMP)).

Note: This restriction does not apply to exchanges of CJI with foreign government agencies under international exchange agreements (i.e. the Preventing and Combating Serious Crime (PCSC) agreements, fugitive extracts, and exchanges made for humanitarian and criminal investigatory purposes in particular circumstances).

Metadata derived from unencrypted CJI shall be protected in the same manner as CJI and shall not be used for any advertising or other commercial purposes by any cloud service provider or other associated entity.

The agency may permit limited use of metadata derived from unencrypted CJI when specifically approved by the agency and its “intended use” is detailed within the service agreement. Such authorized uses of metadata may include, but are not limited to the following: spam and spyware filtering, data loss prevention, spillage reporting, transaction logs (events and content – similar to Section 5.4), data usage/indexing metrics, and diagnostic/syslog data.

5.10.2 Facsimile Transmission of CJI

CJI transmitted via a single or multi-function device over a standard telephone line is exempt from encryption requirements. CJI transmitted external to a physically secure location using a facsimile server, application or service which implements email-like technology, shall meet the encryption requirements for CJI in transit as defined in Section 5.10.

5.10.3 Partitioning and Virtualization

As resources grow scarce, agencies are increasing the centralization of applications, services, and system administration. Advanced software now provides the ability to create virtual machines that allows agencies to reduce the amount of hardware needed. Although the concepts of partitioning and virtualization have existed for a while, the need for securing the partitions and virtualized machines has evolved due to the increasing amount of distributed processing and federated information sources now available across the Internet.

5.10.3.1 Partitioning

The application, service, or information system shall separate user functionality (including user interface services) from information system management functionality.

The application, service, or information system shall physically or logically separate user interface services (e.g. public web pages) from information storage and management services (e.g. database management). Separation may be accomplished through the use of one or more of the following:

1. Different computers.

2. Different central processing units.
3. Different instances of the operating system.
4. Different network addresses.
5. Other methods approved by the FBI CJIS ISO.

5.10.3.2 Virtualization

Virtualization refers to a methodology of dividing the resources of a computer (hardware and software) into multiple execution environments. Virtualized environments are authorized for criminal justice and noncriminal justice activities. In addition to the security controls described in this Policy, the following additional controls shall be implemented in a virtual environment:

1. Isolate the host from the virtual machine. In other words, virtual machine users cannot access host files, firmware, etc.
2. Maintain audit logs for all virtual machines and hosts and store the logs outside the hosts' virtual environment.
3. Virtual Machines that are Internet facing (web servers, portal servers, etc.) shall be physically separate from Virtual Machines (VMs) that process CJI internally or be separated by a virtual firewall.
4. Drivers that serve critical functions shall be stored within the specific VM they service. In other words, do not store these drivers within the hypervisor, or host operating system, for sharing. Each VM is to be treated as an independent system – secured as independently as possible.

The following additional technical security controls shall be applied in virtual environments where CJI is comingled with non-CJI:

1. Encrypt CJI when stored in a virtualized environment where CJI is comingled with non-CJI or segregate and store unencrypted CJI within its own secure VM.
2. Encrypt network traffic within the virtual environment.

The following are additional technical security control best practices and should be implemented wherever feasible:

1. Implement IDS and/or IPS monitoring within the virtual environment.
2. Virtually or physically firewall each VM within the virtual environment to ensure that only allowed protocols will transact.
3. Segregate the administrative duties for the host.

Appendix G-1 provides some reference and additional background information on virtualization.

5.10.4 System and Information Integrity Policy and Procedures

5.10.4.1 Patch Management

The agency shall identify applications, services, and information systems containing software or components affected by recently announced software flaws and potential vulnerabilities resulting from those flaws.

The agency (or the software developer/vendor in the case of software developed and maintained by a vendor/contractor) shall develop and implement a local policy that ensures prompt installation of newly released security relevant patches, service packs and hot fixes. Local policies should include such items as:

1. Testing of appropriate patches before installation.
2. Rollback capabilities when installing patches, updates, etc.
3. Automatic updates without individual user intervention.
4. Centralized patch management.

Patch requirements discovered during security assessments, continuous monitoring or incident response activities shall also be addressed expeditiously.

5.10.4.2 Malicious Code Protection

The agency shall implement malicious code protection that includes automatic updates for all systems with Internet access. Agencies with systems not connected to the Internet shall implement local procedures to ensure malicious code protection is kept current (i.e. most recent update available).

The agency shall employ virus protection mechanisms to detect and eradicate malicious code (e.g., viruses, worms, Trojan horses) at critical points throughout the network and on all workstations, servers and mobile computing devices on the network. The agency shall ensure malicious code protection is enabled on all of the aforementioned critical points and information systems and resident scanning is employed.

5.10.4.3 Spam and Spyware Protection

The agency shall implement spam and spyware protection.

The agency shall:

1. Employ spam protection mechanisms at critical information system entry points (e.g. firewalls, electronic mail servers, remote-access servers).
2. Employ spyware protection at workstations, servers and mobile computing devices on the network.
3. Use the spam and spyware protection mechanisms to detect and take appropriate action on unsolicited messages and spyware/adware, respectively, transported by electronic mail, electronic mail attachments, Internet accesses, removable media (e.g. diskettes or compact disks) or other removable media as defined in this Policy.

5.10.4.4 Security Alerts and Advisories

The agency shall:

1. Receive information system security alerts/advisories on a regular basis.
2. Issue alerts/advisories to appropriate personnel.
3. Document the types of actions to be taken in response to security alerts/advisories.
4. Take appropriate actions in response.

5. Employ automated mechanisms to make security alert and advisory information available throughout the agency as appropriate.

5.10.4.5 Information Input Restrictions

The agency shall restrict the information input to any connection to FBI CJIS services to authorized personnel only.

Restrictions on personnel authorized to input information to the information system may extend beyond the typical access controls employed by the system and include limitations based on specific operational/project responsibilities.

Figure 14 – System and Communications Protection and Information Integrity Use Cases

Use Case 1 – A Local Police Department’s Information Systems & Communications Protections

A local police department implemented a replacement CAD system within a physically secure location that was authorized to process CJI using a FIPS 140-2 encrypted VPN tunnel over the Internet to the state’s CSA. In addition to the policies, physical and personnel controls already in place, the police department employed firewalls both at their border and at key points within their network, intrusion detection systems, a patch-management strategy that included automatic patch updates where possible, virus scanners, spam and spyware detection mechanisms that update signatures automatically, and subscribed to various security alert mailing lists and addressed vulnerabilities raised through the alerts as needed.

Use Case 2 – Faxing from a Single/Multi-function Device over a Traditional Telephone Line

A dispatcher from county A runs a NCIC query on an individual. The results are printed and then sent to an adjoining county using a single/multi-function device with facsimile capability. For faxing, the device is only connected to a traditional telephone line as is the device at the receiving county. Encryption of a document containing CJI is not required because the document travels over a traditional telephone line.

Use Case 3 – Faxing from a Multi-function Device over a Network

A dispatcher from city A runs a NCIC query on an individual. The results are printed and the dispatcher uses a multi-function copier to fax the file to a city in another state. The dispatcher enters the fax number of the receiver and sends the document. The document containing CJI is automatically converted to a digital file and routed to the receiver over the agency network and the Internet. Because the device uses a network and the Internet for transmitting documents containing CJI, encryption in transit using FIPS 140-2 certified 128 bit symmetric encryption is required.

5.11 Policy Area 11: Formal Audits

Formal audits are conducted to ensure compliance with applicable statutes, regulations and policies.

5.11.1 Audits by the FBI CJIS Division

5.11.1.1 Triennial Compliance Audits by the FBI CJIS Division

The FBI CJIS Division is authorized to conduct audits, once every three (3) years as a minimum, to assess agency compliance with applicable statutes, regulations and policies. The CJIS Audit Unit (CAU) shall conduct a triennial audit of each CSA in order to verify compliance with applicable statutes, regulations and policies. This audit shall include a sample of CJAs and, in coordination with the SIB, the NCJAs. Audits may be conducted on a more frequent basis if the audit reveals that an agency has not complied with applicable statutes, regulations and policies. The FBI CJIS Division shall also have the authority to conduct unannounced security inspections and scheduled audits of Contractor facilities.

5.11.1.2 Triennial Security Audits by the FBI CJIS Division

The FBI CJIS Division is authorized to conduct security audits of the CSA and SIB networks and systems, once every three (3) years as a minimum, to assess agency compliance with the CJIS Security Policy. This audit shall include a sample of CJAs and NCJAs. Audits may be conducted on a more frequent basis if the audit reveals that an agency has not complied with the CJIS Security Policy.

5.11.2 Audits by the CSA

Each CSA shall:

1. At a minimum, triennially audit all CJAs and NCJAs which have direct access to the state system in order to ensure compliance with applicable statutes, regulations and policies.
2. In coordination with the SIB, establish a process to periodically audit all NCJAs, with access to CJI, in order to ensure compliance with applicable statutes, regulations and policies.
3. Have the authority to conduct unannounced security inspections and scheduled audits of Contractor facilities.
4. Have the authority, on behalf of another CSA, to conduct a CSP compliance audit of contractor facilities and provide the results to the requesting CSA. If a subsequent CSA requests an audit of the same contractor facility, the CSA may provide the results of the previous audit unless otherwise notified by the requesting CSA that a new audit be performed.

Note: This authority does not apply to the audit requirement outlined in the Security and Management Control Outsourcing Standard for Non-Channeler and Channelers related to outsourcing noncriminal justice administrative functions.

5.11.3 Special Security Inquiries and Audits

All agencies having access to CJI shall permit an inspection team to conduct an appropriate inquiry and audit of any alleged security violations. The inspection team shall be appointed by the APB and shall include at least one representative of the CJIS Division. All results of the inquiry and audit shall be reported to the APB with appropriate recommendations.

5.11.4 Compliance Subcommittees

The Criminal Justice Information Services (CJIS) Advisory Policy Board (APB) established the Compliance Evaluation Subcommittee (CES) to evaluate the results of audits conducted by the CJIS Audit Unit (CAU). The CES makes specific recommendations to the APB concerning compliance with applicable policies and regulations. The most current information regarding the CAU audits that are within the purview of the CES and detailed CES sanctions process procedures are available at CJIS.gov (Law Enforcement Enterprise Portal) CJIS Special Interest Groups CES Section and CJIS Section of FBI.gov.

The National Crime Prevention and Privacy Compact (Compact) Council at Article VI established the Compact Council (Council). The Compact Council Sanctions Committee is responsible for ensuring the use of the Interstate Identification Index System for noncriminal justice purposes complies with the Compact and with rules, standards, and procedures established by the Compact Council. As such, the Sanctions Committee reviews the results of audits conducted by the Federal Bureau of Investigation (FBI) of participants in the FBI's Criminal Justice Services (CJIS) Division programs. The Sanctions Committee reviews the audit results and the participant's response to determine a course of action necessary to bring the participant into compliance and make recommendations to the Compact Council or the FBI. Additional information on the Compact Council Sanctions process is available on the Compact Council's web-site.

Figure 15 – The Audit of a Local Police Department

A local police department implemented a replacement CAD system that integrated to their state's CSA and was authorized to process CJI. Shortly after the implementation, their state's CSA conducted an audit of their policies, procedures, and systems that process CJI. The police department supplied all architectural and policy documentation, including detailed network diagrams, to the auditors in order to assist them in the evaluation. The auditors discovered a deficiency in the police department's systems and marked them "out" in this aspect of the FBI CJIS Security Policy. The police department quickly addressed the deficiency and took corrective action, notifying the auditors of their actions.

5.12 Policy Area 12: Personnel Security

Having proper security measures against the insider threat is a critical component for the CJIS Security Policy. This section's security terms and requirements apply to all personnel who have unescorted access to unencrypted CJI including those individuals with only physical or logical access to devices that store, process or transmit unencrypted CJI.

5.12.1 Personnel Screening Requirements for Individuals Requiring Unescorted Access to Unencrypted CJI

1. To verify identification, state of residency and national fingerprint-based record checks shall be conducted prior to granting access to CJI for all personnel who have unescorted access to unencrypted CJI or unescorted access to physically secure locations or controlled areas (during times of CJI processing). However, if the person resides in a different state than that of the assigned agency, the agency shall conduct state (of the agency) and national fingerprint-based record checks and execute a NLETS CHRI IQ/FQ/AQ query using purpose code C, E, or J depending on the circumstances. When appropriate, the screening shall be consistent with:
 - a. 5 CFR 731.106; and/or
 - b. Office of Personnel Management policy, regulations, and guidance; and/or
 - c. agency policy, regulations, and guidance.

Federal entities bypassing state repositories in compliance with federal law may not be required to conduct a state fingerprint-based record check.

See Appendix J for applicable guidance regarding noncriminal justice agencies performing adjudication of civil fingerprint submissions.

2. All requests for access shall be made as specified by the CSO. The CSO, or their designee, is authorized to approve access to CJI. All CSO designees shall be from an authorized criminal justice agency.
3. If a record of any kind exists, access to CJI shall not be granted until the CSO or his/her designee reviews the matter to determine if access is appropriate.
 - a. If a felony conviction of any kind exists, the Interface Agency shall deny access to CJI. However, the Interface Agency may ask for a review by the CSO in extenuating circumstances where the severity of the offense and the time that has passed would support a possible variance.
 - b. Applicants with a record of misdemeanor offense(s) may be granted access if the CSO, or his or her designee, determines the nature or severity of the misdemeanor offense(s) do not warrant disqualification. The Interface Agency may request the CSO review a denial of access determination. This same procedure applies if the person is found to be a fugitive or has an arrest history without conviction.
 - c. If a record of any kind is found on a contractor, the CGA shall be formally notified and system access shall be delayed pending review of the criminal history record information. The CGA shall in turn notify the contractor's security officer.

4. If the person appears to be a fugitive or has an arrest history without conviction, the CSO or his/her designee shall review the matter to determine if access to CJI is appropriate.
5. If the person already has access to CJI and is subsequently arrested and or convicted, continued access to CJI shall be determined by the CSO. This does not implicitly grant hiring/firing authority with the CSA, only the authority to grant access to CJI. For offenses other than felonies, the CSO has the latitude to delegate continued access determinations to his or her designee.
6. If the CSO or his/her designee determines that access to CJI by the person would not be in the public interest, access shall be denied and the person's appointing authority shall be notified in writing of the access denial.
7. The granting agency shall maintain a list of personnel who have been authorized unescorted access to unencrypted CJI and shall, upon request, provide a current copy of the access list to the CSO.

It is recommended individual background re-investigations be conducted every five years unless Rap Back is implemented.

5.12.2 Personnel Termination

Upon termination of personnel by an interface agency, the agency shall immediately terminate access to local agency systems with access to CJI. Furthermore, the interface agency shall provide notification or other action to ensure access to state and other agency systems is terminated. If the employee is an employee of a NCJA or a Contractor, the employer shall notify all Interface Agencies that may be affected by the personnel change.

5.12.3 Personnel Transfer

The agency shall review CJI access authorizations when personnel are reassigned or transferred to other positions within the agency and initiate appropriate actions such as closing and establishing accounts and changing system access authorizations.

5.12.4 Personnel Sanctions

The agency shall employ a formal sanctions process for personnel failing to comply with established information security policies and procedures.

Figure 16 – A Local Police Department's Personnel Security Controls

A local police department implemented a replacement CAD system that integrated to their state's CSA and was authorized to process CJI. In addition to the physical and technical controls already in place, the police department implemented a variety of personnel security controls to reduce the insider threat. The police department used background screening consistent with the FBI CJIS Security Policy to vet those with unescorted access to areas in which CJI is processed, including the IT administrators employed by a contractor and all janitorial staff. The police department established sanctions against any vetted person found to be in violation of stated

policies. The police department re-evaluated each person's suitability for access to CJI every five years.

5.13 Policy Area 13: Mobile Devices

This policy area describes considerations and requirements for mobile devices including smartphones and tablets. Mobile devices are not limited to a single form factor or communications medium. The requirements in this section augment those in other areas of the Policy to address the gaps introduced by using mobile devices.

The agency shall: (i) establish usage restrictions and implementation guidance for mobile devices; and (ii) authorize, monitor, control wireless access to the information system. Wireless technologies, in the simplest sense, enable one or more devices to communicate without physical connections—without requiring network or peripheral cabling.

Appendix G provides reference material and additional information on mobile devices.

5.13.1 Wireless Communications Technologies

Examples of wireless communication technologies include, but are not limited to: 802.11, cellular, Bluetooth, satellite, microwave, and land mobile radio (LMR). Wireless technologies require at least the minimum security applied to wired technology and, based upon the specific technology or implementation, wireless technologies may require additional security controls as described below.

5.13.1.1 802.11 Wireless Protocols

Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA) cryptographic algorithms, used by all pre-802.11i protocols, do not meet the requirements for FIPS 140-2 and shall not be used.

Agencies shall implement the following controls for all agency-managed wireless access points with access to an agency's network that processes unencrypted CJI:

1. Perform validation testing to ensure rogue APs (Access Points) do not exist in the 802.11 Wireless Local Area Network (WLAN) and to fully understand the wireless network security posture.
2. Maintain a complete inventory of all Access Points (APs) and 802.11 wireless devices.
3. Place APs in secured areas to prevent unauthorized physical access and user manipulation.
4. Test AP range boundaries to determine the precise extent of the wireless coverage and design the AP wireless coverage to limit the coverage area to only what is needed for operational purposes.
5. Enable user authentication and encryption mechanisms for the management interface of the AP.
6. Ensure that all APs have strong administrative passwords and ensure that all passwords are changed in accordance with Section 5.6.2.1.
7. Ensure the reset function on APs is used only when needed and is only invoked by authorized personnel. Restore the APs to the latest security settings, when the reset functions are used, to ensure the factory default settings are not utilized.

8. Change the default service set identifier (SSID) in the APs. Disable the broadcast SSID feature so that the client SSID must match that of the AP. Validate that the SSID character string does not contain any agency identifiable information (division, department, street, etc.) or services.
9. Enable all security features of the wireless product, including the cryptographic authentication, firewall, and other available privacy features.
10. Ensure that encryption key sizes are at least 128-bits and the default shared keys are replaced by unique keys.
11. Ensure that the ad hoc mode has been disabled.
12. Disable all nonessential management protocols on the APs.
13. Ensure all management access and authentication occurs via FIPS compliant secure protocols (e.g. SFTP, HTTPS, SNMP over TLS, etc.). Disable non-FIPS compliant secure access to the management interface.
14. Enable logging (if supported) and review the logs on a recurring basis per local policy. At a minimum logs shall be reviewed monthly.
15. Insulate, virtually (e.g. virtual local area network (VLAN) and ACLs) or physically (e.g. firewalls), the wireless network from the operational wired infrastructure. Limit access between wireless networks and the wired network to only operational needs.
16. When disposing of access points that will no longer be used by the agency, clear access point configuration to prevent disclosure of network configuration, keys, passwords, etc.

5.13.1.2 Cellular Devices

Cellular telephones, smartphones (i.e. Blackberry, iPhones, etc.), tablets, personal digital assistants (PDA), and “aircards” are examples of cellular handheld devices or devices that are capable of employing cellular technology. Additionally, cellular handheld devices typically include Bluetooth, infrared, and other wireless protocols capable of joining infrastructure networks or creating dynamic ad hoc networks.

Threats to cellular handheld devices stem mainly from their size, portability, and available wireless interfaces and associated services. Examples of threats to cellular handheld devices include:

1. Loss, theft, or disposal.
2. Unauthorized access.
3. Malware.
4. Spam.
5. Electronic eavesdropping.
6. Electronic tracking (threat to security of data and safety of the criminal justice professional).
7. Cloning (not as prevalent with later generation cellular technologies).
8. Server-resident data.

5.13.1.2.1 Cellular Service Abroad

Certain internal functions on cellular devices may be modified or compromised by the cellular carrier during international use as the devices are intended to have certain parameters configured by the cellular provider which is considered a “trusted” entity by the device.

When devices are authorized to access CJI outside the U.S., agencies shall perform an inspection to ensure that all controls are in place and functioning properly in accordance with the agency’s policies prior to and after deployment outside of the U.S.

5.13.1.2.2 Voice Transmissions Over Cellular Devices

Any cellular device used to transmit CJI via voice is exempt from the encryption and authentication requirements.

5.13.1.3 Bluetooth

Bluetooth is an open standard for short-range radio frequency (RF) communication. Bluetooth is used primarily to establish wireless personal area networks (WPAN). Bluetooth technology has been integrated into many types of business and consumer devices, including cell phones, laptops, automobiles, medical devices, printers, keyboards, mice, headsets, and biometric capture devices.

Bluetooth technology and associated devices are susceptible to general wireless networking threats (e.g. denial of service [DoS] attacks, eavesdropping, man-in-the-middle [MITM] attacks, message modification, and resource misappropriation) as well as specific Bluetooth-related attacks that target known vulnerabilities in Bluetooth implementations and specifications. Organizational security policy shall be used to dictate the use of Bluetooth and its associated devices based on the agency’s operational and business processes.

5.13.1.4 Mobile Hotspots

Many mobile devices include the capability to function as a WiFi hotspot that allows other devices to connect through the device to the internet over the devices cellular network.

When an agency allows mobile devices that are approved to access or store CJI to function as a Wi-Fi hotspot connecting to the Internet, they shall be configured:

1. Enable encryption on the hotspot
2. Change the hotspot’s default SSID
 - a. Ensure the hotspot SSID does not identify the device make/model or agency ownership
3. Create a wireless network password (Pre-shared key)
4. Enable the hotspot’s port filtering/blocking features if present
5. Only allow connections from agency controlled devices

Note: Refer to the requirements in Section 5.10.1.2 encryption for item #1. Refer to the requirements in Section 5.6.2.2.1 Password for item #3. Only password attributes #1, #2 and #3 are required.

OR

1. Have a MDM solution to provide the same security as identified in items 1 – 5 above.

5.13.2 Mobile Device Management (MDM)

Mobile Device Management (MDM) facilitates the implementation of sound security controls for mobile devices and allows for centralized oversight of configuration control, application usage, and device protection and recovery, if so desired by the agency.

Due to the potential for inconsistent network access or monitoring capability on mobile devices, methods used to monitor and manage the configuration of full-featured operating systems may not function properly on devices with limited-feature operating systems. MDM systems and applications coupled with device specific technical policy can provide a robust method for device configuration management if properly implemented.

Devices that have had any unauthorized changes made to them (including but not limited to being rooted or jailbroken) shall not be used to process, store, or transmit CJI data at any time. User agencies shall implement the following controls when directly accessing CJI from devices running a limited-feature operating system:

1. Ensure that CJI is only transferred between CJI authorized applications and storage areas of the device.
2. MDM with centralized administration configured and implemented to perform at least the following controls:
 - a. Remote locking of device
 - b. Remote wiping of device
 - c. Setting and locking device configuration
 - d. Detection of “rooted” and “jailbroken” devices
 - e. Enforcement of folder or disk level encryption
 - f. Application of mandatory policy settings on the device
 - g. Detection of unauthorized configurations
 - h. Detection of unauthorized software or applications
 - i. Ability to determine the location of agency controlled devices
 - j. Prevention of unpatched devices from accessing CJI or CJI systems
 - k. Automatic device wiping after a specified number of failed access attempts

EXCEPTION: An MDM is not required when receiving CJI from an indirect access information system (i.e. the system provides no capability to conduct transactional activities on state and national repositories, applications or services). However, it is incumbent upon the authorized agency to ensure CJI is delivered to the appropriate requesting agency or individual. The CSO will make the final determination of whether access is considered indirect.

5.13.3 Wireless Device Risk Mitigations

Organizations shall, at a minimum, ensure that wireless devices:

1. Apply available critical patches and upgrades to the operating system as soon as they become available for the device and after necessary testing as described in Section 5.10.4.1.

2. Are configured for local device authentication (see Section 5.13.7.1).
3. Use advanced authentication or CSO approved compensating controls as per Section 5.13.7.2.1.
4. Encrypt all CJI resident on the device.
5. Erase cached information, to include authenticators (see Section 5.6.2.1) in applications, when session is terminated.
6. Employ personal firewalls on full-featured operating system devices or run a Mobile Device Management (MDM) system that facilitates the ability to provide firewall services from the agency level.
7. Employ malicious code protection on full-featured operating system devices or run a MDM system that facilitates the ability to provide anti-malware services from the agency level.

5.13.4 System Integrity

Managing system integrity on limited function mobile operating systems may require methods and technologies significantly different from traditional full-featured operating systems. In many cases, the requirements of Section 5.10 of the CJIS Security Policy cannot be met with a mobile device without the installation of a third party MDM, application, or supporting service infrastructure.

5.13.4.1 Patching/Updates

Based on the varying connection methods for mobile devices, an always on connection cannot be guaranteed for patching and updating. Devices without always-on cellular connections may not be reachable for extended periods of time by the MDM or solution either to report status or initiate patching.

Agencies shall monitor mobile devices to ensure their patch and update state is current.

5.13.4.2 Malicious Code Protection

Appropriately configured MDM software is capable of checking the installed applications on the device and reporting the software inventory to a central management console in a manner analogous to traditional virus scan detection of unauthorized software and can provide a high degree of confidence that only known software or applications are installed on the device.

Agencies that allow smartphones and tablets to access CJI shall have a process to approve the use of specific software or applications on the devices. Any device natively capable of performing these functions without a MDM solution is acceptable under this section.

5.13.4.3 Personal Firewall

For the purpose of this policy, a personal firewall is an application that controls network traffic to and from a user device, permitting or denying communications based on policy. A personal firewall shall be employed on all mobile devices that have a full-feature operating system (i.e. laptops or tablets with Windows or Linux/Unix operating systems). At a minimum, the personal firewall shall perform the following activities:

1. Manage program access to the Internet.

2. Block unsolicited requests to connect to the user device.
3. Filter incoming traffic by IP address or protocol.
4. Filter incoming traffic by destination ports.
5. Maintain an IP traffic log.

Mobile devices with limited-feature operating systems (i.e. tablets, smartphones) may not support a personal firewall. However, these operating systems have a limited number of system services installed, carefully controlled network access, and to a certain extent, perform functions similar to a personal firewall on a device with a full-feature operating system. Appropriately configured MDM software is capable of controlling which applications are allowed on the device.

5.13.5 Incident Response

In addition to the requirements in Section 5.3 Incident Response, agencies shall develop additional or enhanced incident reporting and handling procedures to address mobile device operating scenarios. Rapid response to mobile device related incidents can significantly mitigate the risks associated with illicit data access either on the device itself or within online data resources associated with the device through an application or specialized interface.

Special reporting procedures for mobile devices shall apply in any of the following situations:

1. Loss of device control. For example:
 - a. Device known to be locked, minimal duration of loss
 - b. Device lock state unknown, minimal duration of loss
 - c. Device lock state unknown, extended duration of loss
 - d. Device known to be unlocked, more than momentary duration of loss
2. Total loss of device
3. Device compromise
4. Device loss or compromise outside the United States

5.13.6 Access Control

Multiple user accounts are not generally supported on limited-feature mobile operating systems. Access control (Section 5.5 Access Control) shall be accomplished by the application that accesses CJI.

5.13.7 Identification and Authentication

Due to the technical methods used for identification and authentication on many limited-feature mobile operating systems, achieving compliance may require many different components.

5.13.7.1 Local Device Authentication

When mobile devices are authorized for use in accessing CJI, local device authentication shall be used to unlock the device for use. The authenticator used shall meet the requirements in section 5.6.2.1 Standard Authenticators.

5.13.7.2 Advanced Authentication

When accessing CJI from an authorized mobile device, advanced authentication shall be used by the authorized user unless the access to CJI is indirect as described in Section 5.6.2.2.1. If access is indirect, then AA is not required.

5.13.7.2.1 Compensating Controls

CSO approved compensating controls to meet the AA requirement on agency-issued smartphones and tablets with limited-feature operating systems are permitted. Compensating controls are temporary control measures that are implemented in lieu of the required AA control measures when an agency cannot meet a requirement due to legitimate technical or business constraints. Before CSOs consider approval of compensating controls, Mobile Device Management (MDM) shall be implemented per Section 5.13.2. The compensating controls shall:

1. Meet the intent of the CJIS Security Policy AA requirement
2. Provide a similar level of protection or security as the original AA requirement
3. Not rely upon the existing requirements for AA as compensating controls
4. Expire upon the CSO approved date or when a compliant AA solution is implemented.

Additionally, compensating controls may rely upon other, non-AA, existing requirements as compensating controls and/or be combined with new controls to create compensating controls.

The compensating controls for AA are a combination of controls providing acceptable assurance only the authorized user is authenticating and not an impersonator or (in the case of agency-issued device used by multiple users) controls that reduce the risk of exposure if information is accessed by an unauthorized party.

The following minimum controls shall be implemented as part of the CSO approved compensating controls:

- Possession and registration of an agency issued smartphone or tablet as an indication it is the authorized user
- Use of device certificates per Section 5.13.7.3 Device Certificates
- Implemented CJIS Security Policy compliant standard authenticator protection on the secure location where CJI is stored

5.13.7.3 Device Certificates

Device certificates are often used to uniquely identify mobile devices using part of a public key pair on the device in the form of a public key certificate. While there is value to ensuring the device itself can authenticate to a system supplying CJI, and may provide a critical layer of device identification or authentication in a larger scheme, a device certificate alone placed on the device shall not be considered valid proof that the device is being operated by an authorized user.

When certificates or cryptographic keys used to authenticate a mobile device are used in lieu of compensating controls for advanced authentication, they shall be:

1. Protected against being extracted from the device
2. Configured for remote wipe on demand or self-deletion based on a number of unsuccessful login or access attempts
3. Configured to use a secure authenticator (i.e. password, PIN) to unlock the key for use

APPENDICES

APPENDIX A TERMS AND DEFINITIONS

Access to Criminal Justice Information — The physical or logical (electronic) ability, right or privilege to view, modify or make use of Criminal Justice Information.

Administration of Criminal Justice — The detection, apprehension, detention, pretrial release, post-trial release, prosecution, adjudication, correctional supervision, or rehabilitation of accused persons or criminal offenders. It also includes criminal identification activities; the collection, storage, and dissemination of criminal history record information; and criminal justice employment. In addition, administration of criminal justice includes “crime prevention programs” to the extent access to criminal history record information is limited to law enforcement agencies for law enforcement programs (e.g. record checks of individuals who participate in Neighborhood Watch or “safe house” programs) and the result of such checks will not be disseminated outside the law enforcement agency.

Agency Controlled Mobile Device — A mobile device that is centrally managed by an agency for the purpose of securing the device for potential access to CJI. The device can be agency issued or BYOD (personally owned).

Agency Coordinator (AC) — A staff member of the Contracting Government Agency who manages the agreement between the Contractor and agency.

Agency Issued Mobile Device — A mobile device that is owned by an agency and issued to an individual for use. It is centrally managed by the agency for the purpose of securing the device for potential access to CJI. The device is not BYOD (personally owned).

Agency Liaison (AL) — Coordinator of activities between the criminal justice agency and the noncriminal justice agency when responsibility for a criminal justice system has been delegated by a criminal justice agency to a noncriminal justice agency, which has in turn entered into an agreement with a contractor. The agency liaison shall, inter alia, monitor compliance with system security requirements. In instances in which the noncriminal justice agency's authority is directly from the CJIS systems agency, there is no requirement for the appointment of an agency liaison.

Asymmetric Encryption — A type of encryption that uses key pairs for encryption. One key is used to encrypt a message and another key to decrypt the message. Asymmetric encryption is also commonly known as public key encryption.

Authorized User/Personnel — An individual, or group of individuals, who have been appropriately vetted through a national fingerprint-based record check and have been granted access to CJI.

Authorized Recipient — (1) A criminal justice agency or federal agency authorized to receive CHRI pursuant to federal statute or executive order; (2) A nongovernmental entity authorized by federal statute or executive order to receive CHRI for noncriminal justice purposes; or (3) A government agency authorized by federal statute or executive order, or state statute which has been approved by the United States Attorney General to receive CHRI for noncriminal justice purposes.

Availability — The degree to which information, a system, subsystem, or equipment is operable and in a useable state; frequently represented as a proportion of time the element is in a functioning condition.

Biographic Data — Information collected about individuals associated with a unique case, and not necessarily connected to identity data. Biographic Data does not provide a history of an individual, only information related to a unique case.

Biometric Data — When applied to CJI, it is used to identify individuals, and includes the following types: fingerprints, palm prints, DNA, iris, and facial recognition.

Case / Incident History — All relevant information gathered about an individual, organization, incident, or combination thereof, arranged so as to serve as an organized record to provide analytic value for a criminal justice organization. In regards to CJI, it is the information about the history of criminal incidents.

Certificate Authority (CA) Certificate — Digital certificates required for certificate-based authentication that are issued to tell the client computers and servers that it can trust other certificates that are issued by this CA.

Channeler — A FBI approved contractor, who has entered into an agreement with an Authorized Recipient(s), to receive noncriminal justice applicant fingerprint submissions and collect the associated fees. The Channeler ensures fingerprint submissions are properly and adequately completed, electronically forwards fingerprint submissions to the FBI's CJIS Division for national noncriminal justice criminal history record check, and receives electronic record check results for dissemination to Authorized Recipients. A Channeler is essentially an "expediter" rather than a user of criminal history record check results.

Cloud Client — A machine or software application that accesses cloud services over a network connection, perhaps on behalf of a subscriber.

Cloud Computing — A distributed computing model that permits on-demand network access to a shared pool of configurable computing resources (i.e., networks, servers, storage, applications, and services), software, and information.

Cloud Provider — An organization that provides cloud computing services.

Cloud Subscriber — A person or organization that is a customer of a cloud computing service provider.

CJIS Advisory Policy Board (APB) — The governing organization within the FBI CJIS Advisory Process composed of representatives from criminal justice and national security agencies within the United States. The APB reviews policy, technical, and operational issues relative to CJIS Division programs and makes subsequent recommendations to the Director of the FBI.

CJIS Audit Unit (CAU) — The organization within the FBI CJIS Division responsible to perform audits of CSAs to verify compliance with the CJIS Security Policy.

CJIS Security Policy — The FBI CJIS Security Policy document as published by the FBI CJIS ISO; the document containing this glossary.

CJIS Systems Agency (CSA) — A duly authorized state, federal, international, tribal, or territorial criminal justice agency on the CJIS network providing statewide (or equivalent) service to its criminal justice users with respect to the CJI from various systems managed by the FBI CJIS

Division. There shall be only one CSA per state or territory. In federal agencies, the CSA may be the interface or switch to other federal agencies connecting to the FBI CJIS systems.

CJIS Systems Agency Information Security Officer (CSA ISO) — The appointed FBI CJIS Division personnel responsible to coordinate information security efforts at all CJIS interface agencies.

CJIS Systems Officer (CSO) — The individual located within the CJIS Systems Agency responsible for the administration of the CJIS network on behalf of the CJIS Systems Agency.

Compact Council — The entity created by the National Crime Prevention and Privacy Compact of 1998 that has the authority to promulgate rules and procedures governing the use of the III system for noncriminal justice purposes.

Compact Officers — The leadership of the Compact Council, oversees the infrastructure established by the National Crime Prevention and Privacy Compact Act of 1998, which is used by ratifying states to exchange criminal records for noncriminal justice purposes. Their primary responsibilities are to promulgate rules and procedures for the effective and appropriate use of the III system.

Compensating Controls — Compensating controls are temporary control measures implemented in lieu of the required control measures when an agency cannot meet the AA requirement due to legitimate technical or business constraints. The compensating controls must:

1. Meet the intent of the CJIS Security Policy AA requirement
2. Provide a similar level of protection or security as the original AA requirement
3. Not rely upon the existing requirements for AA as compensating controls

Additionally, compensating controls may rely upon other, non-AA, existing requirements as compensating controls and/or be combined with new controls to create compensating controls.

Computer Security Incident Response Capability (CSIRC) — A collection of personnel, systems, and processes that are used to efficiently and quickly manage a centralized response to any sort of computer security incident which may occur.

Confidentiality — The concept of ensuring that information is observable only to those who have been granted authorization to do so.

Contractor — A private business, agency or individual which has entered into an agreement for the administration of criminal justice or noncriminal justice functions with a Criminal Justice Agency or a Noncriminal Justice Agency. Also, a private business approved by the FBI CJIS Division to contract with Noncriminal Justice Agencies to perform noncriminal justice functions associated with civil fingerprint submission for hiring purposes.

Contracting Government Agency (CGA) — The government agency, whether a Criminal Justice Agency or a Noncriminal Justice Agency, which enters into an agreement with a private contractor.

Crime Reports Data — The data collected through the Uniform Crime Reporting program and reported upon annually by the FBI CJIS division used to analyze the crime statistics for the United States.

Criminal History Record Information (CHRI) — A subset of CJI. Any notations or other written or electronic evidence of an arrest, detention, complaint, indictment, information or other formal criminal charge relating to an identifiable person that includes identifying information regarding the individual as well as the disposition of any charges.

Criminal Justice Agency (CJA) — The courts, a governmental agency, or any subunit of a governmental agency which performs the administration of criminal justice pursuant to a statute or executive order and which allocates a substantial part of its annual budget to the administration of criminal justice. State and federal Inspectors General Offices are included.

Criminal Justice Agency User Agreement — A terms-of-service agreement that must be signed prior to accessing CJI. This agreement is required by each CJA and spells out user's responsibilities, the forms and methods of acceptable use, penalties for their violation, disclaimers, and so on.

Criminal Justice Conveyance — A criminal justice conveyance is any enclosed mobile vehicle used for the purposes of criminal justice activities with the capability to comply, during operational periods, with the requirements of Section 5.9.1.3.

Criminal Justice Information (CJI) — Criminal Justice Information is the abstract term used to refer to all of the FBI CJIS provided data necessary for law enforcement agencies to perform their mission and enforce the laws, including but not limited to: biometric, identity history, person, organization, property (when accompanied by any personally identifiable information), and case/incident history data. In addition, CJI refers to the FBI CJIS-provided data necessary for civil agencies to perform their mission; including, but not limited to data used to make hiring decisions. The following type of data are exempt from the protection levels required for CJI: transaction control type numbers (e.g. ORI, NIC, UCN, etc.) when not accompanied by information that reveals CJI or PII.

Criminal Justice Information Services Division (FBI CJIS or CJIS) — The FBI division responsible for the collection, warehousing, and timely dissemination of relevant CJI to the FBI and to qualified law enforcement, criminal justice, civilian, academic, employment, and licensing agencies.

Data — See Information and CJI.

Decryption – The inverse cryptographic operation used to convert encrypted information back into a plaintext (readable) format.

Degauss — Neutralize a magnetic field to erase information from a magnetic disk or other storage device. In the field of information technology, degauss has become synonymous with erasing information whether or not the medium is magnetic. In the event the device to be degaussed is not magnetic (e.g. solid state drive, USB storage device), steps other than magnetic degaussing may be required to render the information irretrievable from the device.

Department of Justice (DoJ) — The Department within the U.S. Government responsible to enforce the law and defend the interests of the United States according to the law, to ensure public safety against threats foreign and domestic, to provide federal leadership in preventing and controlling crime, to seek just punishment for those guilty of unlawful behavior, and to ensure fair and impartial administration of justice for all Americans.

Digital Media – Any form of electronic media designed to store data in a digital format. This includes, but is not limited to: memory device in laptops, computers, and mobile devices; and any removable, transportable electronic media, such as magnetic tape or disk, optical disk, flash drives, external hard drives, or digital memory card.

Digital Signature – A digital signature consists of three algorithms: (1) A key generation algorithm that selects a private key uniformly at random from a set of possible private keys. The algorithm outputs the private key and a corresponding public key. (2) A signing algorithm that, given a message and a private key, produces a signature. (3) A signature verifying algorithm that, given a message, public key, and a signature, either accepts or rejects the message's claim to authenticity. Two main properties are required. First, a signature generated from a fixed message and fixed private key should verify the authenticity of that message by using the corresponding public key. Secondly, it should be computationally infeasible to generate a valid signature for a party who does not possess the private key.

Direct Access — (1) Having the authority to access systems managed by the FBI CJIS Division, whether by manual or automated methods, not requiring the assistance of, or intervention by, any other party or agency (28 CFR, Chapter 1, Part 20). (2) Having the authority to query or update national databases maintained by the FBI CJIS Division including national queries and updates automatically or manually generated by the CSA.

Dissemination — The transmission/distribution of CJI to Authorized Recipients within an agency.

Encryption – A form of cryptology that applies a cryptographic operation to provide confidentiality of (sensitive) information.

Escort – Authorized personnel who accompany a visitor at all times while within a physically secure location to ensure the protection and integrity of the physically secure location and any Criminal Justice Information therein. The use of cameras or other electronic means used to monitor a physically secure location does not constitute an escort.

Facsimile (Fax) – Facsimile is: (a) a document received and printed on a single or multi-function stand-alone device, (b) a single or multi-function stand-alone device for the express purpose of transmitting and receiving documents from a like device over a standard telephone line, or (c) a facsimile server, application, service which implements email-like technology and transfers documents over a network.

Federal Bureau of Investigation (FBI) — The agency within the DOJ responsible to protect and defend the United States against terrorist and foreign intelligence threats, to uphold and enforce the criminal laws of the United States, and to provide leadership and criminal justice services to federal, state, municipal, and international agencies and partners.

FBI CJIS Information Security Officer (FBI CJIS ISO) — The FBI personnel responsible for the maintenance and dissemination of the FBI CJIS Security Policy; the liaison between the FBI and the CSA's ISOs and other relevant security points-of-contact (POCs); the provider of technical guidance as to the intent and implementation of technical policy issues; the POC for computer incident notification which also disseminates security alerts to the CSOs and ISOs.

Federal Information Security Management Act (FISMA) — The Federal Information Security Management Act of 2002, a US Federal law that established information security standards for the protection of economic and national security interests of the United States. It requires each federal agency to develop, document, and implement an agency-wide program to provide information

security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

For Official Use Only (FOUO) — A caveat applied to unclassified sensitive information that may be exempt from mandatory release to the public under the Freedom of Information Act (FOIA), 5 U.S.C 522. In general, information marked FOUO shall not be disclosed to anybody except Government (Federal, State, tribal, or local) employees or contractors with a need to know.

Full-feature Operating System — Full-feature operating systems are traditional operating systems used by a standard desktop computer (e.g. Microsoft Windows, Apple OSX/macOS, LINUX/UNIX, etc.). These operating systems are generally open to user control and configuration and therefore require configuration management to properly secure, or “harden”, these devices from malicious network based technical attacks (e.g. malware, spyware, hackers, etc.). These operating systems require traditional protection applications such as antivirus programs and personal firewalls.

Guest Operating System — An operating system that has emulated hardware presented to it by a host operating system. Also referred to as the virtual machine (VM).

Hashing — The process of applying a mathematical algorithm to data to produce an alphanumeric value (i.e. hash value) to be used as a representative of that data.

Hash Value — The term that refers to an alphanumeric value which represents the result of applying a cryptographic hash function to data.

Host Operating System — In the context of virtualization, the operating system that interfaces with the actual physical hardware and arbitrates between it and the guest operating systems. It is also referred to as a hypervisor.

Hybrid Encryption — A type of encryption where both asymmetric encryption and symmetric encryption keys are used creating what is referred to as cipher suites. In a hybrid solution the asymmetric encryption keys are used for client/server certificate exchange to provide session integrity while the symmetric encryption keys are used for bulk data encryption to provide data confidentiality.

Hypervisor — See Host Operating System.

Identity History Data — Textual data that corresponds with an individual’s biometric data, providing a history of criminal and/or civil events for the identified individual.

In-Band – The communication service channel (network connection, email, SMS text, phone call, etc.) used to obtain an authenticator is the same as the one used for login.

Indirect Access – Having the authority to access systems containing CJI without providing the user the ability to conduct transactional activities (the capability to query or update) on state and national systems (e.g. CJIS Systems Agency (CSA), State Identification Bureau (SIB), or national repositories).

Information — See data and CJI.

Information Exchange Agreement — An agreement that codifies the rules by which two parties engage in the sharing of information. These agreements typically include language which establishes some general duty-of-care over the other party’s information, whether and how it can be further disseminated, penalties for violations, the laws governing the agreement (which

establishes venue), procedures for the handling of shared information at the termination of the agreement, and so on. This document will ensure consistency with applicable federal laws, directives, policies, regulations, standards and guidance.

Information Security Officer (ISO) — Typically a member of an organization who has the responsibility to establish and maintain information security policy, assesses threats and vulnerabilities, performs risk and control assessments, oversees the governance of security operations, and establishes information security training and awareness programs. The ISO also usually interfaces with security operations to manage implementation details and with auditors to verify compliance to established policies.

Information System — A system of people, data, and processes, whether manual or automated, established for the purpose of managing information.

Integrated Automated Fingerprint Identification System (IAFIS) — The national fingerprint and criminal history system maintained by the FBI CJIS Division that provides the law enforcement community with automated fingerprint search capabilities, latent searching capability, electronic image storage, and electronic exchange of fingerprints and responses.

Integrity — The perceived consistency of expected outcomes, actions, values, and methods of an individual or organization. As it relates to data, it is the concept that data is preserved in a consistent and correct state for its intended use.

Interconnection Security Agreement (ISA) — An agreement much like an Information Exchange Agreement as mentioned above, but concentrating more on formalizing the technical and security requirements pertaining to some sort of interface between the parties' information systems.

Interface Agency — A legacy term used to describe agencies with direct connections to the CSA. This term is now used predominantly in a common way to describe any sub-agency of a CSA or SIB that leverages the CSA or SIB as a conduit to FBI CJIS information.

Internet Protocol (IP) — A protocol used for communicating data across a packet-switched internetwork using the Internet Protocol Suite, also referred to as TCP/IP. IP is the primary protocol in the Internet Layer of the Internet Protocol Suite and has the task of delivering distinguished protocol datagrams (packets) from the source host to the destination host solely based on their addresses.

Interstate Identification Index (III) — The CJIS service that manages automated submission and requests for CHRI that is warehoused subsequent to the submission of fingerprint information. Subsequent requests are directed to the originating State as needed.

Intrusion Detection — The process of monitoring the events occurring in an information system or network and analyzing them for signs of possible incidents.

Intrusion Detection System — Software which automates the intrusion detection process.

Intrusion Prevention — The process of monitoring events occurring in an information system or network and analyzing them for signs of possible incidents and attempting to stop detected possible incidents.

Intrusion Prevention System — Software which has all the capabilities of an intrusion detection system and can also attempt to stop possible incidents.

Jailbreak (Jailbroken) — The process of attaining privileged control (known as “root access”) of a device running the Apple iOS operating system that ultimately allows a user the ability to alter or replace system applications and settings, run specialized applications that require administrator-level permissions, or perform other operations that are otherwise not allowed.

Laptop Devices – Laptop devices are mobile devices with a full-featured operating system (e.g. Microsoft Windows, Apple OSX/macOS, LINUX/UNIX, etc.). Laptops are typically intended for transport via vehicle mount or portfolio-sized carry case, but not on the body. This definition does not include pocket/handheld devices (e.g. smartphones), or mobile devices that feature a limited-feature operating system (e.g. tablets).

Law Enforcement Enterprise Portal (LEEP) — A secure, Internet-based communications portal provided by the FBI CJIS Division for use by law enforcement, first responders, criminal justice professionals, and anti-terrorism and intelligence agencies around the globe. Its primary purpose is to provide a platform on which various law enforcement agencies can collaborate on FOUO matters.

Limited-feature Operating System — Limited-feature operating systems are designed specifically for the mobile environment where battery life and power efficiency are primary design drivers (e.g. Apple iOS, Android, Windows Mobile, Blackberry OS, etc.). These operating systems permit limited user control, but are inherently more resistant than a full-feature operating system to certain types of network based technical attacks due to the limited-feature sets. Devices using these operating systems are required to be managed by a mobile device management solution.

Logical Access – The technical means (e.g., read, create, modify, delete a file, execute a program, or use an external connection) for an individual or other computer system to utilize CJI or CJIS applications.

Logical Partitioning – When the host operating system, or hypervisor, allows multiple guest operating systems to share the same physical resources.

Local Agency Security Officer (LASO) — The primary Information Security contact between a local law enforcement agency and the CSA under which this agency interfaces with the FBI CJIS Division. The LASO actively represents their agency in all matters pertaining to Information Security, disseminates Information Security alerts and other material to their constituents, maintains Information Security documentation (including system configuration data), assists with Information Security audits of hardware and procedures, and keeps the CSA informed as to any Information Security needs and problems.

Management Control Agreement (MCA) — An agreement between parties that wish to share or pool resources that codifies precisely who has administrative control over, versus overall management and legal responsibility for, assets covered under the agreement. An MCA must ensure the CJA’s authority remains with regard to all aspects of Section 3.2.2. The MCA usually results in the CJA having ultimate authority over the CJI supporting infrastructure administered by the NCJA.

Metadata — Structured information that describes, explains, locates or otherwise makes it easier to retrieve, use or manage an information resource. Metadata is commonly referred to as data about data, information about information, or information describing the characteristics of data.

Mobile Device — Any portable device used to access CJI via a wireless connection (e.g. cellular, WiFi, Bluetooth, etc.).

Mobile Device Management (MDM) — Centralized administration and control of mobile devices specifically including, but not limited to, cellular phones, smart phones, and tablets. Management typically includes the ability to configure device settings and prevent a user from changing them, remotely locating a device in the event of theft or loss, and remotely locking or wiping a device. Management can also include over-the-air distribution of applications and updating installed applications.

Mobile (WiFi) Hotspot — A mobile (WiFi) hotspot is a zone or area associated with a mobile device (e.g. smartphone, air card) allowing wireless connectivity to the Internet typically through a cellular connection.

National Crime Information Center (NCIC) — An information system which stores CJJ which can be queried by appropriate Federal, state, and local law enforcement and other criminal justice agencies.

National Instant Criminal Background Check System (NICS) — A system mandated by the Brady Handgun Violence Prevention Act of 1993 that is used by Federal Firearms Licensees (FFLs) to instantly determine via telephone or other electronic means whether the transfer of a firearm would be in violation of Section 922 (g) or (n) of Title 18, United States Code, or state law, by evaluating the prospective buyer's criminal history.

National Institute of Standards and Technology (NIST) — Founded in 1901, NIST is a non-regulatory federal agency within the U.S. Department of Commerce whose mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic and national security.

Noncriminal Justice Agency (NCJA) — A governmental agency, or any subunit thereof, that provides services primarily for purposes other than the administration of criminal justice. Examples of services include, but not limited to, employment suitability, licensing determinations, immigration and naturalization matters, and national security clearances.

NCJA (Government) — A Federal, state, local, or tribal governmental agency or any subunit thereof whose charter does not include the responsibility to administer criminal justice, but may have a need to process CJJ. An example would be the central IT organization within a state government that administers equipment on behalf of a state law-enforcement agency.

NCJA (Private) — A private agency or subunit thereof whose charter does not include the responsibility to administer criminal justice, but may have a need to process CJJ. An example would include a local bank.

NCJA (Public) — A public agency or sub-unit thereof whose charter does not include the responsibility to administer criminal justice, but may have a need to process CJJ. An example would include a county school board which uses CHRI to assist in employee hiring decisions.

Noncriminal Justice Purpose — The uses of criminal history records for purposes authorized by federal or state law other than purposes relating to the administration of criminal justice, including employment suitability, licensing determinations, immigration and naturalization matters, and national security clearances.

Office of Management and Budget (OMB) — The agency within the Executive Branch of the Federal government responsible to oversee the preparation of the federal budget, to assist in the

supervision of other Executive Branch agencies, and to oversee and coordinate the Presidential Administration's procurement, financial management, information, and regulatory policies.

One-time Password — A disposable, single-use standard authenticator for access CJI. One-time passwords are: minimum of six (6) randomly generated characters, valid for a single session, and if not used, expire within a minimum of five (5) minutes after issuance.

Out-of-Band — The communication service channel (network connection, email, SMS text, phone call, etc.) used to obtain an authenticator is separate from that used for login.

Outsourcing — The process of delegating in-house operations to a third-party. For instance, when the administration of criminal justice functions (network operations, dispatch functions, system administration operations, etc.) are performed for the criminal justice agency by a city or county information technology department or are contracted to be performed by a vendor.

Outsourcing Standard — National Crime Prevention and Privacy Compact Council's Outsourcing Standard. The Compact Council's uniform standards and processes for the interstate and Federal-State exchange of criminal history records for noncriminal justice purposes.

Partitioning – Managing guest operating system, or virtual machine, access to hardware so that each guest OS can access its own resources but cannot encroach on the other guest operating systems resources or any resources not allocated for virtualization use.

Password Verifier (Verifier) – An entity or process that verifies the claimant's identity by verifying the claimant's possession and control of one or two authenticators using an authentication protocol. To do this, the Verifier may also need to validate credentials that link the authenticator(s) to the subscriber's identifier and check their status.

Personal Firewall — An application which controls network traffic to and from a computer, permitting or denying communications based on a security policy.

Personally Identifiable Information (PII) — PII is information which can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name.

Physical Access – The physical ability, right or privilege to view, modify or make use of Criminal Justice Information (CJI) by means of physical presence within the proximity of computers and network devices (e.g. the ability to insert a boot disk or other device into the system, make a physical connection with electronic equipment, etc.).

Physical Media – Physical media refers to media in printed form. This definition includes, but is not limited to, printed documents, printed imagery, printed facsimile.

Physical Partitioning – When the host operating system, or hypervisor, assigns separate physical resources to each guest operating systems, or virtual machine.

Physically Secure Location — A facility, a criminal justice conveyance, or an area, a room, or a group of rooms, within a facility with both the physical and personnel security controls sufficient to protect CJI and associated information systems.

Pocket/Handheld Mobile Device – Pocket/Handheld mobile devices (e.g. smartphones) are intended to be carried in a pocket or holster attached to the body and feature an operating system

with limited functionality (e.g., iOS, Android, BlackBerry, etc.). This definition does not include tablet and laptop devices.

Property Data — Information about vehicles and property associated with a crime.

Rap Back — A NGI service that allows authorized agencies to receive notification of subsequent criminal activity reported to the FBI committed by persons of interest.

Receive-Only Terminal (ROT) – A device that is configured to accept a limited type of data but is technically prohibited from forming or transmitting data, browsing or navigating internal or external networks, or otherwise performing outside the scope of receive only (e.g., a printer, dumb terminal, etc.).

Repository Manager, or Chief Administrator — The designated manager of the agency having oversight responsibility for a CSA’s fingerprint identification services. If both state fingerprint identification services and CJIS systems control are managed within the same state agency, the repository manager and CSO may be the same person.

Root (Rooting, Rooted) — The process of attaining privileged control (known as “root access”) of a device running the Android operating system that ultimately allows a user the ability to alter or replace system applications and settings, run specialized applications that require administrator-level permissions, or perform other operations that are otherwise not allowed.

Salting –The process of applying a non-secret value to data prior to applying a cryptographic process, such as hashing. This process changes the value to be hashed in a manner designed to ensure an attacker cannot reuse the results of computations for one instance.

Secondary Dissemination — The promulgation of CJI from a releasing agency to an authorized recipient agency when the recipient agency has not been previously identified in a formal information exchange agreement.

Security Addendum (SA) — A uniform addendum to an agreement between the government agency and a private contractor, approved by the Attorney General of the United States, which specifically authorizes access to criminal history record information, limits the use of the information to the purposes for which it is provided, ensures the security and confidentiality of the information consistent with existing regulations and the CJIS Security Policy, provides for sanctions, and contains such other provisions as the Attorney General may require.

Sensitive But Unclassified (SBU) — Designation of information in the United States federal government that, though unclassified, often requires strict controls over its distribution. SBU is a broad category of information that includes material covered by such designations as For Official Use Only (FOUO), Law Enforcement Sensitive (LES), Sensitive Homeland Security Information, Security Sensitive Information (SSI), Critical Infrastructure Information (CII), etc. Some categories of SBU information have authority in statute or regulation (e.g. SSI, CII) while others, including FOUO, do not. As of May 9, 2008, the more appropriate terminology to use is Controlled Unclassified Information (CUI).

Server/Client Computer Certificate (device-based) – Digital certificates that are issued to servers or client computers or devices by a CA and used to prove device identity between server and/or client computer devices during the authentication process.

Service — The organized system of apparatus, appliances, personnel, etc, that supply some tangible benefit to the consumers of this service. In the context of CJI, this usually refers to one of the applications that can be used to process CJI.

Shredder — A device used for shredding documents, often as a security measure to prevent unapproved persons from reading them. Strip-cut shredders, also known as straight-cut or spaghetti-cut, slice the paper into long, thin strips but are not considered secure. Cross-cut shredders provide more security by cutting paper vertically and horizontally into confetti-like pieces.

Smartphone — See pocket/handheld mobile devices.

Social Engineering — The act of manipulating people into performing actions or divulging confidential information. While similar to a confidence trick or simple fraud, the term typically applies to trickery or deception for the purpose of information gathering, fraud, or computer system access; in most cases the attacker never comes face-to-face with the victim.

Software Patch — A piece of software designed to fix problems with, or update, a computer program or its supporting data. This includes fixing security vulnerabilities and other bugs and improving the usability or performance. Though meant to fix problems, poorly designed patches can sometimes introduce new problems. As such, patches should be installed in a test environment prior to being installed in a live, operational system. Patches often can be found in multiple locations but should be retrieved only from sources agreed upon through organizational policy.

State and Federal Agency User Agreement — A written agreement that each CSA or SIB Chief shall execute with the FBI CJIS Division stating their willingness to demonstrate conformance with the FBI CJIS Security Policy prior to the establishment of connectivity between organizations. This agreement includes the standards and sanctions governing use of CJIS systems, as well as verbiage to allow the FBI to periodically audit the CSA as well as to allow the FBI to penetration test its own network from the CSA's interfaces to it.

State Compact Officer — The representative of a state that is party to the National Crime Prevention and Privacy Compact, and is the chief administrator of the state's criminal history record repository or a designee of the chief administrator who is a regular full-time employee of the repository.

State Identification Bureau (SIB) — The state agency with the responsibility for the state's fingerprint identification services.

State Identification Bureau (SIB) Chief — The SIB Chief is the designated manager of state's SIB. If both state fingerprint identification services and CJIS systems control are managed within the same state agency, the SIB Chief and CSO may be the same person.

State of Residency — A state of residency is the state in which an individual claims and can provide documented evidence as proof of being his/her permanent living domicile. CJIS Systems Officers have the latitude to determine what documentation constitutes acceptable proof of residency.

Symmetric Encryption — A type of encryption where the same key is used to encrypt and decrypt a message. Symmetric encryption is also known as secret key encryption.

System — Refer to connections to the FBI's criminal justice information repositories and the equipment used to establish said connections. In the context of CJI, this usually refers to

applications and all interconnecting infrastructure required to use those applications that process CJI.

Tablet Devices – Tablet devices are mobile devices with a limited-feature operating system (e.g. iOS, Android, Windows RT, etc.). Tablets typically consist of a touch screen without a permanently attached keyboard intended for transport via vehicle mount or portfolio-sized carry case but not on the body. This definition does not include pocket/handheld devices (e.g. smartphones) or mobile devices with full-featured operating systems (e.g. laptops).

Terminal Agency Coordinator (TAC) — Serves as the point-of-contact at the local agency for matters relating to CJIS information access. A TAC administers CJIS systems programs within the local agency and oversees the agency's compliance with CJIS systems policies.

User Certificate (user-based) – Digital certificates that are unique and issued to individuals by a CA. Though not always required to do so, these specific certificates are often embedded on smart cards or other external devices as a means of distribution to specified users. This certificate is used when individuals need to prove their identity during the authentication process.

Virtual Escort – Authorized personnel who actively monitor a remote maintenance session on Criminal Justice Information (CJI)-processing systems. The escort must have the ability to end the session at any time deemed necessary to ensure the protection and integrity of CJI at all times.

Virtual Machine (VM) – See Guest Operating System

Virtualization — Refers to a methodology of dividing the resources of a computer (hardware and software) into multiple execution environments, by applying one or more concepts or technologies such as hardware and software partitioning, time-sharing, partial or complete machine simulation or emulation allowing multiple operating systems, or images, to run concurrently on the same hardware.

Voice over Internet Protocol (VoIP) — A set of software, hardware, and standards designed to make it possible to transmit voice over packet switched networks, either an internal Local Area Network, or across the Internet.

Wireless Access Point – A wireless access point is a device that logically connects a wireless client device to an organization's enterprise network which processes unencrypted CJI.

Wireless (WiFi) Hotspot – A wireless (WiFi) hotspot is a zone or area within a fixed location allowing wireless connectivity to the Internet typically through a wired connection. Hotspots are typically available in public areas such as airports, hotels and restaurants.

APPENDIX B ACRONYMS

Acronym	Term
AA	Advanced Authentication
AC	Agency Coordinator
ACL	Access Control List
AES	Advanced Encryption Standard
AP	Access Point
APB	Advisory Policy Board
BD-ADDR	Bluetooth-Enabled Wireless Devices and Addresses
BYOD	Bring Your Own Device
CAD	Computer-Assisted Dispatch
CAU	CJIS Audit Unit
CFR	Code of Federal Regulations
CGA	Contracting Government Agency
CHRI	Criminal History Record Information
CJA	Criminal Justice Agency
CJI	Criminal Justice Information
CJIS	Criminal Justice Information Services
ConOps	Concept of Operations
CSA	CJIS Systems Agency
CSIRC	Computer Security Incident Response Capability
CSO	CJIS Systems Officer
DAA	Designated Approving Authority
DoJ	Department of Justice

DoJCERT	DoJ Computer Emergency Response Team
FBI	Federal Bureau of Investigation
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FOIA	Freedom of Information Act
FOUO	For Official Use Only
HIDS	Host-based Intrusion Detection System
HIPS	Host-based Intrusion Prevention System
HTTP	Hypertext Transfer Protocol
IAFIS	Integrated Automated Fingerprint Identification System
IDS	Intrusion Detection System
III	Interstate Identification Index
IP	Internet Protocol
IPS	Intrusion Prevention System
IPSEC	Internet Protocol Security
ISA	Interconnection Security Agreement
ISO	Information Security Officer
IT	Information Technology
LASO	Local Agency Security Officer
LEEP	Law Enforcement Enterprise Portal
LMR	Land Mobile Radio
MAC	Media Access Control
MCA	Management Control Agreement
MDM	Mobile Device Management
MITM	Man-in-the-Middle

MOU	Memorandum of Understanding
NCIC	National Crime Information Center
NCJA	Noncriminal Justice Agency
NICS	National Instant Criminal Background Check System
NIDS	Network-based Intrusion Detection System
NIPS	Network-based Intrusion Prevention System
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
ORI	Originating Agency Identifier
OTP	One-time Password
PBX	Private Branch Exchange
PCSC	Preventing and Combating Serious Crime
PDA	Personal Digital Assistant
PII	Personally Identifiable Information
PIN	Personal Identification Number
PKI	Public Key Infrastructure
POC	Point-of-Contact
PSTN	Public Switched Telephone Network
QA	Quality Assurance
QoS	Quality of Service
RCMP	Royal Canadian Mounted Police
RF	Radio Frequency
SA	Security Addendum
SCO	State Compact Officer
SIB	State Identification Bureau

SIG	Special Interest Group
SP	Special Publication
SPRC	Security Policy Resource Center
SSID	Service Set Identifier
TAC	Terminal Agency Coordinator
TLS	Transport Layer Security
UCN	Universal Control Number
VLAN	Virtual Local Area Network
VM	Virtual Machine
VoIP	Voice Over Internet Protocol
VPN	Virtual Private Network
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access

APPENDIX C NETWORK TOPOLOGY DIAGRAMS

Network diagrams, i.e. topological drawings, are an essential part of solid network security. Through graphical illustration, a comprehensive network diagram provides the “big picture” – enabling network managers to quickly ascertain the interconnecting nodes of a network for a multitude of purposes, including troubleshooting and optimization. Network diagrams are integral to demonstrating the manner in which each agency ensures criminal justice data is afforded appropriate technical security protections and is protected during transit and at rest.

The following diagrams, labeled Appendix C.1-A through C.1-D, are examples for agencies to utilize during the development, maintenance, and update stages of their own network diagrams. By using these example drawings as a guideline, agencies can form the foundation for ensuring compliance with Section 5.7.1.2 of the CJIS Security Policy.

The purpose for including the following diagrams in this Policy is to aid agencies in their understanding of diagram expectations and should not be construed as a mandated method for network topologies. It should also be noted that agencies are not required to use the identical icons depicted in the example diagrams and should not construe any depiction of a particular vendor product as an endorsement of that product by the FBI CJIS Division.

Appendix C.1-A is a conceptual overview of the various types of agencies that can be involved in handling of CJJ, and illustrates several ways in which these interconnections might occur. This diagram is not intended to demonstrate the level of detail required for any given agency’s documentation, but it provides the reader with some additional context through which to digest the following diagrams. Take particular note of the types of network interfaces in use between agencies, in some cases dedicated circuits with encryption mechanisms, and in other cases VPNs over the Internet. This diagram attempts to show the level of diversity possible within the law enforcement community. These diagrams in no way constitute a standard for network engineering, but rather, for the expected quality of documentation.

The next three topology diagrams, C.1-B through C.1-D, depict conceptual agencies. For C.1-B through C.1-D, the details identifying specific “moving parts” in the diagrams by manufacturer and model are omitted, but it is expected that any agencies producing such documentation will provide diagrams with full manufacturer and model detail for each element of the diagram. Note that the quantities of clients should be documented in order to assist the auditor in understanding the scale of assets and information being protected.

Appendix C.1-B depicts a conceptual state law enforcement agency’s network topology and demonstrates a number of common technologies that are in use throughout the law enforcement community (some of which are compulsory per CJIS policy, and some of which are optional) including Mobile Broadband cards, VPNs, Firewalls, Intrusion Detection Devices, VLANs, and so forth. Note that although most state agencies will likely have highly-available configurations, the example diagram shown omits these complexities and only shows the “major moving parts” for clarity but please note the Policy requires the logical location of all components be shown. The level of detail depicted should provide the reader with a pattern to model future documentation from, but should not be taken as network engineering guidance.

Appendix C.1-C depicts a conceptual county law enforcement agency. A number of common technologies are presented merely to reflect the diversity in the community, including proprietary

Packet-over-RF infrastructures and advanced authentication techniques, and to demonstrate the fact that agencies can act as proxies for other agencies.

Appendix C.1-D depicts a conceptual municipal law enforcement agency, presumably a small one that lacks any precinct-to-patrol data communications. This represents one of the smallest designs that could be assembled that, assuming all other details are properly considered, would meet the criteria for Section 5.7.1.2. This diagram helps to demonstrate the diversity in size that agencies handling criminal justice data exhibit.

Figure C-1-A Overview: Conceptual Connections Between Various Agencies

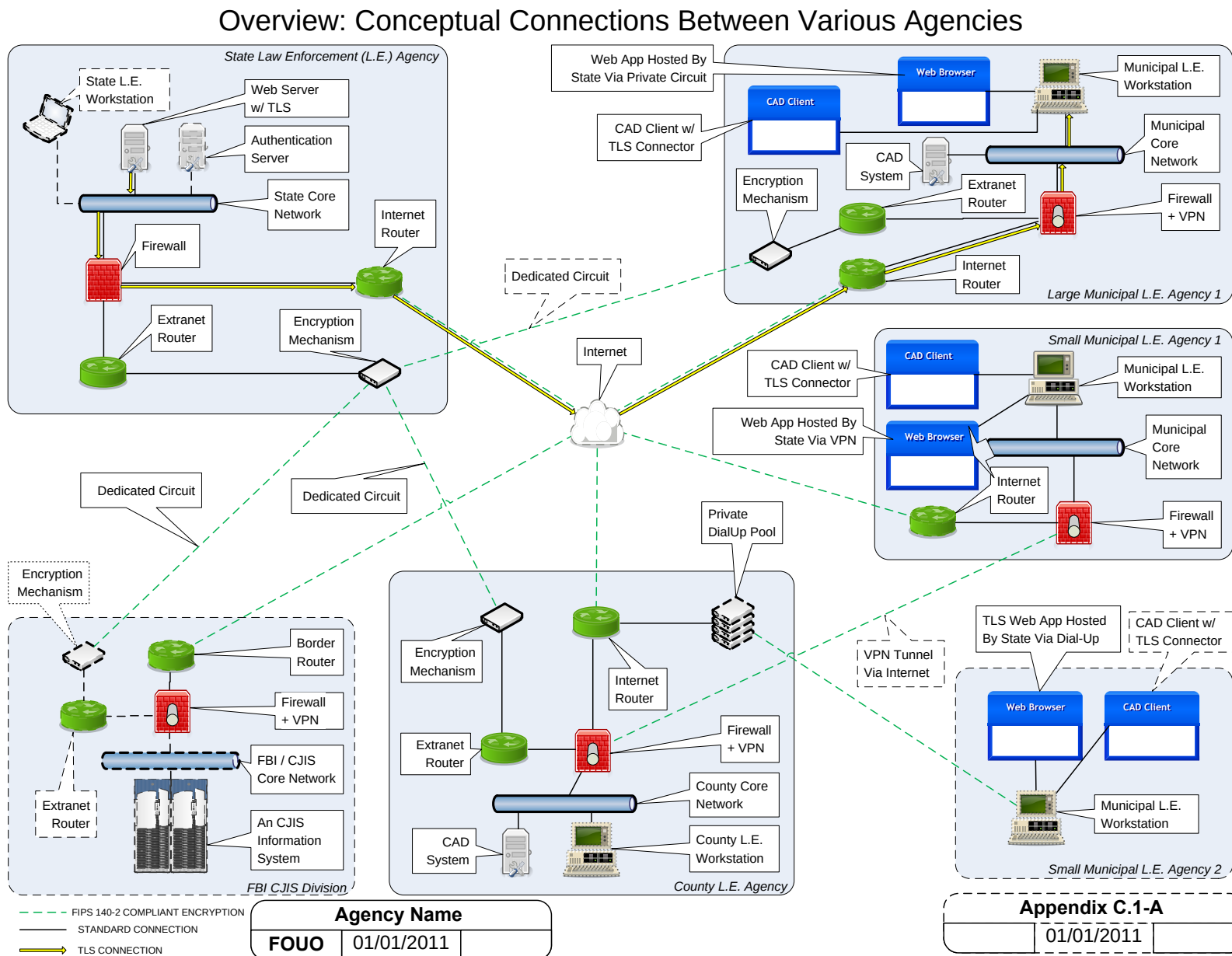
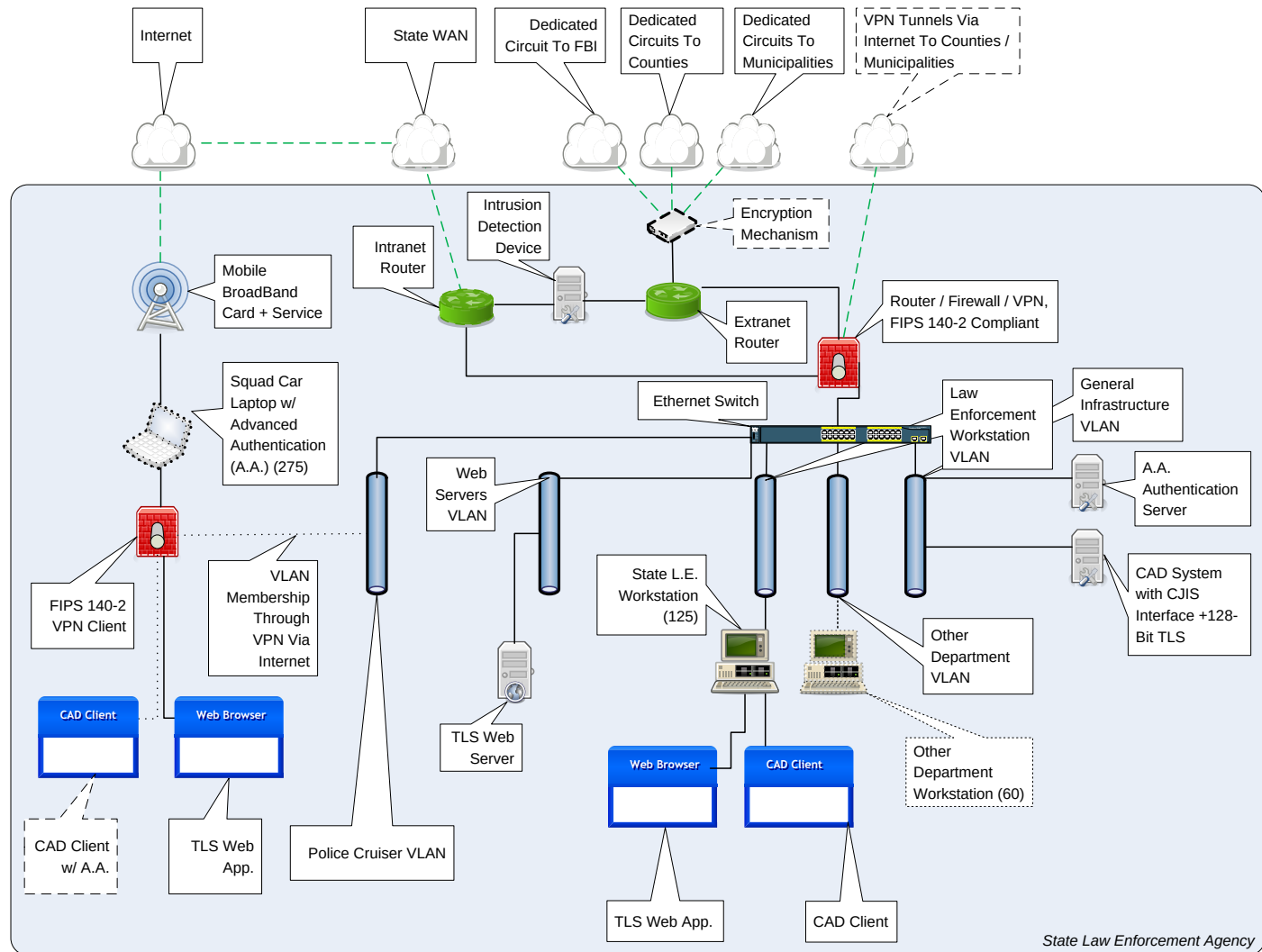


Figure C-1-B Conceptual Topology Diagram for a State Law Enforcement Agency

Conceptual Topology Diagram For A State Law Enforcement Agency



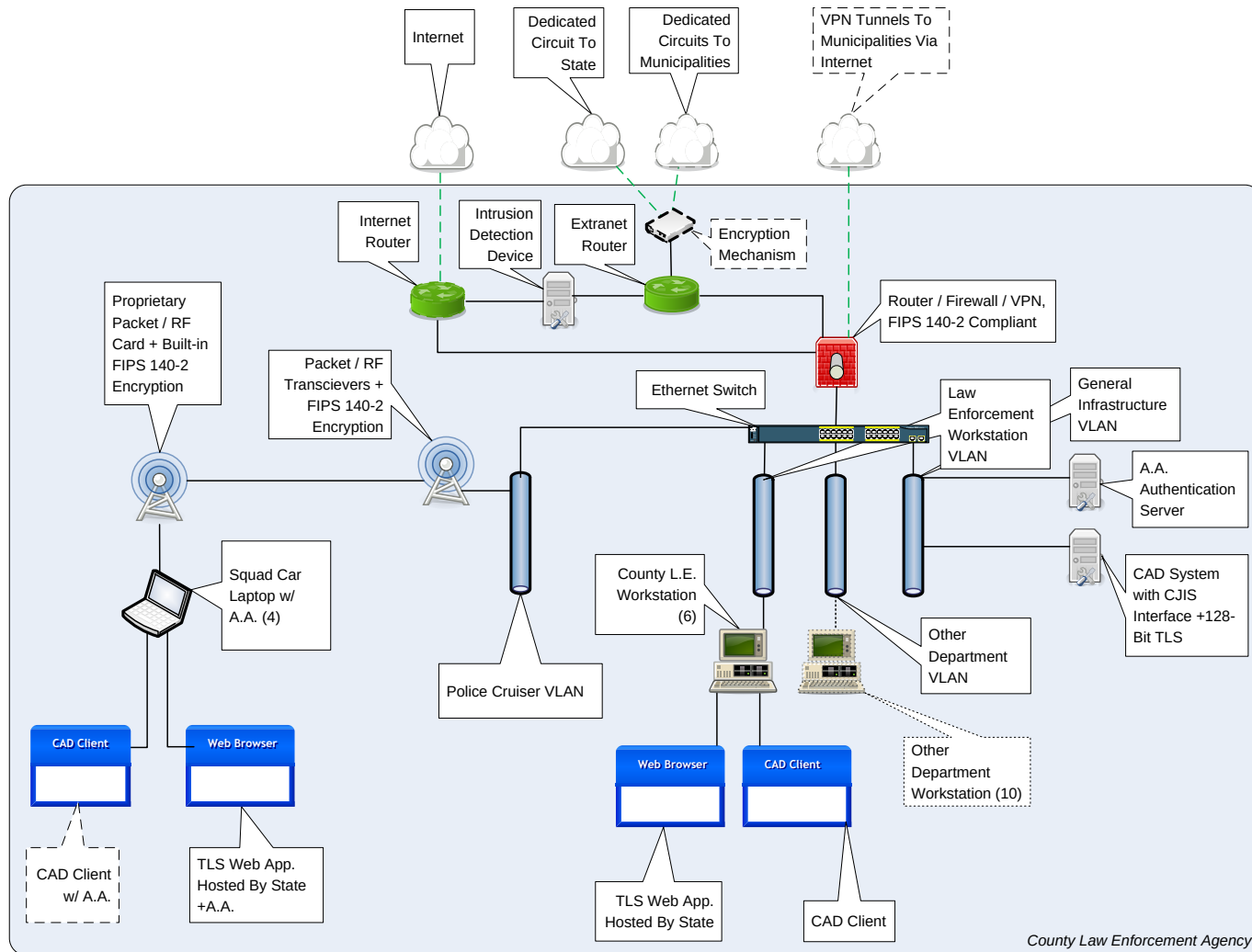
--- FIPS 140-2 COMPLIANT ENCRYPTION
 — STANDARD CONNECTION

Sample State Agency		
FOUO	01/01/2011	

Appendix C.1-B		
	01/01/2011	

Figure C-1-C Conceptual Topology Diagram for a County Law Enforcement Agency

Conceptual Topology Diagram For A County Law Enforcement Agency



--- FIPS 140-2 COMPLIANT ENCRYPTION
 — STANDARD CONNECTION

Sample County Agency

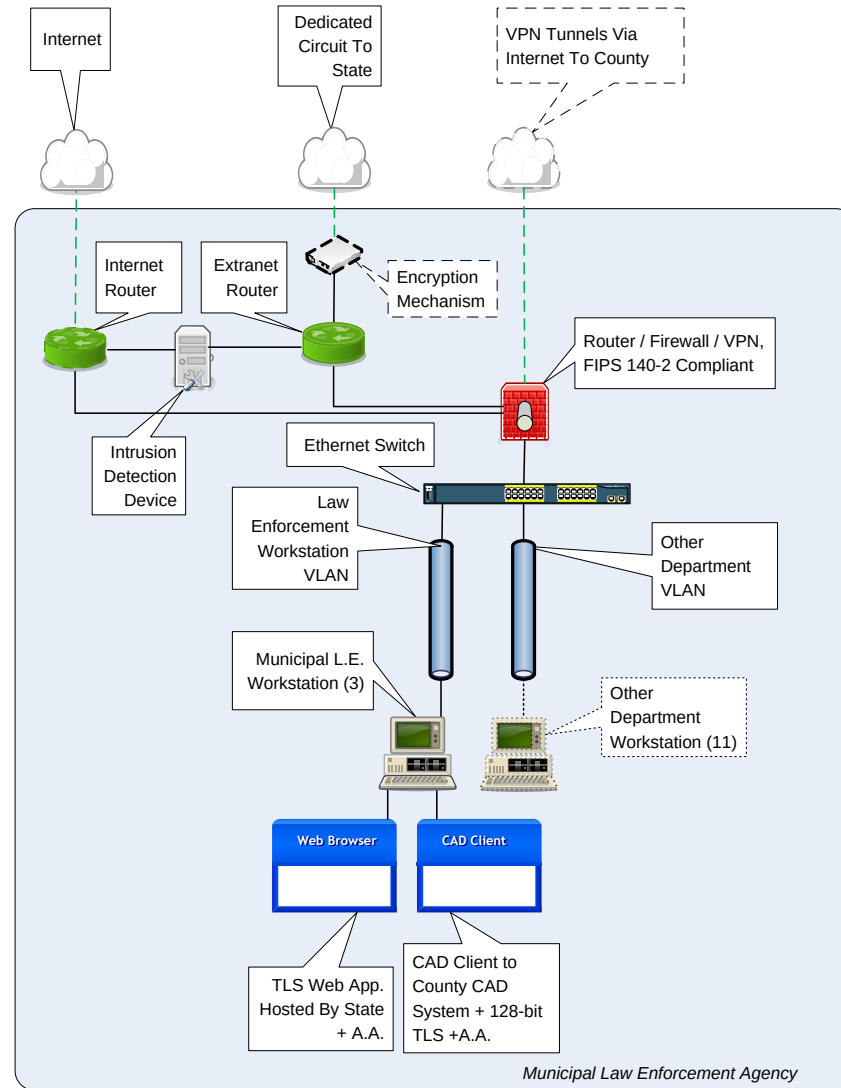
FOUO	01/01/2011	

Appendix C.1-C

01/01/2011	

Figure C-1-D Conceptual Topology Diagram for a Municipal Law Enforcement Agency

Conceptual Topology Diagram For A Municipal Law Enforcement Agency



--- FIPS 140-2 COMPLIANT ENCRYPTION
 — STANDARD CONNECTION

Sample Municipal Agency

FOUO 01/01/2011

Appendix C.1-D

01/01/2011

APPENDIX D SAMPLE INFORMATION EXCHANGE AGREEMENTS

D.1 CJIS User Agreement

CRIMINAL JUSTICE INFORMATION SERVICES (CJIS) SYSTEMS USER AGREEMENT

The FBI CJIS Division provides state-of-the-art identification and information services to the local, state, tribal, federal, and international criminal justice communities, as well as the noncriminal justice community, for licensing and employment purposes. These services are administered and maintained by the FBI CJIS Division and managed in cooperation with the CJIS Systems Agency (CSA) and its administrator for CJIS data, the CJIS Systems Officer (CSO). The CJIS Systems include, but are not limited to: the Interstate Identification Index (III); National Crime Information Center (NCIC); Uniform Crime Reporting (UCR), whether summary or incident-based reporting to the National Incident-Based Reporting System; Fingerprint Identification Record System; Law Enforcement National Data Exchange (N-DEx); Law Enforcement Enterprise Portal; and the National Instant Criminal Background Check System (NICS).

The FBI CJIS Division provides the following services to its users, as applicable:

1. Operational, technical, and investigative assistance.
2. Telecommunication lines to state, federal, and regulatory interfaces.
3. Legal and legislative review of matters pertaining to all CJIS Systems.
4. Timely information on all aspects of all CJIS Systems and other related programs by means of operating manuals, code manuals, technical and operational updates, various newsletters, information letters, frequently asked questions, and other relevant documents.
5. Training assistance and up-to-date materials provided to each CSO, NICS Point of Contact (POC), state Compact Officer, State Administrator, Information Security Officer (ISO), and other appropriate personnel.
6. Ongoing assistance to Systems' users through meetings and briefings with the CSOs, State Administrators, Compact Officers, ISOs, and NICS State POCs to discuss operational and policy issues.
7. Advisory Process through which authorized users have input as to the policies and procedures governing the operation of CJIS programs.

8. National Crime Prevention and Privacy Compact Administrative Office through which states and other authorized users may submit issues concerning the noncriminal justice use of the III System.
9. Annual NICS Users Conference.
10. Audit.
11. Staff research assistance.

PART 1

The purpose behind a designated CSO is to unify responsibility for Systems user discipline and to ensure adherence to established procedures and policies within each signatory state/territory/tribal agency and by each federal user. This agreement outlines the responsibilities of each CSO as they relate to all CJIS Systems and other related CJIS administered programs. These individuals are ultimately responsible for planning necessary hardware, software, funding, and training for access to all CJIS Systems.

To ensure continued access as set forth above, the CSA agrees to adhere to all applicable CJIS policies including, but not limited to, the following:

1. The signatory state/tribal agency will provide fingerprints that meet submission criteria for all qualifying arrests. In addition, states/tribal agencies will make their records available for interstate exchange for criminal justice and other authorized purposes unless restricted by state/tribal law, and, where applicable, continue to move toward participation in the III and, upon ratification of the National Crime Prevention and Privacy Compact, the National Fingerprint File.
2. Appropriate and reasonable quality assurance procedures; e.g., hit confirmation, audits for record timeliness, and validation, must be in place to ensure that only complete, accurate, and valid information is maintained in the CJIS Systems.
3. Biannual file synchronization of information entered into the III by participating states.
4. Security - Each agency is responsible for appropriate security measures as applicable to physical security of terminals and telecommunication lines; personnel security to include background screening requirements; technical security to protect against unauthorized use; data security to include III use, dissemination, and logging; and security of criminal history

records. Additionally, each CSO must ensure that all agencies establish an information security structure that provides for an ISO and complies with the CJIS Security Policy.

5. Audit - Each agency shall be responsible for complying with all audit requirements for use of CJIS Systems. Each CSO is responsible for completing a triennial audit of all agencies with access to CJIS Systems through the CSO's lines.
6. Training - Each agency shall be responsible for training requirements, including compliance with operator training mandates.
7. Integrity of the Systems - Each agency shall be responsible for maintaining the integrity of the system in accordance with FBI CJIS Division/state/federal/tribal policies to ensure only authorized terminal access; only authorized transaction submission; and proper handling and dissemination of CJL. Each agency shall also be responsible for computer security incident reporting as required by the *CJIS Security Policy*.

The following documents are incorporated by reference and made part of this agreement for CSA users:

1. Bylaws for the CJIS Advisory Policy Board and Working Groups.
2. CJIS Security Policy.
3. Interstate Identification Index Operational and Technical Manual, National Fingerprint File Operations Plan, NCIC 2000 Operating Manual, UCR Handbook-NIBRS Edition, and National Incident-Based Reporting System Volumes 1, 2, and 4.
4. National Crime Prevention and Privacy Compact, 42 United States Code (U.S.C.) §14616.
5. NCIC Standards and UCR Standards, as recommended by the CJIS Advisory Policy Board.
6. The National Fingerprint File Qualification Requirements.
7. Title 28, Code of Federal Regulations, Parts 20 and 25, §50.12, and Chapter IX.
8. Electronic Fingerprint Transmission Specifications.

9. Other relevant documents, to include: NCIC Technical and Operational Updates, CJIS Information Letters, NICS User Manual, NICS Interface Control Document.
10. Applicable federal, state, and tribal laws and regulations.

PART 2

Additionally, there are authorized federal regulatory recipients and other authorized users that provide electronic fingerprint submissions through a CJIS Wide Area Network (WAN) connection (or other approved form of electronic connection) to the CJIS Division that are required to comply with the following CJIS policies:

1. The authorized user will provide fingerprints that meet submission criteria and apply appropriate and reasonable quality assurance procedures.
2. Security - Each agency is responsible for appropriate security measures as applicable to physical security of communication equipment; personnel security to include background screening requirements; technical security to protect against unauthorized use; and security of criminal history records.
3. Audit - Each authorized user shall be responsible for complying with all audit requirements for CJIS Systems. Additionally, each authorized user is subject to a triennial audit by the CJIS Division Audit staff.
4. Training - Each authorized user receiving criminal history record information shall be responsible for training requirements, including compliance with proper handling of criminal history records.

The following documents are incorporated by reference and made part of this agreement for non-CSA authorized users:

1. CJIS Security Policy.
2. National Crime Prevention and Privacy Compact, 42 U.S.C. §14616.
3. Title 28, Code of Federal Regulations, Parts 20 and 25, § 50.12, and Chapter IX.
4. Other relevant documents, to include CJIS Information Letters.

5. Applicable federal, state, and tribal laws and regulations.

GENERAL PROVISIONS

Funding:

Unless otherwise agreed in writing, each party shall bear its own costs in relation to this agreement. Expenditures will be subject to federal and state budgetary processes and availability of funds pursuant to applicable laws and regulations. The parties expressly acknowledge that this in no way implies that Congress will appropriate funds for such expenditures.

Termination:

1. All activities of the parties under this agreement will be carried out in accordance to the above-described provisions.
2. This agreement may be amended or terminated by the mutual written consent of the parties authorized representatives.
3. Either party may terminate this agreement upon 30-days written notification to the other party. Such notice will be the subject of immediate consultation by the parties to decide upon the appropriate course of action. In the event of such termination, the following rules apply:
 - a. The parties will continue participation, financial or otherwise, up to the effective date of termination.
 - b. Each party will pay the costs it incurs as a result of termination.
 - c. All information and rights therein received under the provisions of this agreement prior to the termination will be retained by the parties, subject to the provisions of this agreement.

ACKNOWLEDGMENT AND CERTIFICATION

As a CSO or CJIS WAN Official (or other CJIS authorized official), I hereby acknowledge the duties and responsibilities as set out in this agreement. I acknowledge that these duties and responsibilities have been developed and approved by CJIS Systems users to ensure the reliability, confidentiality, completeness, and accuracy of all information contained in, or obtained by means of, the CJIS Systems. I further acknowledge that failure to comply with these duties and responsibilities may result in the imposition of sanctions against the offending state/agency; other federal, tribal, state, and local criminal justice users; and approved noncriminal justice users with System access, whether direct or indirect. The Director of the FBI (or the National Crime Prevention and Privacy Compact Council), may approve sanctions to include the termination of CJIS services.

I hereby certify that I am familiar with all applicable documents that are made part of this agreement and to all applicable federal and state laws and regulations relevant to the receipt and dissemination of documents provided through the CJIS Systems.

This agreement is a formal expression of the purpose and intent of both parties and is effective when signed. It may be amended by the deletion or modification of any provision contained therein, or by the addition of new provisions, after written concurrence of both parties. The "Acknowledgment and Certification" is being executed by the CSO or CJIS WAN Official (or other CJIS authorized official) in both an individual and representative capacity. Accordingly, this agreement will remain in effect after the CSO or CJIS WAN Official (or other CJIS authorized official) vacates his/her position or until it is affirmatively amended or rescinded in writing. This agreement does not confer, grant, or authorize any rights, privileges, or obligations to any third party.

SYSTEMS USER AGREEMENT

Please execute either Part 1 or Part 2

PART 1

CJIS Systems Officer

Date: _____

Printed Name/Title

CONCURRENCE OF CSA HEAD:

CSA Head

Date: _____

Printed Name/Title

PART 2

CJIS WAN Official (or other CJIS Authorized Official)

Date: _____

Printed Name/Title

CONCURRENCE OF CJIS WAN AGENCY HEAD:

CJIS WAN Agency Head

Date: _____

Printed Name/Title

FBI CJIS DIVISION:

Date: _____

[Name]

Assistant Director

FBI CJIS Division

* The FBI Designated Federal Officer should be notified when a CSO or other CJIS WAN/authorized Official vacates his/her position. The name and telephone number of the Acting CSO or other CJIS WAN/authorized Official, and when known, the name and telephone number of the new CSO or other CJIS WAN/authorized Official, should be provided. Revised: 05/03/2006

D.2 Management Control Agreement

Management Control Agreement

Pursuant to the CJIS Security Policy, it is agreed that with respect to administration of that portion of computer systems and network infrastructure interfacing directly or indirectly with the state network (Network Name) for the interstate exchange of criminal history/criminal justice information, the (Criminal Justice Agency) shall have the authority, via managed control, to set, maintain, and enforce:

- (1) Priorities.
- (2) Standards for the selection, supervision, and termination of personnel access to Criminal Justice Information (CJI).
- (3) Policy governing operation of justice systems, computers, access devices, circuits, hubs, routers, firewalls, and any other components, including encryption, that comprise and support a telecommunications network and related criminal justice systems to include but not limited to criminal history record/criminal justice information, insofar as the equipment is used to process or transmit criminal justice systems information guaranteeing the priority, integrity, and availability of service needed by the criminal justice community.
- (4) Restriction of unauthorized personnel from access or use of equipment accessing the State network.
- (5) Compliance with all rules and regulations of the (Criminal Justice Agency) Policies and CJIS Security Policy in the operation of all information received.

“...management control of the criminal justice function remains solely with the Criminal Justice Agency.” Section 5.1.1.4

This agreement covers the overall supervision of all (Criminal Justice Agency) systems, applications, equipment, systems design, programming, and operational procedures associated with the development, implementation, and maintenance of any (Criminal Justice Agency) system to include NCIC Programs that may be subsequently designed and/or implemented within the (Criminal Justice Agency).

John Smith, CIO
Any State Department of Administration

Date

Joan Brown, CIO
(Criminal Justice Agency)

Date

D.3 Noncriminal Justice Agency Agreement & Memorandum of Understanding

MEMORANDUM OF UNDERSTANDING

BETWEEN

THE FEDERAL BUREAU OF INVESTIGATION

AND

(Insert Name of Requesting Organization)

FOR

THE ESTABLISHMENT AND ACCOMMODATION OF
THIRD-PARTY CONNECTIVITY TO THE
CRIMINAL JUSTICE INFORMATION SERVICES DIVISION'S WIDE AREA NETWORK

1. **PURPOSE:** This Memorandum of Understanding (MOU) between the Federal Bureau of Investigation (FBI) and **(insert requesting organization's name)**, hereinafter referred to as the "parties," memorializes each party's responsibilities with regard to establishing connectivity to records services accessible via the Wide Area Network (WAN) of the FBI's Criminal Justice Information Services (CJIS) Division.

2. **BACKGROUND:** The requesting organization, **(insert requesting organization's name)**, being approved for access to systems of records accessible via the CJIS WAN, desires connectivity to the CJIS WAN or via a secure Virtual Private Network (VPN) Connection (Internet) to the CJIS WAN. The CJIS Division has created a framework for accommodating such requests based on the type of connection.

In preparing for such non-CJIS-funded connectivity to the CJIS WAN, the parties plan to acquire, configure, and place needed communications equipment at suitable sites and to make electronic connections to the appropriate systems of records via the CJIS WAN.

To ensure that there is a clear understanding between the parties regarding their respective roles in this process, this MOU memorializes each party's responsibilities regarding the development, operation, and maintenance of third-party connectivity to the CJIS WAN. Unless otherwise contained in an associated contract, the enclosed terms apply. If there is a conflict between terms and provisions contained in both the contract and this MOU, the contract will prevail.

3. **AUTHORITY:** The FBI is entering into this MOU under the authority provided by Title 28, United States Code (U.S.C.), Section 534; 42 U.S.C. § 14616; and/or Title 28, Code of Federal Regulations, Part 906.

4. **SCOPE:**

a. The CJIS Division agrees to:

i. Provide the requesting organization with a "CJIS WAN Third-Party Connectivity Package" that will detail connectivity requirements and options compatible with the CJIS Division's WAN architecture upon receipt of a signed nondisclosure statement.

ii. Configure the requesting organization's connection termination equipment suite at Clarksburg, West Virginia, and prepare it for deployment or shipment under the CJIS WAN option. In the Secure VPN arrangement only, the third party will develop, configure, manage, and maintain its network connectivity to its preferred service provider.

iii. Work with the requesting organization to install the connection termination equipment suite and verify connectivity.

iv. Perform installation and/or routine maintenance on the requesting organization's third-party dedicated CJIS WAN connection termination equipment after coordinating with the requesting organization's designated point of contact (POC) and during a time when the CJIS Division's technical personnel are near the requesting organization's site.

v. Perform periodic monitoring and troubleshooting of the requesting organization's CJIS WAN connection termination equipment. Software patches will be maintained on the dedicated CJIS WAN connected network equipment only. Under the Secure VPN option, no availability or data thru-put rates will be guaranteed.

vi. Provide 24 hours a day, 7 days a week uninterrupted monitoring from the CJIS Division's Network Operations Center.

vii. Provide information regarding potential hardware end-of-life replacement cycles to the requesting organization for its budgeting purposes.

viii. Maintain third-party dedicated CJIS WAN connection termination equipment as if in the CJIS Division's operational environment.

ix. Update the appropriate software on the requesting organization's dedicated connection termination equipment connected to the CJIS WAN (i.e., Cisco Internetwork Operating System, SafeNet frame relay encryptor firmware, etc.) pursuant to the requesting organization's authorized maintenance contracts.

x. Provide a POC and telephone number for MOU-related issues.

b. The **(insert requesting organization's name)** agrees to:

i. Coordinate requests for third-party connectivity to the CJIS WAN or the Secure VPN with the CJIS Division's POC.

ii. Purchase hardware and software that are compatible with the CJIS WAN.

iii. Pay for the telecommunications infrastructure that supports its connection to the CJIS WAN or Secure VPN.

iv. Maintain telecommunication infrastructure in support of Secure VPN connectivity.

v. Provide any/all hardware and software replacements and upgrades as mutually agreed to by the parties.

vi. Pay for all telecommunication requirements related to its connectivity.

vii. Provide required information for dedicated service relating to Data Link Connection Identifiers, Circuit Identifier, Permanent Virtual Circuit Identifiers, Local Exchange Carrier Identifier, POC, location, etc., as determined by the parties.

viii. Transport the CJIS WAN connection termination equipment suite to the CJIS Division for configuration and preparation for deployment under the dedicated service option.

ix. Provide registered Internet Protocol information to be used by the requesting organization's system to the CJIS Division.

x. Provide the CJIS Division with six months advance notice or stated amount of time for testing activities (i.e., disaster recovery exercises).

xi. Provide the CJIS Division with applicable equipment maintenance contract numbers and level of service verifications needed to perform software upgrades on connection termination equipment.

xii. Provide the CJIS Division with applicable software upgrade and patch images (or information allowing the CJIS Division to access such images).

xiii. Transport only official, authorized traffic over the Secure VPN.

xiv. Provide a POC and telephone number for MOU-related issues.

5. FUNDING: There are no reimbursable expenses associated with this level of support. Each party will fund its own activities unless otherwise agreed to in writing. This MOU is not an obligation or commitment of funds, nor a basis for transfer of funds, but rather is a basic statement of understanding between the parties hereto of the nature of the relationship for the connectivity efforts. Unless otherwise agreed to in writing, each party shall bear its own costs in relation to this MOU. Expenditures by each party will be subject to its budgetary processes and to the availability of funds and resources pursuant to applicable laws, regulations, and policies. The parties expressly acknowledge that the above language in no way implies that Congress will appropriate funds for such expenditures.

6. SETTLEMENT OF DISPUTES: Disagreements between the parties arising under or relating to this MOU will be resolved only by consultation between the parties and will not be referred to any other person or entity for settlement.

7. SECURITY: It is the intent of the parties that the actions carried out under this MOU will be conducted at the unclassified level. No classified information will be provided or generated under this MOU.

8. AMENDMENT, TERMINATION, ENTRY INTO FORCE, AND DURATION:

a. All activities of the parties under this MOU will be carried out in accordance with the above - described provisions.

b. This MOU may be amended or terminated by the mutual written consent of the parties' authorized representatives.

c. Either party may terminate this MOU upon 30-days written notification to the other party. Such notice will be the subject of immediate consultation by the parties to decide upon the appropriate course of action. In the event of such termination, the following rules apply:

i. The parties will continue participation, financial or otherwise, up to the effective date of the termination.

ii. Each party will pay the costs it incurs as a result of the termination.

iii. All information and rights therein received under the provisions of this MOU prior to the termination will be retained by the parties, subject to the provisions of this MOU.

9. FORCE AND EFFECT: This MOU, which consists of nine numbered sections, will enter into effect upon signature of the parties and will remain in effect until terminated. The parties should review the contents of this MOU annually to determine whether there is a need for the deletion, addition, or amendment of any provision. This MOU is not intended, and should not be construed, to create any right or benefit, substantive or procedural, enforceable at law or otherwise by any third party against the parties, their parent agencies, the United States, or the officers, employees, agents, or other associated personnel thereof.

The foregoing represents the understandings reached between the parties.

FOR THE FEDERAL BUREAU OF INVESTIGATION

[Name]

Date

Assistant Director

Criminal Justice Information Services Division

FOR THE (insert requesting organization name)

Date

D.4 Interagency Connection Agreement

CRIMINAL JUSTICE INFORMATION SERVICES (CJIS)

Wide Area Network (WAN) USER AGREEMENT

BY INTERIM REMOTE LATENT USERS

The responsibility of the FBI CJIS Division is to provide state-of-the-art identification and information services to the local, state, federal, and international criminal justice communities, as well as the civil community for licensing and employment purposes. The data provided by the information systems administered and maintained by the FBI CJIS Division are routed to and managed in cooperation with the designated interface agency official. This information includes, but is not limited to, the Interstate Identification Index (III), National Crime Information Center (NCIC), Uniform Crime Reporting (UCR)/National Incident-Based Reporting System (NIBRS), and the Integrated Automated Fingerprint Identification System (IAFIS) programs.

In order to fulfill this responsibility, the FBI CJIS Division provides the following services to its users:

- Operational, technical, and investigative assistance;
- Telecommunications lines to local, state, federal and authorized interfaces;
- Legal and legislative review of matters pertaining to IAFIS, CJIS WAN and other related services;
- Timely information on all aspects of IAFIS, CJIS WAN, and other related programs by means of technical and operational updates, various newsletters, and other relative documents;
- Shared management through the CJIS Advisory Process and the Compact Council;
- Training assistance and up-to-date materials provided to each designated agency official, and;
- Audit.

The concept behind a designated interface agency official is to unify responsibility for system user discipline and ensure adherence to system procedures and policies within each interface agency. These individuals are ultimately responsible for planning necessary hardware, software, funding, training, and the administration of policy and procedures including security and integrity for complete access to CJIS related systems and CJIS WAN related data services by authorized agencies.

The following documents and procedures are incorporated by reference and made part of this agreement:

- *CJIS Security Policy*;
- *Title 28, Code of Federal Regulations, Part 20*;
- Computer Incident Response Capability (CIRC);
- Applicable federal and state laws and regulations.

To ensure continued access as set forth above, the designated interface agency agrees to adhere to all CJIS policies, including, but not limited to, the following:

1. The signatory criminal agency will provide fingerprints for all qualifying arrests either via electronic submission or fingerprint card that meet submission criteria. In addition, the agency will make their records available for interstate exchange for criminal justice and other authorized purposes.
2. The signatory civil agency with legislative authority will provide all qualifying fingerprints via electronic submission or fingerprint card that meet submission criteria.
3. Appropriate and reasonable quality assurance procedures must be in place to ensure that only complete, accurate, and valid information is maintained in the system.
4. Security - Each agency is responsible for appropriate security measures as applicable to physical security of terminals and telecommunications lines; Interim Distributed Imaging System (IDIS) equipment shall remain stand-alone

devices and be used only for authorized purposes; personnel security to meet background screening requirements; technical security to protect against unauthorized use; data security, dissemination, and logging for audit purposes; and actual security of criminal history records. Additionally, each agency must establish an information security structure that provides for an Information Security Officer (ISO) or a security point of contact.

5. Audit - Each agency shall be responsible for complying with the appropriate audit requirements.
6. Training - Each agency shall be responsible for training requirements, including compliance with training mandates.
7. Integrity of the system shall be in accordance with FBI CJIS Division and interface agency policies. Computer incident reporting shall be implemented.

Until states are able to provide remote latent connectivity to their respective latent communities via a state WAN connection, the CJIS Division may provide direct connectivity to IAFIS via a dial-up connection or through the Combined DNA Index System (CODIS) and/or National Integrated Ballistics Information Network (NIBIN) connections. When a state implements a latent management system and is able to provide intrastate connectivity and subsequent forwarding to IAFIS, this agreement may be terminated. Such termination notice will be provided in writing by either the FBI or the state CJIS Systems Agency.

It is the responsibility of the local remote latent user to develop or acquire an IAFIS compatible workstation. These workstations may use the software provided by the FBI or develop their own software, provided it is IAFIS compliant.

The CJIS Division will provide the approved modem and encryptors required for each dial-up connection to IAFIS. The CJIS Communication Technologies Unit will configure and test the encryptors before they are provided to the user. Users requesting remote latent connectivity through an existing CODIS and/or NIBIN connection must receive verification from the FBI that there are a sufficient number of Ethernet ports on the router to accommodate the request.

If at any time search limits are imposed by the CJIS Division, these individual agency connections will be counted toward the total state allotment.

ACKNOWLEDGMENT AND CERTIFICATION

As a CJIS WAN interface agency official serving in the CJIS system, I hereby acknowledge the duties and responsibilities as set out in this agreement. I acknowledge that these duties and responsibilities have been developed and approved by CJIS system users in order to ensure the reliability, confidentiality, completeness, and accuracy of all information contained in or obtained by means of the CJIS system. I further acknowledge that a failure to comply with these duties and responsibilities may subject our agency to various sanctions adopted by the CJIS Advisory Policy Board and approved by the Director of the FBI. These sanctions may include the termination of CJIS service.

As the designated CJIS WAN interface agency official serving in the CJIS system, I hereby certify that I am familiar with the contents of the *Title 28, Code of Federal Regulations, Part 20; CJIS Security Policy; Computer Incident Response Capability*; and applicable federal or state laws and regulations applied to IAFIS and CJIS WAN Programs for the dissemination of criminal history records for criminal and noncriminal justice purposes.

*

Signature

Print or Type

CJIS WAN Agency Official

Date

CONCURRENCE OF FEDERAL/REGULATORY AGENCY HEAD OR STATE CJIS SYSTEMS OFFICER (CSO):

*

Signature

Print or Type

*

Title

Date

State CSO

FBI CJIS DIVISION:

Signature – [Name]

Assistant Director _____

Title

Date

* If there is a change in the CJIS WAN interface agency official, the FBI Designated Federal Employee must be notified in writing 30 days prior to the change.

5/27/2004 UA modification reflects change in CTO title to CSO.

APPENDIX E SECURITY FORUMS AND ORGANIZATIONAL ENTITIES

Online Security Forums / Organizational Entities
AntiOnline
Black Hat
CIO.com
CSO Online
CyberSpeak Podcast
FBI Criminal Justice Information Services Division (CJIS)
Forrester Security Forum
Forum of Incident Response and Security Teams (FIRST)
Information Security Forum (ISF)
Information Systems Audit and Control Association (ISACA)
Information Systems Security Association (ISSA)
Infosyssec
International Organization for Standardization (ISO)
International Information Systems Security Certification Consortium, Inc. (ISC) ²
Metasploit
Microsoft Developer Network (MSDN) Information Security
National Institute of Standards and Technology (NIST)
Open Web Application Security Project (OWASP)
SANS (SysAdmin, Audit, Network, Security) Institute
SC Magazine
Schneier.com
Security Focus
The Register
US Computer Emergency Response Team (CERT)
US DoJ Computer Crime and Intellectual Property Section (CCIPS)

APPENDIX F SAMPLE FORMS

This appendix contains sample forms.

F.1 Security Incident Response Form

**FBI CJIS DIVISION
INFORMATION SECURITY OFFICER (ISO)
SECURITY INCIDENT REPORTING FORM**

NAME OF PERSON REPORTING THE INCIDENT: _____

DATE OF REPORT: _____ (mm/dd/yyyy)

DATE OF INCIDENT: _____ (mm/dd/yyyy)

POINT(S) OF CONTACT (Include Phone/Extension/Email): _____

LOCATION(S) OF INCIDENT: _____

INCIDENT DESCRIPTION: _____

SYSTEM(S) AFFECTED: _____

SYSTEM(S) AFFECTED (e.g. CAD, RMS, file server, etc.): _____

METHOD OF DETECTION: _____

ACTIONS TAKEN/RESOLUTION: _____

Copies To:

John C. Weatherly

(FBI CJIS Division ISO)

1000 Custer Hollow Road

Clarksburg, WV 26306-0102

(304) 625-3660

iso@fbi.gov

APPENDIX G BEST PRACTICES

G.1 Virtualization

Virtualization

This appendix documents security considerations for implementing and operating virtual environments that process, store, and/or transmit Criminal Justice Information.

The FBI CJIS ISO has fielded several inquiries from various states requesting guidance on implementing virtual environments within their data centers. With the proliferation of virtual environments across industry in general there is a realistic expectation that FBI CJIS Auditors will encounter virtual environments during the upcoming year. Criminal Justice Agencies (CJAs) and Noncriminal Justice Agencies (NCJAs) alike need to understand and appreciate the foundation of security protection measures required for virtual environments.

From Microsoft's Introduction to Windows Server 2008

<http://www.microsoft.com/windowsserver2008/en/us/hyperv.aspx>:

"Server virtualization, also known as hardware virtualization, is a hot topic in the IT world because of the potential for serious economic benefits. Server virtualization enables multiple operating systems to run on a single physical machine as virtual machines (VMs). With server virtualization, you can consolidate workloads across multiple underutilized server machines onto a smaller number of machines. Fewer physical machines can lead to reduced costs through lower hardware, energy, and management overhead, plus the creation of a more dynamic IT infrastructure."

From a trade publication, kernelthread.com

<http://www.kernelthread.com/publications/virtualization/>:

"Virtualization is a framework or methodology of dividing the resources of a computer into multiple execution environments, by applying one or more concepts or technologies such as hardware and software partitioning, time-sharing, partial or complete machine simulation, emulation, quality of service, and many others."

From an Open Source Software developer

<http://www.kallasoft.com/pc-hardware-virtualization-basics/>:

"Virtualization refers to virtualizing hardware in software, allowing multiple operating systems, or images, to run concurrently on the same hardware. There are two main types of virtualization software:

- *"Type-1 Hypervisor, which runs 'bare-metal' (on top of the hardware)*
- *"Type-2 Hypervisor which requires a separate application to run within an operating system*

“Type1 hypervisors usually offer the best in efficiency, while Type-2 hypervisors allow for greater support of hardware that can be provided by the operating system. For the developer, power user, and small business IT professionals, virtualization offers the same basic idea of collapsing multiple physical boxes into one. For instance, a small business can run a web server and an Exchange server without the need for two boxes. Developers and power users can use the ability to contain different development environments without the need to modify their main operating system. Big businesses can also benefit from virtualization by allowing software maintenance to be run and tested on a separate image on hardware without having to take down the main production system.”

Industry leaders and niche developers are bringing more products to market every day. The following article excerpts, all posted during September 2008, on www.virtualization.com are examples of industry offerings.

“Microsoft and Novell partnered together for joint virtualization solution. Microsoft and Novell are announcing the availability of a joint virtualization solution optimized for customers running mixed-source environments. The joint offering includes SUSE Linux Enterprise Server configured and tested as an optimized guest operating system running on Windows Server 2008 Hyper-V, and is fully supported by both companies’ channel partners. The offering provides customers with the first complete, fully supported and optimized virtualization solution to span Windows and Linux environments.”

“Sun Microsystems today announced the availability of Sun xVM Server software and Sun xVM Ops Center 2.0, key components in its strategy. Sun also announced the addition of comprehensive services and support for Sun xVM Server software and xVM Ops Center 2.0 to its virtualization suite of services. Additionally, Sun launched xVMserver.org, a new open source community, where developers can download the first source code bundle for Sun xVM Server software and contribute to the direction and development of the product.”

“NetEx, specialist in high-speed data transport over TCP, today announced Virtual HyperIP bandwidth optimization solutions for VMware environments that deliver a threefold to tenfold increase in data replication performance. Virtual HyperIP is a software-based Data Transport Optimizer that operates on the VMware ESX server and boosts the performance of storage replication applications from vendors such as EMC, NetApp, Symantec, IBM, Data Domain, and FalconStor. Virtual HyperIP mitigates TCP performance issues that are common when moving data over wide-area network (WAN) connections because of bandwidth restrictions, latency due to distance and/or router hop counts, packet loss and network errors. Like the company’s award-winning appliance-based HyperIP, Virtual HyperIP eliminates these issues with an innovative software design developed specifically to accelerate traffic over an IP based network.”

From several sources, particularly:

<http://www.windowsecurity.com/articles/security-virtualization.html>

<http://csrc.nist.gov/publications/drafts/6--64rev2/draft-sp800-64-Revision2.pdf>

Virtualization provides several benefits:

- Make better use of under-utilized servers by consolidating to fewer machines saving on hardware, environmental costs, management, and administration of the server infrastructure.
- Legacy applications unable to run on newer hardware and/or operating systems can be loaded into a virtual environment – replicating the legacy environment.
- Provides for isolated portions of a server where trusted and untrusted applications can be ran simultaneously – enabling hot standbys for failover.
- Enables existing operating systems to run on shared memory multiprocessors.
- System migration, backup, and recovery are easier and more manageable.

Virtualization also introduces several vulnerabilities:

- Host Dependent.
- If the host machine has a problem then all the VMs could potentially terminate.
- Compromise of the host makes it possible to take down the client servers hosted on the primary host machine.
- If the virtual network is compromised then the client is also compromised.
- Client share and host share can be exploited on both instances. Potentially this can lead to files being copied to the share that fill up the drive.

These vulnerabilities can be mitigated by the following factors:

- Apply “least privilege” technique to reduce the attack surface area of the virtual environment and access to the physical environment.
- Configuration and patch management of the virtual machine and host, i.e. Keep operating systems and application patches up to date on both virtual machines and hosts.
- Install the minimum applications needed on host machines.
- Practice isolation from host and virtual machine.
- Install and keep updated antivirus on virtual machines and the host.
- Segregation of administrative duties for host and versions.
- Audit logging as well as exporting and storing the logs outside the virtual environment.
- Encrypting network traffic between the virtual machine and host IDS and IPS monitoring.
- Firewall each virtual machine from each other and ensure that only allowed protocols will transact.

G.2 Voice over Internet Protocol

Voice over Internet Protocol (VoIP)

Attribution:

The following information has been extracted from NIST Special Publication 800-58, Security Considerations for Voice over IP Systems.

Definitions:

Voice over Internet Protocol (VoIP) – A set of software, hardware, and standards designed to make it possible to transmit voice over packet switched networks, either an internal Local Area Network, or across the Internet.

Internet Protocol (IP) - A protocol used for communicating data across a packet-switched internetwork using the Internet Protocol Suite, also referred to as TCP/IP. IP is the primary protocol in the Internet Layer of the Internet Protocol Suite and has the task of delivering distinguished protocol datagrams (packets) from the source host to the destination host solely based on their addresses.

Summary:

Voice over Internet Protocol (VoIP) has been embraced by organizations globally as an addition to, or replacement for, public switched telephone network (PSTN) and private branch exchange (PBX) telephone systems. The immediate benefits are alluring since the typical cost to operate VoIP is less than traditional telephone services and VoIP can be installed in-line with an organization's existing Internet Protocol services. Unfortunately, installing a VoIP network is not a simple "plug-and-play" procedure. There are myriad security concerns, cost issues with new networking hardware requirements, and overarching quality of service (QoS) factors that have to be considered carefully.

What are some of the advantages of VoIP?

- a. Cost – a VoIP system is usually cheaper to operate than an equivalent office telephone system with a Private Branch Exchange and conventional telephone service.
- b. Integration with other services – innovative services are emerging that allow customers to combine web access with telephone features through a single PC or terminal. For example, a sales representative could discuss products with a customer using the company's web site. In addition, the VoIP system may be integrated with video across the Internet, providing a teleconferencing facility.

What are some of the disadvantages of VoIP?

- a. Startup cost – although VoIP can be expected to save money in the long run, the initial installation can be complex and expensive. In addition, a single standard has not yet emerged for many aspects of VoIP, so an organization must plan to support more than one standard, or expect to make relatively frequent changes as the VoIP field develops.
- b. Security – the flexibility of VoIP comes at a price: added complexity in securing voice and data. Because VoIP systems are connected to the data network, and share many of the same hardware and software components, there are more ways for intruders to attack a VoIP system than a conventional voice telephone system or PBX.

VoIP Risks, Threats, and Vulnerabilities

This section details some of the potential threats and vulnerabilities in a VoIP environment, including vulnerabilities of both VoIP phones and switches. Threat discussion is included because the varieties of threats faced by an organization determine the priorities in securing its communications equipment. Not all threats are present in all organizations. A commercial firm may be concerned primarily with toll fraud, while a government agency may need to prevent disclosure of sensitive information because of privacy or national security concerns. Information security risks can be broadly categorized into the following three types: confidentiality, integrity, and availability, (which can be remembered with the mnemonic “CIA”). Additional risks relevant to switches are fraud and risk of physical damage to the switch, physical network, or telephone extensions.

Packet networks depend for their successful operation on a large number of configurable parameters: IP and MAC (physical) addresses of voice terminals, addresses of routers and firewalls, and VoIP specific software such as Call Managers and other programs used to place and route calls. Many of these network parameters are established dynamically every time a network component is restarted, or when a VoIP telephone is restarted or added to the network. Because there are so many places in a network with dynamically configurable parameters, intruders have a wide array of potentially vulnerable points to attack.

Vulnerabilities described in this section are generic and may not apply to all systems, but investigations by NIST and other organizations have found these vulnerabilities in a number of VoIP systems. In addition, this list is not exhaustive; systems may have security weaknesses that are not included in the list. For each potential vulnerability, a recommendation is included to eliminate or reduce the risk of compromise.

Confidentiality and Privacy

Confidentiality refers to the need to keep information secure and private. For home computer users, this category includes confidential memoranda, financial information, and security information such as passwords. In a telecommunications switch, eavesdropping on conversations is an obvious concern, but the confidentiality of other information on the switch must be protected to defend against toll fraud, voice and data interception, and denial of service attacks. Network IP addresses, operating system type, telephone extension to IP address mappings, and communication protocols are all examples of information that, while not critical as individual pieces of data, can make an attacker’s job easier.

With conventional telephones, eavesdropping usually requires either physical access to tap a line, or penetration of a switch. Attempting physical access increases the intruder's risk of being discovered, and conventional PBXs have fewer points of access than VoIP systems. With VoIP, opportunities for eavesdroppers increase dramatically, because of the many nodes in a packet network.

Switch Default Password Vulnerability

It is common for switches to have a default login/password set, e.g., admin/admin, or root/root. This vulnerability also allows for wiretapping conversations on the network with port mirroring or bridging. An attacker with access to the switch administrative interface can mirror all packets on one port to another, allowing the indirect and unnoticeable interception of all communications. Failing to change default passwords is one of the most common errors made by inexperienced users.

REMEDIATION: If possible, remote access to the graphical user interface should be disabled to prevent the interception of plaintext administration sessions. Some devices provide the option of a direct USB connection in addition to remote access through a web browser interface. Disabling port mirroring on the switch should also be considered.

Classical Wiretap Vulnerability

Attaching a packet capture tool or protocol analyzer to the VoIP network segment makes it easy to intercept voice traffic.

REMEDIATION: A good physical security policy for the deployment environment is a general first step to maintaining confidentiality. Disabling the hubs on IP Phones as well as developing an alarm system for notifying the administrator when an IP Phone has been disconnected will allow for the possible detection of this kind of attack.

ARP Cache Poisoning and ARP Floods

Because many systems have little authentication, an intruder may be able to log onto a computer on the VoIP network segment, and then send ARP commands corrupting ARP caches on sender(s) of desired traffic, then activate IP. An ARP flood attack on the switch could render the network vulnerable to conversation eavesdropping. Broadcasting ARP replies blind is sufficient to corrupt many ARP caches. Corrupting the ARP cache makes it possible to re-route traffic to intercept voice and data traffic.

REMEDIATION: Use authentication mechanisms wherever possible and limit physical access to the VoIP network segment.

Web Server interfaces

Both VoIP switches and voice terminals are likely to have a web server interface for remote or local administration. An attacker may be able to sniff plaintext HTTP packets to gain confidential information. This would require access to the local network on which the server resides.

REMEDIATION: If possible, do not use an HTTP server. If it is necessary to use a web server for remote administration, use the more secure HTTPS (HTTP over SSL or TLS) protocol.

IP Phone Netmask Vulnerability

A similar effect of the ARP Cache Vulnerability can be achieved by assigning a subnet mask and router address to the phone crafted to cause most or all of the packets it transmits to be sent to an attacker's MAC address. Again, standard IP forwarding makes the intrusion all but undetectable.

REMEDIATION: A firewall filtering mechanism can reduce the probability of this attack. Remote access to IP phones is a severe risk.

Extension to IP Address Mapping Vulnerability

Discovering the IP address corresponding to any extension requires only calling that extension and getting an answer. A protocol analyzer or packet capture tool attached to the hub on the dialing instrument will see packets directly from the target instrument once the call is answered. Knowing the IP address of a particular extension is not a compromise in itself, but makes it easier to accomplish other attacks. For example, if the attacker is able to sniff packets on the local network used by the switch, it will be easy to pick out packets sent and received by a target phone. Without knowledge of the IP address of the target phone, the attacker's job may be much more difficult to accomplish and require much longer, possibly resulting in the attack being discovered.

REMEDIATION: Disabling the hub on the IP Phone will prevent this kind of attack. However, it is a rather simple task to turn the hub back on.

Integrity Issues

Integrity of information means that information remains unaltered by unauthorized users. For example, most users want to ensure that bank account numbers cannot be changed by anyone else, or that passwords are changed only by the user or an authorized security administrator. Telecommunication switches must protect the integrity of their system data and configuration. Because of the richness of feature sets available on switches, an attacker who can compromise the system configuration can accomplish nearly any other goal. For example, an ordinary extension could be re-assigned into a pool of phones that supervisors can listen in on or record conversations for quality control purposes. Damaging or deleting information about the IP network used by a VoIP switch results in an immediate denial of service.

The security system itself provides the capabilities for system abuse and misuse. That is, compromise of the security system not only allows system abuse but also allows the elimination of all traceability and the insertion of trapdoors for intruders to use on their next visit. For this reason, the security system must be carefully protected. Integrity threats include any in which system functions or data may be corrupted, either accidentally or as a result of malicious actions. Misuse may involve legitimate users (i.e. insiders performing unauthorized operations) or intruders.

A legitimate user may perform an incorrect, or unauthorized, operations function (e.g., by mistake or out of malice) and may cause deleterious modification, destruction, deletion, or disclosure of switch software and data. This threat may be caused by several factors including the possibility that the level of access permission granted to the user is higher than what the user needs to remain functional.

Intrusion - An intruder may masquerade as a legitimate user and access an operations port of the switch. There are a number of serious intrusion threats. For example, the intruder may use the permission level of the legitimate user and perform damaging operations functions such as:

- Disclosing confidential data
- Causing service deterioration by modifying the switch software
- Crashing the switch
- Removing all traces of the intrusion (e.g., modifying the security log) so that it may not be readily detected

Insecure state - At certain times the switch may be vulnerable due to the fact that it is not in a secure state. For example:

- After a system restart, the old security features may have been reset to insecure settings, and new features may not yet be activated. (For example, all old passwords may have reverted to the default system-password, even though new passwords are not yet assigned.) The same may happen at the time of a disaster recovery.
- At the time of installation the switch may be vulnerable until the default security features have been replaced.

DHCP Server Insertion Attack

It is often possible to change the configuration of a target phone by exploiting the DHCP response race when the IP phone boots. As soon as the IP phone requests a DHCP response, a rogue DHCP server can initiate a response with data fields containing false information.

This attack allows for possible man in the middle attacks on the IP-media gateway, and IP Phones. Many methods exist with the potential to reboot the phone remotely, e.g. “social engineering”, ping flood, MAC spoofing (probably SNMP hooks, etc.).

REMEDIATION: If possible, use static IP addresses for the IP Phones. This will remove the necessity of using a DHCP server. Further, using a state based intrusion detection system can filter out DHCP server packets from IP Phone ports, allowing this traffic only from the legitimate server.

TFTP Server Insertion Attack

It is possible to change the configuration of a target phone by exploiting the TFTP response race when the IP phone is resetting. A rogue TFTP server can supply spurious

information before the legitimate server is able to respond to a request. This attack allows an attacker to change the configuration of an IP Phone.

REMEDIATION: Using a state based intrusion detection system can filter out DHCP server packets from IP Phone ports, allowing such traffic only from the legitimate server. Organizations looking to deploy VoIP systems should look for IP Phone instruments that can download signed binary files.

Availability and Denial of Service

Availability refers to the notion that information and services be available for use when needed. Availability is the most obvious risk for a switch. Attacks exploiting vulnerabilities in the switch software or protocols may lead to deterioration or even denial of service or functionality of the switch. For example: if unauthorized access can be established to any branch of the communication channel (such as a CCS link or a TCP/IP link), it may be possible to flood the link with bogus messages causing severe deterioration (possibly denial) of service. A voice over IP system may have additional vulnerabilities with Internet connections. Because intrusion detection systems fail to intercept a significant percentage of Internet based attacks, attackers may be able to bring down VoIP systems by exploiting weaknesses in Internet protocols and services.

Any network may be vulnerable to denial of service attacks, simply by overloading the capacity of the system. With VoIP the problem may be especially severe, because of its sensitivity to packet loss or delay.

CPU Resource Consumption Attack without any account information.

An attacker with remote terminal access to the server may be able to force a system restart (shutdown all/restart all) by providing the maximum number of characters for the login and password buffers multiple times in succession. Additionally, IP Phones may reboot as a result of this attack.

In addition to producing a system outage, the restart may not restore uncommitted changes or, in some cases, may restore default passwords, which would introduce intrusion vulnerabilities.

REMEDIATION: The deployment of a firewall disallowing connections from unnecessary or unknown network entities is the first step to overcoming this problem. However, there is still the opportunity for an attacker to spoof his MAC and IP address, circumventing the firewall protection.

Default Password Vulnerability

It is common for switches to have a default login/password set, e.g., admin/admin, or root /root. Similarly, VoIP telephones often have default keypad sequences that can be used to unlock and modify network information.

This vulnerability would allow an attacker to control the topology of the network remotely, allowing for not only complete denial of service to the network, but also a port mirroring attack to the attacker's location, giving the ability to intercept any other conversations taking place over the same switch. Further, the switch may have a web server interface, providing an attacker with the ability to disrupt the network without advance knowledge of switch operations and commands. In most systems, telephones download their configuration data on startup using TFTP or similar protocols. The configuration specifies the IP addresses for Call Manager nodes, so an attacker could substitute another IP address pointing to a call manager that would allow eavesdropping or traffic analysis.

REMEDIATION: Changing the default password is crucial. Moreover, the graphical user interface should be disabled to prevent the interception of plaintext administration sessions.

Exploitable software flaws

Like other types of software, VoIP systems have been found to have vulnerabilities due to buffer overflows and improper packet header handling. These flaws typically occur because the software is not validating critical information properly. For example, a short integer may be used as a table index without checking whether the parameter passed to the function exceeds 32,767, resulting in invalid memory accesses or crashing of the system.

Exploitable software flaws typically result in two types of vulnerabilities: denial of service or revelation of critical system parameters. Denial of service can often be implemented remotely, by passing packets with specially constructed headers that cause the software to fail. In some cases the system can be crashed, producing a memory dump in which an intruder can find IP addresses of critical system nodes, passwords, or other security-relevant information. In addition, buffer overflows that allow the introduction of malicious code have been found in VoIP software, as in other applications.

REMEDIATION: These problems require action from the software vendor, and distribution of patches to administrators. Intruders monitor announcements of vulnerabilities, knowing that many organizations require days or weeks to update their software. Regular checking for software updates and patches is essential to reducing these vulnerabilities. Automated patch handling can assist in reducing the window of opportunity for intruders to exploit known software vulnerabilities.

Account Lockout Vulnerability

An attacker will be able to provide several incorrect login attempts at the telnet prompt until the account becomes locked out. (This problem is common to most password-protected systems, because it prevents attackers from repeating login attempts until the correct password is found by trying all possible combinations.)

The account is unable to connect to the machine for the set lockout time.

REMEDIATION: If remote access is not available, this problem can be solved with physical access control.

NIST Recommendations.

Because of the integration of voice and data in a single network, establishing a secure VoIP and data network is a complex process that requires greater effort than that required for data-only networks. In particular, start with these general guidelines, recognizing that practical considerations, such as cost or legal requirements, may require adjustments for the organization:

1. Develop appropriate network architecture.

- Separate voice and data on logically different networks if feasible. Different subnets with separate RFC 1918 address blocks should be used for voice and data traffic, with separate DHCP servers for each, to ease the incorporation of intrusion detection and VoIP firewall protection at the voice gateway, which interfaces with the PSTN, disallow H.323, SIP, or other VoIP protocols from the data network. Use strong authentication and access control on the voice gateway system, as with any other critical network component. Strong authentication of clients towards a gateway often presents difficulties, particularly in key management. Here, access control mechanisms and policy enforcement may help.
- A mechanism to allow VoIP traffic through firewalls is required. There are a variety of protocol dependent and independent solutions, including application level gateways (ALGs) for VoIP protocols, Session Border Controllers, or other standards-based solutions when they mature.
- Stateful packet filters can track the state of connections, denying packets that are not part of a properly originated call. (This may not be practical when multimedia protocol inherent security or lower layer security is applied, e.g., H.235 Annex D for integrity provision or TLS to protect SIP signaling).
- Use IPsec or Secure Shell (SSH) for all remote management and auditing access. If practical, avoid using remote management at all and do IP PBX access from a physically secure system.
- If performance is a problem, use encryption at the router or other gateway, not the individual endpoints, to provide for IPsec tunneling. Since some VoIP endpoints are not computationally powerful enough to perform encryption, placing this burden at a central point ensures all VoIP traffic emanating from the enterprise network has been encrypted. Newer IP phones are able to provide Advanced Encryption System (AES) encryption at reasonable cost. Note that Federal Information Processing Standard (FIPS) 140-2, Security Requirements for Cryptographic Modules, is applicable to all Federal agencies that use cryptographic-based security systems to protect sensitive information in computer

and telecommunication systems (including voice systems) as defined in Section 5131 of the Information Technology Management Reform Act of 1996, Public Law 104-106.

2. Ensure that the organization has examined and can acceptably manage and mitigate the risks to their information, system operations, and continuity of essential operations when deploying VoIP systems.

VoIP can provide more flexible service at lower cost, but there are significant tradeoffs that must be considered. VoIP systems can be expected to be more vulnerable than conventional telephone systems, in part because they are tied in to the data network, resulting in additional security weaknesses and avenues of attack (see VoIP Risks, Threats, and Vulnerabilities section for more detailed discussion of vulnerabilities of VoIP and their relation to data network vulnerabilities).

Confidentiality and privacy may be at greater risk in VoIP systems unless strong controls are implemented and maintained. An additional concern is the relative instability of VoIP technology compared with established telephony systems. Today, VoIP systems are still maturing and dominant standards have not emerged. This instability is compounded by VoIP's reliance on packet networks as a transport medium. The public switched telephone network is ultra-reliable. Internet service is generally much less reliable, and VoIP cannot function without Internet connections, except in the case of large corporate or other users who may operate a private network. Essential telephone services, unless carefully planned, deployed, and maintained, will be at greater risk if based on VoIP.

3. Special consideration should be given to E-911 emergency services communications, because E-911 automatic location service is not available with VoIP in some cases.

Unlike traditional telephone connections, which are tied to a physical location, VoIP's packet switched technology allows a particular number to be anywhere. This is convenient for users, because calls can be automatically forwarded to their locations. But the tradeoff is that this flexibility severely complicates the provision of E-911 service, which normally provides the caller's location to the 911 dispatch office. Although most VoIP vendors have workable solutions for E-911 service, government regulators and vendors are still working out standards and procedures for 911 services in a VoIP environment. Agencies must carefully evaluate E-911 issues in planning for VoIP deployment.

4. Agencies should be aware that physical controls are especially important in a VoIP environment and deploy them accordingly.

Unless the VoIP network is encrypted, anyone with physical access to the office LAN could potentially connect network monitoring tools and tap into telephone conversations. Although conventional telephone lines can also be monitored when physical access is obtained, in most offices there are many more points to connect with a LAN without arousing suspicion. Even if encryption is used, physical access to VoIP servers and gateways may allow an attacker to do traffic analysis (i.e., determine which parties are communicating). Agencies therefore should ensure that adequate physical security is in place to restrict access to VoIP network components. Physical security measures, including barriers, locks, access control systems, and guards, are the first line of defense. Agencies must make sure that the proper physical countermeasures are in place to mitigate some of

the biggest risks such as insertion of sniffers or other network monitoring devices. Otherwise, practically speaking this means that installation of a sniffer could result in not just data but all voice communications being intercepted.

5. VoIP-ready firewalls and other appropriate protection mechanisms should be employed. Agencies must enable, use, and routinely test the security features that are included in VoIP systems.

Because of the inherent vulnerabilities (e.g. susceptibility to packet sniffing) when operating telephony across a packet network, VoIP systems incorporate an array of security features and protocols. Organization security policy should ensure that these features are used. In particular, firewalls designed for VoIP protocols are an essential component of a secure VoIP system.

6. If practical, “softphone” systems, which implement VoIP using an ordinary PC with a headset and special software, should not be used where security or privacy are a concern.

Worms, viruses, and other malicious software are extraordinarily common on PCs connected to the internet, and very difficult to defend against. Well-known vulnerabilities in web browsers make it possible for attackers to download malicious software without a user’s knowledge, even if the user does nothing more than visit a compromised web site. Malicious software attached to email messages can also be installed without the user’s knowledge, in some cases even if the user does not open the attachment. These vulnerabilities result in unacceptably high risks in the use of “softphones”, for most applications. In addition, because PCs are necessarily on the data network, using a softphone system conflicts with the need to separate voice and data networks to the greatest extent practical.

7. If mobile units are to be integrated with the VoIP system, use products implementing WiFi Protected Access (WPA), rather than 802.11 Wired Equivalent Privacy (WEP).

The security features of 802.11 WEP provide little or no protection because WEP can be cracked with publicly available software. The more recent WiFi Protected Access (WPA), a snapshot of the ongoing 802.11i standard, offers significant improvements in security, and can aid the integration of wireless technology with VoIP. NIST strongly recommends that the WPA (or WEP if WPA is unavailable) security features be used as part of an overall defense-in-depth strategy. Despite their weaknesses, the 802.11 security mechanisms can provide a degree of protection against unauthorized disclosure, unauthorized network access, or other active probing attacks. However, the Federal Information Processing Standard (FIPS) 140-2, Security Requirements for Cryptographic Modules, is mandatory and binding for Federal agencies that have determined that certain information must be protected via cryptographic means. As currently defined, neither WEP nor WPA meets the FIPS 140-2 standard. In these cases, it will be necessary to employ higher level cryptographic protocols and applications such as secure shell (SSH), Transport Level Security (TLS) or Internet Protocol Security (IPsec) with FIPS 140-2 validated cryptographic modules and associated algorithms to protect information, regardless of whether the nonvalidated data link security protocols are used.

8. Carefully review statutory requirements regarding privacy and record retention with competent legal advisors.

Although legal issues regarding VoIP are beyond the scope of this document, readers should be aware that laws and rulings governing interception or monitoring of VoIP lines, and retention of call records, may be different from those for conventional telephone systems. Agencies should review these issues with their legal advisors. See Section 2.5 for more on these issues.

G.3 Cloud Computing

Cloud Computing

Purpose:

This paper is provided to define and describe cloud computing, discuss CJIS Security Policy (CSP) compliance, detail security and privacy, and provide general recommendations.

Attribution:

- NIST SP 800-144, Guidelines on Security and Privacy in Public Cloud Computing (Dec. 2011)
- NIST SP 800-145, the NIST Definition of Cloud Computing (Sept. 2011)
- NIST SP 800-146, Cloud Computing Synopsis and Recommendations (May 2011)
- CJIS Security Policy, Version 5.0

Definitions and Terms:

Cloud computing – A distributed computing model that permits on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services), software, and information.

Cloud subscriber – A person or organization that is a customer of a cloud

Cloud client – A machine or software application that accesses a cloud over a network connection, perhaps on behalf of a subscriber

Cloud provider – An organization that provides cloud services

Summary:

With many law enforcement agencies looking for ways to attain greater efficiency while grappling with reduced budgets, the idea of cloud computing to maintain data and applications is a viable business solution. But the unique security and legal characteristics of law enforcement agencies means any migration to cloud services may be challenging. Anytime the security of information and transactions must be maintained, as it must be with access to the FBI's CJIS systems and the protection of Criminal Justice Information (CJI), security and policy compliance concerns are bound to arise.

Cloud computing has become a popular and sometimes contentious topic of discussion for both the private and public sectors. This is in part because of the difficulty in describing cloud computing in general terms, because it is not a single kind of system. The “cloud” spans a spectrum of underlying technologies, configuration possibilities, service and deployment models. Cloud computing offers the ability to conveniently rent access to fully featured applications, software development and deployment environments, and computing infrastructure assets - such as network-accessible data storage and processing from a cloud service provider.

One of the benefits of cloud computing is the ability to outsource many of the technical functions agencies may not want to perform for various reasons. Ultimately, the move to cloud computing is a business and security risk decision in which the following relevant factors are given proper consideration:

- readiness of existing applications for cloud deployment
- transition costs
- life-cycle costs
- maturity of service orientation in existing infrastructure
- security and privacy requirements – federal, state, and local

Achieving CJIS Security Policy Compliance:

The question that is often asked is, “Can an Agency be compliant with the CJIS Security Policy and also cloud compute?”

Because the CJIS Security Policy is device and architecture independent (per CSP Section 2.2), the answer is yes, and this can be accomplished— assuming the vendor of the cloud technology is able to meet the existing requirements of the CJIS Security Policy.

There are security challenges that must be addressed if CJI is to be sent into or through, stored within, or accessed from the cloud.

Admittedly, the existing CJIS Security Policy requirements may be difficult for some cloud-computing vendors due to the sheer numbers and the geographic disbursement of their personnel; however, the requirements aren’t new to vendors serving the criminal justice community and many vendors have been successfully meeting the Policy requirements for years. Even so, they are the minimum security requirements which will provide an acceptable level of assurance that law enforcement and personally identifiable information (PII) will be protected when shared with other law enforcement agencies across the nation.

General CJIS Security Policy Applicability Questions

Before tackling these challenges, the cloud subscriber should first be aware of what security and legal requirements they are subject to prior to entering into any agreement with a cloud provider. Asking the following general questions will help frame the process of determining compliance with the existing requirements of the CJIS Security Policy.

- Will access to Criminal Justice Information (CJI) within a cloud environment fall within the category of remote access? (5.5.6 Remote Access)
- Will advanced authentication (AA) be required for access to CJI within a cloud environment? (5.6.2.2 Advanced Authentication, 5.6.2.2.1 Advanced Authentication Policy and Rationale)
- Does/do any cloud service provider's datacenter(s) used in the transmission or storage of CJI meet all the requirements of a physically secure location? (5.9.1 Physically Secure Location)
- Are the encryption requirements being met? (5.10.1.2 Encryption)
 - Who will be providing the encryption as required in the CJIS Security Policy (client or cloud service provider)? *Note: individuals with access to the keys can decrypt the stored files and therefore have access to unencrypted CJI.*
 - Is the data encrypted while at rest and in transit?
- What are the cloud service provider's incident response procedures? (5.3 Policy Area 3: Incident Response)
 - Will the cloud subscriber be notified of any incident?
 - If CJI is compromised, what are the notification and response procedures?
- Is the cloud service provider a private contractor/vendor?
 - If so, they are subject to the same screening and agreement requirements as any other private contractors hired to handle CJI? (5.1.1.5 Private Contractor User Agreements and CJIS Security Addendum; 5.12.1.2 Personnel Screening for Contractors and Vendors)
- Will the cloud service provider allow the CSA and FBI to conduct compliance and security audits? *Note: Cloud facilities such as datacenters in which CJI will be stored or processed should be audited as would any other datacenter housing and processing CJI.* (5.11.1 Audits by the FBI CJIS Division; 5.11.2 Audits by the CSA)

- How will event and content logging be handled? (5.4 Policy Area 4, Auditing and Accountability)
 - Will the cloud service provider handle the events and content logging required by the CJIS Security Policy and provide that upon request?
 - What are the cloud service provider's responsibilities with regard to media protection and destruction? (5.8 Policy Area 8: Media Protection)

Ultimately, the goal is to remain committed to using technology in its information sharing processes, but not at the sacrifice of the security of the information with which it has been entrusted. As stated in the CJIS Security Policy, device and architecture independence permits the use of cloud computing, but the security requirements do not change.

Cloud Utilization Scenarios

1. Encrypted CJI in a Cloud Environment–Key Management Control, Security Awareness Training, and Personnel Controls

Prior to permitting CJI to be stored or traverse through a cloud environment, the agency should ensure proper encryption key management control procedures are implemented to determine who has access and control over the encryption keys. Proper key management control is vital to CJI security as those individuals (agency or cloud employees) with access to the keys can decrypt the stored files, and therefore, have unescorted access to unencrypted CJI. This means all those individuals must be subjected to security awareness training (CJIS Security Policy section 5.2) and must meet personnel security (CJIS Security Policy Section 5.12) requirements as individuals with unescorted access to unencrypted CJI.

Note: As a best security practice, the CJIS ISO Program does not recommend allowing the cloud service provider access to the encryption keys used to protect CJI. However, it may not always be reasonable to expect the agency, criminal justice or noncriminal justice, to accomplish this task.

- a. Scenario 1–Agency Stores CJI in a Cloud:

A CJA stores encrypted CJI (Backup files and drives) in a cloud service provider's environment. To access CJI, the agency will extract the CJI from the cloud to its local machine, and then decrypt the CJI. The CJI is processed, re-encrypted, and then re-uploaded to the cloud environment for storage. In this scenario, the agency always encrypts the CJI prior to placing it in the cloud and only authorized users of the agency have access to the encryption keys. Since the agency maintains the encryption keys, the cloud service provider employees would not need to undergo fingerprint-based background checks, nor have security awareness training. These requirements are negated, because only authorized personnel with access to the keys have the ability to view this CJI in an unencrypted form.

- b. Scenario 2–Agency Accesses CJI While in a Cloud:

A CJA stores CJI (files and drives) in a cloud service provider's environment, but as part of daily operations authorized users will remotely access the encrypted CJI in the cloud. The user will decrypt the CJI while it is in the cloud's virtual environment, process the data, and then re-encrypt the data prior to ending the remote session. The agency maintains the keys and the cloud service provider does not have access to the encryption keys. However, since the CJI is decrypted within the cloud's virtual environment, any administrative personnel employed by the cloud provider having the ability to access the virtual environment must be identified and subjected to security awareness training and personnel security controls as described in the CJIS Security Policy.

c. Scenario 3—CJI Impact from a Cloud Datacenter Critical Systems Crash—Core Dump² Recovery:

A CJA utilizes a cloud service provider (IaaS or PaaS) to store CJI and remotely accesses the environment to process CJI. During normal operation, the cloud provider experiences systems outages within the datacenter in which CJI is processed and stored. The cloud provider's administrators need to repair the systems and restore service using data from a core dump to return to normal operations. The cloud service provider as part of the Service Level Agreement (SLA) with the CJA has been authorized to maintain the encryption keys in order respond to such an event. The cloud administrators with such access have underwent fingerprint-based background checks and security awareness training. This allows the cloud administrators to decrypt CJI so that it is written to the core dump files for restoration following the system outage. CJI, however, is encrypted at all times except when part of the core dump files. As part of the SLA, the cloud service provider has agreed to treat the core dump files as CJI to ensure all protection are in place in compliance with the CJIS Security Policy.

Note: Writing encrypted data to a core dump corrupts the data and makes it unusable because the key no longer decrypts the data. This is problematic when attempting to recover encrypted data written to a core dump. The CJA could have ensured the cloud provider exclude encrypted data (CJI) from the core dump, but chose against it.

The Cloud Model Explained:

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

² Core Dump - A file of a computer's documented memory of when a program or computer crashed. The file consists of the recorded status of the working memory at an explicit time, usually close to when the system crashed or when the program ended atypically as it presents the risk that the system failure would ensure the loss of the encrypted data.

The cloud model as defined by NIST consists of five essential characteristics, offers the option of three service models, and may be deployed via any of four deployment models as shown in Figure 1 below:

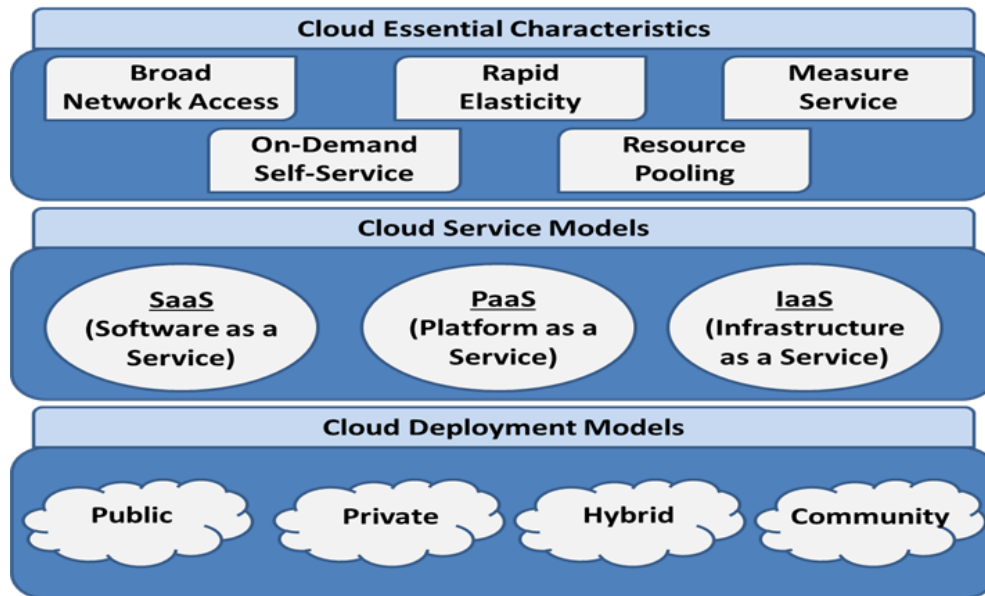


Figure 1 - Visual Depiction of the NIST Cloud Computing Definition

Essential Characteristics:

On-demand self-service

A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

Broad network access

Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).

Resource pooling

The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in which the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction

(e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth.

Rapid elasticity

Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.

Measured service

Cloud systems automatically control and optimize resource use by leveraging a metering capability* at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

** Typically this is done on a pay-per-use or charge-per-use basis.*

Deployment Models:

Private cloud

The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

Community cloud

The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.

Public cloud

The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.

Hybrid cloud

The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

Service Models:

Software as a Service (SaaS)

This model provides the consumer the capability to use the provider's applications running on a cloud infrastructure*.

** A cloud infrastructure is the collection of hardware and software that enables the five essential characteristics of cloud computing. The cloud infrastructure can be viewed as containing both a physical layer and an abstraction layer. The physical layer consists of the hardware resources that are necessary to support the cloud services being provided, and typically includes server, storage and network components. The abstraction layer consists of the software deployed across the physical layer, which manifests the essential cloud characteristics. Conceptually the abstraction layer sits above the physical layer.*

The SaaS service model is often referred to as “Software deployed as a hosted service and accessed over the Internet.”

The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface.

When using the SaaS service model it should be understood that the consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

Platform as a Service (PaaS)

This model provides the consumer the capability to deploy consumer-created or acquired applications* created using programming languages, libraries, services, and tools supported by the provider onto the cloud infrastructure.

** This capability does not necessarily preclude the use of compatible programming languages, libraries, services, and tools from other sources.*

When using the PaaS service model the consumer may have control over the deployed applications and possibly configuration settings for the application-hosting environment, but does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage.

Infrastructure as a Service (IaaS)

This model provides the consumer the capability to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, including operating systems and applications.

When using the IaaS service model the consumer may have control over operating systems, storage, and deployed applications; and possibly limited control of select

networking components (e.g., host firewalls), but does not manage or control the underlying cloud infrastructure.

Key Security and Privacy Issues:

Although the emergence of cloud computing is a recent development, insights into critical aspects of security can be gleaned from reported experiences of early adopters and also from researchers analyzing and experimenting with available cloud provider platforms and associated technologies. The sections below highlight privacy and security-related issues that are believed to have long-term significance for public cloud computing and, in many cases, for other cloud computing service models.

Because cloud computing has grown out of an amalgamation of technologies, including service oriented architecture, virtualization, Web 2.0, and utility computing, many of the privacy and security issues involved can be viewed as known problems cast in a new setting. The importance of their combined effect in this setting, however, should not be discounted. Public cloud computing does represent a thought-provoking paradigm shift from conventional norms to an open organizational infrastructure—*at the extreme, displacing applications from one organization's infrastructure to the infrastructure of another organization, where the applications of potential adversaries may also operate.*

Governance

Governance implies control and oversight by the organization over policies, procedures, and standards for application development and information technology service acquisition, as well as the design, implementation, testing, use, and monitoring of deployed or engaged services. With the wide availability of cloud computing services, lack of organizational controls over employees engaging such services arbitrarily can be a source of problems. While cloud computing simplifies platform acquisition, it doesn't alleviate the need for governance; instead, it has the opposite effect, amplifying that need.

Dealing with cloud services requires attention to the roles and responsibilities involved between the organization and cloud provider, particularly with respect to managing risks and ensuring organizational requirements are met. Ensuring systems are secure and risk is managed is challenging in any environment and even more daunting with cloud computing. Audit mechanisms and tools should be in place to determine how data is stored, protected, and used, to validate services, and to verify policy enforcement. A risk management program should also be in place that is flexible enough to deal with the continuously evolving and shifting risk landscape.

Compliance

Compliance refers to an organization's responsibility to operate in agreement with established laws, regulations, standards, and specifications. Various types of security and privacy laws and regulations exist within different countries at the national, state, and local levels, making compliance a potentially complicated issue for cloud computing.

Law and Regulations

Cloud providers are becoming more sensitive to legal and regulatory concerns, and may be willing to commit to store and process data in specific jurisdictions and apply required safeguards for security and privacy. However, the degree to which they will accept liability in their service agreements, for exposure of content under their control, remains to be seen. Even so, organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf.

Data Location

One of the most common compliance issues facing an organization is data location. A characteristic of many cloud computing services is that data is stored redundantly in multiple physical locations and detailed information about the location of an organization's data is unavailable or not disclosed to the service consumer. This situation makes it difficult to ascertain whether sufficient safeguards are in place and whether legal and regulatory compliance requirements are being met. External audits and security certifications can alleviate this issue to some extent, but they are not a panacea.

When information crosses borders, the governing legal, privacy, and regulatory regimes can be ambiguous and raise a variety of concerns. Consequently, constraints on the trans-border flow of sensitive data, as well as the requirements on the protection afforded the data, have become the subject of national and regional privacy and security laws and regulations.

Electronic Discovery

The capabilities and processes of a cloud provider, such as the form in which data is maintained and the electronic discovery-related tools available, affect the ability of the organization to meet its obligations in a cost effective, timely, and compliant manner. A cloud provider's archival capabilities may not preserve the original metadata as expected, causing spoliation (i.e., the intentional, reckless, or negligent destruction, loss, material alteration, or obstruction of evidence that is relevant to litigation), which could negatively impact litigation.

Trust

Under the cloud computing paradigm, an organization relinquishes direct control over many aspects of security and privacy, and in doing so, confers a high level of trust onto the cloud provider. At the same time, federal agencies have a responsibility to protect information and information systems commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction, regardless of whether the information is collected or maintained by or on behalf of the agency; or whether the information systems are used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency

Insider Access

Data processed or stored outside the physical confines of an organization, its firewall, and other security controls bring with it an inherent level of risk. The insider security threat is a well-known issue for most organizations. Incidents may involve various types of fraud, sabotage of information resources, and theft of sensitive information.

Data Ownership

The organization's ownership rights over the data must be firmly established in the service contract to enable a basis for trust and privacy of data. The continuing controversy over privacy and data ownership rights for social networking users illustrates the impact that ambiguous terms can have on the parties involved.

Ideally, the contract should state clearly that the organization retains exclusive ownership over all its data; that the cloud provider acquires no rights or licenses through the agreement, including intellectual property rights or licenses, to use the organization's data for its own purposes; and that the cloud provider does not acquire and may not claim any interest in the data due to security. For these provisions to work as intended, the terms of data ownership must not be subject to unilateral amendment by the cloud provider.

Visibility

Continuous monitoring of information security requires maintaining ongoing awareness of security controls, vulnerabilities, and threats to support risk management decisions. Transition to public cloud services entails a transfer of responsibility to the cloud provider for securing portions of the system on which the organization's data and applications operate.

Ancillary Data

While the focus of attention in cloud computing is mainly on protecting application data, cloud providers also hold significant details about the accounts of cloud consumers that could be compromised and used in subsequent attacks.

Risk Management

Assessing and managing risk in systems that use cloud services can be a challenge. With cloud-based services, some subsystems or subsystem components fall outside of the direct control of a client organization. Many organizations are more comfortable with risk when they have greater control over the processes and equipment involved. Establishing a level of trust about a cloud service is dependent on the degree of control an organization is able to exert on the provider to provision the security controls necessary to protect the organization's data and applications, and also the evidence provided about the effectiveness of those controls. Ultimately, if the level of trust in the service falls below expectations and the organization is unable to employ compensating controls, it must either reject the service or accept a greater degree of risk.

Architecture

The architecture of the software and hardware used to deliver cloud services can vary significantly among public cloud providers for any specific service model. It is important to understand the technologies the cloud provider uses to provision services and the implications the technical controls involved have on security and privacy of the system throughout its lifecycle. With such information, the underlying system architecture of a cloud can be decomposed and mapped to a framework of security and privacy controls that can be used to assess and manage risk.

Identity and Access Management

Data sensitivity and privacy of information have become increasingly an area of concern for organizations. The identity proofing and authentication aspects of identity management entail the use, maintenance, and protection of PII collected from users. Preventing unauthorized access to information resources in the cloud is also a major consideration. One recurring issue is that the organizational identification and authentication framework may not naturally extend into a public cloud and extending or changing the existing framework to support cloud services may prove difficult.

Software Isolation

High degrees of multi-tenancy over large numbers of platforms are needed for cloud computing to achieve the envisioned flexibility of on-demand provisioning of reliable services and the cost

benefits and efficiencies due to economies of scale. Regardless of the service model and multi-tenant software architecture used, the computations of different consumers must be able to be carried out in isolation from one another, mainly through the use of logical separation mechanisms.

Data Protection

Data stored in a public cloud typically resides in a shared environment collocated with data from other customers. Organizations placing sensitive and regulated data into a public cloud, therefore, must account for the means by which access to the data is controlled and the data is kept secure. Similar concerns exist for data migrated within or between clouds.

Value Concentration

Having data collocated with that of an organization with a high threat profile could also lead to a denial of service, as an unintended casualty from an attack targeted against that organization. Similarly, side effects from a physical attack against a high profile organization's cloud-based resources are also a possibility. For example, over the years, facilities of the Internal Revenue Service have attracted their share of attention from would-be attackers.

Data Isolation

Database environments used in cloud computing can vary significantly. Accordingly, various types of multi-tenant arrangements exist for databases. Each arrangement pools resources differently, offering different degrees of isolation and resource efficiency. Regardless of implementation decision, data must be secured while at rest, in transit, and in use, and access to the data must be controlled.

Data Sanitization

The data sanitization practices that a cloud provider implements have obvious implications for security. Sanitization involves the expunging of data from storage media by overwriting, degaussing, or other means, or the destruction of the media itself, to prevent unauthorized disclosure of information. Data sanitization also applies to backup copies made for recovery and restoration of service and residual data remaining upon termination of service.

In a public cloud computing environment, data from one consumer is physically collocated (e.g., in an IaaS data store) or commingled (e.g., in a SaaS database) with the data of other consumers, which can complicate matters. Service agreements should stipulate sufficient measures that are taken to ensure data sanitization is performed appropriately throughout the system lifecycle.

Encryption

Client end-to-end encryption (e.g. encryption/decryption occurs on the law enforcement controlled client prior to data entering the cloud and decryption occurs only on the client device after encrypted data is removed from the cloud service) with cryptographic keys managed solely by law enforcement would prevent exposure of sensitive data.

- May cause significant cloud service functionality limitations on available service types made available for sensitive data. This may also increase expenses to cover key items, such as key management and client software. Additionally, a number of specific SLA or contract clauses may be necessary for the implementation of client end-to end encryption.

Use of cloud services without end-to-end encryption implemented by the client is another option that would require cloud service provider participation in the encryption of data.

- This would require at least some cloud provider personnel to undergo personnel background screening and training.
- Specialized Service Level Agreements (SLA) and/or contractual clauses would be necessary to identify those personnel that may have access to unencrypted, sensitive data.
- Conducting the analysis and gaining approval of particular cloud service implementations not utilizing end-to-end encryption for sensitive law enforcement data may be costly and time consuming due to the high degree of technical complexity.

Availability

In simple terms, availability is the extent to which an organization's full set of computational resources is accessible and usable. Denial of service attacks, equipment outages, and natural disasters are all threats to availability. The concern is that most downtime is unplanned and can impact the mission of the organization. Some examples of unplanned service interruptions that cause concerns are:

- Temporary Outages
- Prolonged and Permanent Outages
- Denial of Service

Incident Response

The complexity of a cloud service can obscure recognition and analysis of incidents. Revising an organization's incident response plan to address differences between the organizational computing environment and a cloud computing environment is an important, but easy-to-overlook prerequisite to transitioning applications and data.

Data Availability

The availability of relevant data from event monitoring is essential for timely detection of security incidents. Cloud consumers are often confronted with extremely limited capabilities for detection of incidents in public cloud environments. The situation varies among cloud service models and cloud providers. For example, PaaS providers typically do not make event logs available to consumers, who are then left mainly with event data from self-deployed applications (e.g., via application logging). Similarly, SaaS consumers are completely dependent upon the cloud provider to provide event data such as activity logging, while IaaS consumers control more of the information stack and have access to associated event sources.

Incident Analysis and Resolution

An analysis to confirm the occurrence of an incident or determine the method of exploit needs to be performed quickly and with sufficient detail of documentation and care to ensure that traceability and integrity is maintained for subsequent use, if needed (e.g., a forensic copy of incident data for legal proceedings). Issues faced by cloud consumers when performing incident analysis include lack of detailed information about the architecture of the cloud relevant to an incident, lack of information about relevant event and data sources held by the cloud provider, ill-defined or vague incident handling responsibilities stipulated for the cloud provider, and limited capabilities for gathering and preserving pertinent data sources as evidence. Understanding and negotiating the provisions and procedures for incident response should be done before entering into a service contract, rather than as an afterthought.

General Recommendations:

A number of significant security and privacy issues were covered in the previous subsections. Table 1 summarizes those issues and related recommendations for organizations to follow when planning, reviewing, negotiating, or initiating a public cloud service outsourcing arrangement.

Table 1: Security and Privacy Issue Areas and Recommendations

Areas	Recommendations
Governance	• Extend organizational practices pertaining to the policies, procedures, and standards used for application development and service provisioning in the cloud, as well as the design, implementation, testing, use, and monitoring of deployed or engaged services. • Put in place audit mechanisms and tools to ensure organizational practices are followed throughout the system lifecycle.
Compliance	• Understand the various types of laws and regulations that impose security and privacy obligations on the organization and potentially impact cloud computing initiatives, particularly those involving data location, privacy and security controls, records management, and electronic discovery requirements. • Review and assess the cloud provider's offerings with respect to the organizational requirements to be met and ensure that the contract terms adequately meet the requirements. • Ensure that the cloud provider's electronic discovery capabilities and processes do not compromise the privacy or security of data and applications.
Trust	• Ensure that service arrangements have sufficient means to allow visibility into the security and privacy controls and processes employed by the cloud provider, and their performance over time. • Establish clear, exclusive ownership rights over data. • Institute a risk management program that is flexible enough to adapt to the constantly evolving and shifting risk landscape for the lifecycle of the system. • Continuously monitor the security state of the information system to support on-going risk management decisions.
Architecture	• Understand the underlying technologies that the cloud provider uses to provision services, including the implications that the technical controls involved have on the security and privacy of the system, over the full system lifecycle and across all system components.
Identity and Access Management	• Ensure that adequate safeguards are in place to secure authentication, authorization, and other identity and access management functions, and are suitable for the organization.
Software Isolation	• Understand virtualization and other logical isolation techniques that the cloud provider employs in its multi-tenant software architecture, and assess the risks involved for the organization.
Data Protection	• Evaluate the suitability of the cloud provider's data management solutions for the organizational data concerned and the ability to control access to data, to secure data while at rest, in transit, and in use, and to sanitize data.

	• Take into consideration the risk of collating organizational data with that of other organizations whose threat profiles are high or whose data collectively represent significant concentrated value. • Fully understand and weigh the risks involved in cryptographic key management with the facilities available in the cloud environment and the processes established by the cloud provider.
Availability	• Understand the contract provisions and procedures for availability, data backup and recovery, and disaster recovery, and ensure that they meet the organization's continuity and contingency planning requirements. • Ensure that during an intermediate or prolonged disruption or a serious disaster, critical operations can be immediately resumed, and that all operations can be eventually reinstituted in a timely and organized manner.
Incident Response	• Understand the contract provisions and procedures for incident response and ensure that they meet the requirements of the organization. • Ensure that the cloud provider has a transparent response process in place and sufficient mechanisms to share information during and after an incident. • Ensure that the organization can respond to incidents in a coordinated fashion with the cloud provider in accordance with their respective roles and responsibilities for the computing environment.

G.4 Mobile Appendix

Mobile Appendix

Introduction

Mobile devices present a unique security challenge with regard to the correct application of CJIS Security Policy requirements. This appendix is intended to provide best practices based on industry standards and on methods to achieve policy compliance in mobile device employment scenarios. The technical methods used to achieve compliance with CJIS Security Policy will typically be different within the mobile environment than those used in fixed locations. Many of the security features and capabilities inherited by endpoint devices from the fixed environment are either not present or present in a different form in the mobile environment. Additionally, the basic technologies used in some types of mobile devices may adequately fulfill some of the CJIS Security Policy requirements which would require additional software or added features in a traditional fixed computing environment. Due to the complexity and rapid evolution of the mobile environment, this Appendix will remain as device and vendor agnostic as practical, however certain key requirements for specific mobile operating systems will be identified for the major mobile operating systems (e.g. Apple iOS, Android) as the underlying technologies are fundamentally different and offer different levels of built-in compliance to CJIS Security Policy.

Sections within this appendix will provide recommendations regarding priorities and level of effort versus value of applying certain security controls in the mobile environment. These recommendations do not supersede or modify the requirements listed in the CJIS Security Policy, and are intended to describe the effect of inherent security functions and inherent device limitations in many mobile platforms that impact the application of policy elements in the mobile environment.

Mobile Device Risk Scenarios

There are multiple risk scenarios that may apply to mobile devices depending on the category of device (e.g. Laptop, Tablet, and 'Pocket sized' devices such as smartphones) and the methods of device connectivity (e.g. cellular service, WiFi + Cellular, WiFi only). Device category and method of connection define the technology types within the device which inherently affects the total level of compliance with CJIS Security Policy that can be obtained by the mobile device.

It is advisable for acquiring agencies to review the mobile device guidance in this Appendix prior to completing selection and acquisition of particular devices. Both the device category and connectivity methods installed and configured on the device will impact the overall risk scenario associated with the device and may significantly affect the effective cost to bring use of the device in compliance with the CJIS Security Policy. For instance, inclusion of cellular radios with the ability to remotely control a device significantly changes the risk scenario by allowing remote tracking, file deletion, and device management which could provide a higher level of CJIS Security Policy compliance than a WiFi only device that does not guarantee the ability to remotely manage the device. However, inclusion of cellular technology may significantly increase the initial device costs and incur ongoing subscription costs. Appropriate choices based on the intended use of the device along with the types and methods of Criminal Justice Information (CJI) data to be accessed could greatly reduce agency cost and enhance security.

Device Categories

This appendix defines risk levels for three categories of devices. Prior to reading individual sections of this Appendix, the agency should identify which device categories will apply to their employment scenario. If multiple categories of devices are employed, individual technical configurations and local policy will likely need to be defined for each category of device based on the risk inherent in the technical characteristics associated with each device category.

Laptop devices

The laptop device category includes mobile devices in a larger format that are transported either in a vehicle mount or a carrying case and include a monitor with attached keyboard. This includes all traditional laptop computers that utilize a ‘traditional’, full-featured operating system (e.g. Windows or a Linux variant). Also included in this category are ‘tablet’ type full-featured computers running a traditional full-featured operating system but without an attached keyboard. The main defining factor is the use of a full-featured operating system and a form factor too large to be carried in a pocket. In general, devices of this type connect via WiFi only, but may include an internal cellular access card in some cases.

The risks associated with this device type are similar to a standard desktop computer at the technical level, but are increased due to the potential to connect directly to the internet without the benefit of organizational network security layers (e.g. network firewall, IDS/IPS, network monitoring devices). There is also an increased risk of intentional device theft from vehicles or unsecure locations as these devices are too large to be carried on the authorized user’s body. There may be increased risk from the limited technical ability to wipe or track a lost/stolen device depending on the particular technical means used for remote device connectivity (e.g. cellular or WiFi).

In general, the technical configurations for compliance with most of the CJIS Security Policy that is accomplished via the operating system (e.g. auditing, access control, etc) will remain consistent with normal fixed location computing systems for laptop devices, but some functions may operate in an unexpected manner due to lack of constant connectivity. Thorough testing of applied security policy elements within the expected mobile environments will help ensure the applied policy configurations remain effective and appropriate when applied to mobile laptop devices.

NOTE: Some newer devices running multi-function operating systems (e.g. Windows 8 or similar multi-mode operating systems) may exhibit technical features associated with both laptop and tablet device categories based on their current operating mode which may be reconfigured by the user on demand. If this is the case, it will be necessary to assess and configure multiple operating modes to be compliant with CJIS Security Policy on the device, or restrict the operating mode to one category of operation.

Tablet devices

The tablet device category includes larger format devices transported via vehicle mount or portfolio sized carry case that typically consist of a touch screen without attached keyboard. These devices utilize a limited-feature operating system (e.g. Apple iOS, Google Android, Windows mobile) that is inherently more resistant than a traditional operating system to certain types of network based technical attacks due to the limited-feature sets. Additionally, limited functionality operating systems are designed specifically for the mobile environment where battery life and power efficiency are primary design drivers. This inherently limits the types of services that can

function effectively on the devices (e.g. traditional real-time anti-virus software) as the base operating system may not be designed to allow installed applications enhanced execution priority in the background and or the ability to examine the contents or communications associated within another application. However, this same design methodology significantly limits the vectors available for malware transmission and the device or application data actually accessible to malware if a device becomes infected.

Tablet devices will have different risks associated depending on the installed and configured methods for network access (e.g. ‘always on cellular’ vs. WiFi only). Physical risks associated with this category are similar to the laptop category for enhanced likelihood of intentional theft or device hijacking while unattended, while the technical risks are similar to the pocket device category.

Pocket devices/Handheld devices

The pocket/handheld device category is technically similar or identical to the tablet category and is primarily differentiated by device form factor. Pocket/handheld devices are characterized as having a limited functionality operating system and a small form factor intended for carry in a pocket or ‘holster’ attached to the body. The bulk of this category will be cellular ‘smartphones’ with integrated cellular data connectivity, however devices intended to be worn or carried on the body (e.g. portable fingerprint devices) may also be included in this category if they operate using a limited functionality operating system. Custom or specialty devices may meet the form factor distinction for this category, but operate using a full-feature operating system. In rare cases of this nature the employing agency should apply security guidance and principles in this appendix for both the laptop and pocket device categories.

Risks associated with this category are a reduced threat of theft to a stored devices (e.g. device left unattended in a vehicle) since these devices are typically carried continuously by the authorized user, but include a greater risk of temporary or permanent loss of control due to the device being misplaced by the authorized user.

Due to the installation of a limited functionality operating system, the technical threat to these devices via a network based attack is significantly lower than the laptop category, however, the threat of unauthorized access at the device level may be higher if the device is lost due to technical limits on multi-factor authentication to the operating system itself and practical limits to device passwords due to screen/software keyboard limitations.

NOTE: Data accessible on pocket or tablet devices simply through the entry of a single device PIN or password should not be considered secure due to the likelihood of enhanced password guessing based on fingerprints/smudges on the device touch screen. Any data stored on devices of these types should be protected within a separate secure container using Advanced Authentication.

Device Connectivity

There are three main categories of device connectivity that are associated with varying risk levels and threats to the devices. The Three categories are: Cellular Network Only (always on), WiFi Only (includes ‘on demand’ cellular), and Cellular (always on) + WiFi network. The risks associated with connectivity categories are general risks and may apply differently to any particular device at different points in its usage or lifecycle. Particular device configurations either through the operating system or a third-party mobile device management (MDM) system may be

able to significantly control and define which particular connectivity risks may be associated with a particular device.

Cellular Network Only (always on)

Cellular network connectivity is characterized by ‘always on’ network connection through the device internal radio to a cellular network provider. There is a reasonable assurance that devices with ‘always on’ cellular can be tracked, managed, or wiped remotely if lost or stolen. This will significantly reduce risks associated with loss of the device and attempted illicit access to the device. One important consideration for this risk category is characterization of the device as ‘always on’ or ‘on demand’. In effect the difference is typically a configuration setting, which in some cases may be changeable by the user. In particular most cellular smart phones contain ‘airplane’ mode settings that disable all internal radios allowing a user authenticated to the device operating system via password or personal identification number (PIN) to disable the cellular system. Access to this functionality may be disabled through the use of some MDM systems which would necessitate a complete power down of the device while carried on aircraft. Additionally, someone illicitly obtaining a device with properly configured password requirements and screen lock timeouts would be unlikely to guess the device password before the device was reported stolen in order for them to disable the cellular connection and prevent tracking or a remote wipe of the device.

Cellular networks do not allow for the same level of exposure of individual devices to random access from the internet. This significantly reduces the potential network based attack vectors that might reach a cellular connected device. The risk scenario in most cases from a network based attack would be similar to a device protected behind rudimentary network defenses (e.g. standard firewall but NOT advanced intrusion detection/prevention) Cellular device communications cannot typically be accessed by other ‘eavesdropping’ devices physically close to them without significant specialized equipment and can be considered well protected against network attacks below the nation/state level of technical capability by the hosting technical infrastructure and technology inherent in the device. However, network based attacks that utilize connections initiated by the user device may still succeed over the cellular infrastructure. For this reason, the technical protections inherent in the cellular infrastructure provide limited protection against user/device initiated actions (e.g. web surfing on a cellular connected web browser). Therefore, the protections provided by always on cellular connections are primarily in the ability to remotely access the mobile device for tracking or data deletion in case of device loss or compromise, which combined with a limited functionality device operating system, the protections are generally equivalent to a ‘personal firewall’ if properly configured and supported by a well-designed organizational infrastructure. However, that equivalency does not apply to full-featured operating systems connected through cellular infrastructure.

NOTE: It should be noted that a technically capable, intentional, thief knowingly obtaining an ‘always on’ cellular device for the purpose of data theft can physically disable the radio by utilizing a Faraday cage or similar external electromagnetic shield device while attempting to guess the device password. While technically possible these methods require specialized equipment and high technical expertise and would be very unlikely to be employed except for specifically targeted attacks. When always on cellular connectivity is combined with a robust incident reporting process and user training for rapid response to device loss or theft, the associated risks can be minimized.

WiFi only (includes ‘on-demand’ cellular)

WiFi only devices do not include cellular radios or include cellular radio that must be manually activated or ‘connected’ to the cellular network. They connect to the network or internet through WiFi ‘hotspots’ or external access points or manually to cellular networks. Some MDM or device configurations may be able to limit the types and specific WiFi access points the device can connect to, which may change the risk scenario of the device to a similar risk scenario as the Cellular Network Only scenario. However, if mobile devices are permitted (through technical and or policy decisions) to connect to any WiFi access point designated by the device user, the overall device risk scenario is high and the device may be accessible to a large number of potential network based attack vectors. Unrestricted WiFi access is not recommended on any agency owned device, but must be assumed to exist on any personally owned device authorized to access CJI. Significant compensating controls may be needed to ensure devices accessing CJI over ‘public’ WiFi access points are not susceptible to communications network eavesdropping, credential hijacking or any of the various potential man-in-the-middle attacks possible through access point spoofing. The communications security risks can be significantly mitigated by mandatory device configurations (e.g. MDM based policy) that only allow devices to connect to cryptographically verified agency controlled WiFi access points.

WiFi only or devices with ‘on-demand’ cellular access (e.g. user or event driven cellular access initiated from the device and not from a centralized management location) are significantly more at risk from data loss subsequent to device loss or theft as there is no guarantee the tracking or remote wipe can be initiated once the device is out of agency control. This can be mitigated by utilizing tracking/anti-theft products that require a periodic network connection to authorize access and perform automated device locking (‘bricking’) or remote wipe if network connections are not made within a specified period. Software of this nature is generally available for full-featured laptops but may not be available for limited-feature mobile operating systems.

Cellular (always on) + WiFi Network

This is a hybrid scenario that has become typical with most ‘smartphones’. These devices contain both the always on cellular connection, but may also be configured to access local WiFi networks for enhanced bandwidth. In considering devices with these technical characteristics, the theft/loss risks are similar to the cellular only scenario (due to tracking and remote access through the cellular connection), while the data and network based risks must be considered to be similar to the WiFi scenario unless the capability of the device to connect to WiFi networks is limited by technology or policy to agency owned WiFi Access Points configured in accordance with the CJIS Security Policy. Careful consideration must be made to the particular configurations, management systems, and human oriented operational policies based on the particular technical capabilities and configurations of these types of devices.

Incident Handling (CJIS Security Policy Section 5.3)

Additional or enhanced incident reporting and handling procedures will need to be developed to cover mobile device operating scenarios. Various exploits and methods to compromise mobile devices require either specialized equipment or lengthy operations to implement. Rapid response to mobile device related incidents can significantly mitigate the risks associated with illicit data access either on the device itself or within online data resources associated with the device through an application or specialized interface. However, parallel or special incident handling procedures with associated equipment or systems may need to be put in place to properly respond to incidents involving mobile devices. This section lists three areas where enhanced incident handling and

response processes may need to be implemented to ensure mobile device compliance to the incident handling policy in Section 5.3.

If personally owned devices are utilized within the environment in a Bring Your Own device (BYOD) scenario, specialized and costly incident handling procedures and processes may need to be developed to support compliance for those devices. The costs associated with enhanced incident handling procedures may need to be incorporated in the cost and risk based analysis to allow personally owned devices in the BYOD scenario, as the technical methods and risk to achieve compliance under BYOD scenarios may exceed any cost savings potentially achieved through BYOD.

Loss of device Control

Mobile device users should be trained and provided with explicit user actions in case positive control of a mobile device is lost for any period of time. Loss of positive control means the device is in the physical control of non-CJIS authorized individual or the device is left unattended in an unsecure location (e.g. counter of the coffee shop). Even if the device is recovered quickly there is significant risk that either the device settings could be tampered with or data on the device could be illicitly accessed. The level of detail and particular scenarios identified in the agency incident response plan should be consistent with the presence of persistent CJI on the device or the technical means used to access CJI from the device (e.g. ask the question: “Is it reasonable to assume CJI could be accessed”) as well as the degree of device configuration control exercised by the user from the device main login. At a minimum, special incident handling procedures should be developed for the following scenarios:

- Device known to be locked, control loss of minimal duration
- Device lock state unknown at time of control loss, duration of loss minimal
- Device lock state unknown at time of control loss, duration of loss extended
- Device known to be unlocked at time of control loss, duration of loss more than momentary.

NOTE: Organizations should define appropriate time value criteria based on the operational environment for the above scenarios. For instance, a ‘momentary’ loss of control might be considered a matter of seconds in a situation where no one could reasonably have accessed the device, while ‘minimal’ durations might include a few minutes of time and ‘extended’ periods would be any time longer than a few minutes.

Other scenarios should be addressed as appropriate to the intended device employment, with explicit user and organizational actions identified based on the device technologies and any organizational management capabilities.

Total Loss of device

Incident response scenarios for the total loss of the device should be developed based on the methods/storage of CJI on the device, the lock state of the device at time of loss (known locked, known unlocked, or unknown), and the technical methods available for remote tracking or wiping of the device. It is critical to implement incident handling procedures quickly in this case. Remote wipe functions can be implemented for always on cellular devices with a high potential for success that may include positive confirmation from the device that the wipe was completed. However, for WiFi only and on demand cellular devices, incident handling procedures that lock the device out

of accessing CJI may be necessary, while there would be no guarantee that any CJI stored on the device could not eventually be accessed. For this reason, CJI should not generally be stored directly on WiFi only or on-demand cellular devices unless an extremely robust anti-tamper system is in place on the device itself.

Potential device Compromise (software/application)

Incident response scenarios for potential device compromise through intentional or unintentional user action should be developed to ensure compliance with policy. This includes rooting, jailbreaking or malicious application installation on the device during a loss of device control scenario or inappropriate user action in the installation of applications to the device (compromise can occur from either intentional threat agent actions or accidental user actions). Triggers for this incident handling process may be driven from either user notification or electronic detection of device tampering from an audit or MDM compliance check.

Audit and Accountability (CJIS Security Policy Section 5.4)

The ability to implement some Audit and Accountability functions specified in the CJIS Security Policy on mobile devices with limited function operating systems (e.g. Android, Apple iOS) is not natively included within the operating system. Either additional device management systems, enterprise mobility management (EMM) or MDM, or auditing from systems accessed by the mobile device will be necessary to ensure appropriate levels of auditing exist.

Auditable Events (reference 5.4.1)

Some of the specific audit requirements in the CJIS Security Policy may not be technically relevant to the mobile operating system due to its internal functioning. To achieve compliance with the CJIS Security Policy it will be necessary in most cases to utilize some form of MDM or EMM system. Additional auditable events that compensate for the technical limitations of limited function mobile operating systems may be available through the use of MDM systems (e.g. association of event with global positioning system (GPS) location of the device). Specific auditable events of interest in the mobile environment will depend on the intended device usage, compartmentalization of data on the device, and options available with the specific technologies employed. For instance, item 2 in Section 5.4.1.1 indicates an auditable event includes attempts to modify elements of user account modification. Due to the limited internal functions of mobile operating systems, this event type is not relevant to the operating system itself as they are generally provisioned with only a single non-modifiable user account on the device. To achieve compliance in a scenario where CJI is stored or accessed from a secure application on the device, auditing of access to the secure application either through application design, or third party MDM capability may provide an acceptable compensating control. For compliance with the policy each auditable event and event content must be compared to the particular technologies and applications employed to determine if adequate compensating controls are being met for audit items that either do not apply to mobile technologies or cannot be implemented within the technology itself.

Alternative and compensating controls that provide detailed audit of access to CJI either on the mobile device itself or through a controlled application to a central server may provide equivalent auditing capability to the events specified in the policy. However, multiple auditing systems may be required to replicate the auditing provided at the operating system level by a full function operating system. Therefore, the overall auditing design should take into account retrieval and

consolidation of events or audit data from multiple auditing systems as appropriate to comply with policy.

Audit Event Collection

Mobile devices without an ‘always-on’ cellular connection may pose technical challenges to ensure any audit records collected and stored on the mobile device itself can be retrieved for review and analysis per the CJIS Security Policy. Alternatively systems which explicitly require a network connection to a central server to access data or decrypt on-device storage may provide acceptable audit event collection and reporting since there is a guarantee that network connections must be in place for CJI to be accessed. Careful consideration should be made regarding the accessibility of audit records when developing the mobile audit scheme.

Access Control (CJIS Policy Section 5.5)

Access control associated to limited functionality mobile operating systems will typically operate in a different manner than full function operating systems. For instance there is normally not a provision for multiple user accounts on many mobile operating systems which may mean the policy requirements for access control (e.g. regarding account management) would not be apply to the mobile operating system, but should rather be applied to a particular application, either stand-alone to the device or as part of a client server architecture. Application of access control policy identified in the CJIS Security Policy will often need to be applied to elements of the total system beyond the device operating system.

For example, CJI stored or accessed from a secure mobile application that requires connectivity to a CJIS authorized server architecture could potentially accomplish most or all of the access control policy elements based on user authorization via the secured application and be largely independent of the mobile operating system. Alternatively, if storing CJI in ‘general’ purpose data storage containers on a mobile device it may not be possible to achieve compliance with the CJIS Security Policy. Careful consideration and deliberate design of mobile applications or data storage will be required to achieve compliance on mobile devices.

Due to the inherent nature of limited function mobile operating systems, very tight access controls to specific data is actually implemented within the operating system. This effectively prevents applications from accessing or manipulating data associated with other applications to a very high degree of confidence as long as the device is not rooted or jailbroken. However, the device user is automatically granted access to all device data through the associated application unless the application itself has a secondary authentication and access control methodology. Additionally, since basic device functions (e.g. phone) are typically protected using the same password or PIN as the device level encryption, use of a weak PIN to allow easy access to basic device functions largely negates the value of the integrated device encryption.

If personally owned devices are utilized within the environment (BYOD scenario), specialized and costly access control methods may be required to reach compliance with CJIS Security Policy. The costs associated with enhanced access control procedures and technologies should be incorporated in the cost and risk based analysis to determine whether or not to allow personally BYOD, as the technical methods and compensating controls required for CJIS Security Policy compliance are likely to exceed any potential cost savings for implementing BYOD.

Device Control levels and access.

Limited function mobile operating systems are typically very constrained on the levels of access provided to the user. However, intentional user actions (e.g. installing an application and accepting inappropriate security access levels for that application) may bypass some of the built in security protections inherent in the limited functionality devices. Compliance with CJIS Security Policy may be difficult without the addition of strict device control policy. In a mixed environment (e.g. agency owned devices and BYOD), access control policy with BYOD systems may be impractical or impossible to fully implement.

Embedded passwords/login tied to device PIN.

Limited function mobile operating systems typically allow the association of multiple passwords and access credentials with particular applications. The system access provided by these embedded credentials will often be tied to the device password or PIN. An example would be access to device integrated email and calendar applications. Alternatively a 'corporate' email application may independently encrypt the data associated with the application and require a separate login from the device itself. Access to CJI utilizing only the device level password or PIN and device embedded credentials is not compliant with CJIS Security Policy unless protected with Advanced Authentication, which is not currently possible on most devices. Therefore, use of integrated device functions (e.g. built in email or chat) to store or transmit CJI would also not be compliant.

Access requirement specification

In general, due to weaknesses associated with password guessing based on analysis of fingerprints or swipes on the device touch screen, short (4-8 digit) device PIN numbers provide limited security to a determined password guessing attack. Conversely, utilization of a robust password at the device level may be inconsistent with quick access to basic device functions (e.g. phone). When developing specific CJIS compliant access control and authentication schemas a layered approach with the device PIN protecting only the basic device functions (e.g. phone, camera, non-secure applications) and a more robust password or multifactor authentication used to protect applications or data storage may achieve policy compliance where the device password/PIN would not. In a layered security deployment, careful attention must be placed on the capability to share data (e.g. cut and paste or screenshot functions) between secure applications with CJI or CJI access and basic device functions with limited security controls.

Special Login attempt limit

Depending on the access and authentication scheme applied to the mobile device, it may be appropriate to fully comply with the CJIS login attempt limits within a secure application or container and not solely at the device level. However, the device itself should have login attempt limits consistent with the risk associated to the data or configurations accessible on the device itself. Since mobile devices are inherently portable, and can easily be removed from a location. Brute force attempts to gain access to the system, especially when protected only by a short PIN, are likely to be successful given sufficient time. Special consideration should be made based on device connectivity methods (cellular, WiFi, etc) on the appropriate number of unsuccessful login attempts that will be allowed and the resultant actions taken by the device. Most devices either natively allow for the device to wipe itself after a failed number of attempts, or allow the application of EMM/MDM applications to perform wiping actions after a predetermined number of failed login attempts.

Login failure actions

Mobile devices with or without MDM software can typically be configured to perform actions based on serial unsuccessful login attempts. Appropriate actions to configure may be dependent on the data resident on the device and the connectivity method employed by the device. Most devices can be configured to delete all data on the device and/or issue an alert to the network if a number of incorrect passwords are entered. This is a very advantageous feature, however specific configuration of the number of attempts and resultant action must be considered against the state of the device after an unsuccessful attempt action is triggered. A full device wipe will typically leave the device in a fully or partially non-functional state which could introduce risk if part of the intended use is time critical phone calls. Where possible, full device wipe associated with unsuccessful attempts at the device level password should be configured but the number of invalid attempts may exceed the CJIS Security Policy at the device level if all CJI on the device is protected by an additional layer of encryption protected by a subsequent secure application authentication method that is technically prevented (via complexity rules or entry rules) from being the same as the device level authentication and the secure application is configured in accordance with the policy and also contains a secure data wipe capability after a specified number of incorrect authentication attempts.

System use Notification (CJIS Policy reference 5.5.4)

Agency policy should include specific mandatory language consistent with the CJIS Security Policy to identify the device restrictions and consent. However, due to screen size limits, some mobile devices may not be technically capable of displaying the full text used with traditional operating systems. To achieve compliance agencies should contact their legal department for appropriate wording of a short version of the system use notification that can be set to display within the constraints of the device lock screen. This may be accomplished through embedding the text into an image displayed on the lock screen or some other external device labeling method if the device does not permit sufficient text to be displayed.

In a BYOD environment or mixed (agency owned and BYOD), it may be necessary to develop or deploy custom applications that can achieve compliance with the system use notification upon access and prior to any CJI access being allowed.

Session Lock (CJIS Policy reference 5.5.5)

Due to the portable nature of mobile devices the session lock limit in the general CJIS Security Policy may be excessive in the mobile environment for certain device functions and insufficient for other functions based on intended device usage. Agencies should examine the minimum lock time practical for all mobile devices based on their employment scenario and ease for which a user can manually lock the device. The actual session lock times should be adjusted as appropriate to the device type, device operational location, and the data accessible on the device when unlocked. Pocket size devices are at greatest risk if screen lock times are insufficient, however, for devices used in emergency response or communication, extended lock times at the basic device level may be considered if CJI is subsequently protected by an application or web interface utilizing more stringent secure locking functions. A well designed solution may include multiple session lock settings at the device and individual application levels to ensure the CJIS Security Policy requirements are met for CJI access, while other device functions are accessible under different session lock configurations.

Device WiFi Policy

Specific WiFi configuration policy should be developed based on the intended use environment and data access requirements for the device. The policy should explicitly cover configuration of device connections. Technical methods specific to the mobile technologies may need to be implemented to ensure all mobile devices are compliant with CJIS Security Policy. Current CJIS Security Policy provides detailed configuration requirements for WiFi connections, however it was originally intended for defining requirements for fixed infrastructure WiFi (802.11) supporting wireless within a facility. The security requirements identified for fixed infrastructure installations are applicable to mobile usage, however there are several mobile specific scenarios where the requirements may not be clear. The following sections identify areas not specifically covered in the existing policy that will require special handling to ensure wireless connections are compliant.

Hotspot capability

Many mobile devices now include the capability to activate an internal WiFi hotspot that allows other devices to connect through the hosting device to the internet over the devices cellular radio. While this is a potentially valuable capability when multiple law enforcement devices may need localized internet or network access, mobile hotspots should be configured as consistent with the CJIS Security Policy on wireless access points. Connections must only be accepted from known and approved devices in order to protect the integrity of the hosting device as well as the communications security of other connected devices. Since most mobile hotspots are not technically capable of providing the device authentication required for infrastructure wireless, use of mobile hotspot capability should assume the overall portable WiFi network itself is not secure and CJI should not be transmitted or exposed on the network without appropriate encryption.

Connection to public hotspots

There are significant risks to connecting to public wireless access points. Rogue access points masquerading as legitimate public access points may allow for man-in-the-middle, eavesdropping, and session hijacking attacks. While not specifically prohibited in the current CJIS Security Policy, it is recommended that connection to public internet access points be technically restricted by device configuration or MDM systems if possible. CJI access mechanisms from mobile devices should include robust authentication methods specifically designed to prevent interception or hijacking of CJI or user information through the use of a rogue access point masquerading as a legitimate public wireless access point. Transmission encryption alone may not provide sufficient protections when device connections originate at public hotspots. Since the public hotspot controls access to all network services at the connection point (e.g. Domain Name System) attacks against the transmission path are possible that would not normally be feasible in a fixed environment where communications exist between two secured network enclaves.

Cellular Service abroad

If mobile devices are used outside of the United States, especially if connected to foreign cellular networks, specific handling procedures may need to be developed for the use of the device while abroad and the assessment or configuration check of the device state once the devices are returned to the United States. Certain device internal functions on cellular devices may be modified or compromised by the cellular carrier as the devices are intended to have certain parameters configured by the cellular service provider which is considered a 'trusted' entity by the device.

Cellular carriers within the United States are constrained by United States laws regarding acceptable modifications to devices. Similar legal constraints cannot be assumed to exist in some areas of the world where laws and regulations for data and personal privacy may allow cellular carriers significantly more leeway in changes made to devices on their networks.

Security plans involving cellular connected devices that will be connected to foreign cellular networks should include technical and policy controls to ensure device use while abroad, data resident on the device while abroad, and the software integrity of the device once returned to the United States are all appropriate to the specific device and threat levels associated with the expected foreign travel. This should explicitly include considerations for devices in which an internal subscriber identity module (SIM) card is inserted into the device to obtain Global System for Mobile (GSM) cellular connections abroad to ensure any residual data on the SIM card is properly purged. Additionally, incident handling procedures may need to specify more stringent responses to even momentary loss of device control, and it may not be possible to assume tracking, anti-theft, and remote data wipe functions that work in the United States would be functional in all potentially visited geographic and political regions.

Bluetooth

Mobile devices utilizing Bluetooth should be evaluated for their ability to comply with the CJIS Security Policy Bluetooth requirements prior to acquisition. This includes the data device itself and any authorized Bluetooth accessories which will be associated to the device. While the technical security in current versions of Bluetooth is significantly stronger than legacy versions, mis-configuration of devices can still pose a significant threat in the mobile environment. If not specifically utilized for a required purpose, it would likely be most cost effective to disable or restrict the device Bluetooth radio utilizing device configurations or an MDM product. Additionally, the using agency may need to develop technically extensive training or user awareness programs to ensure use of Bluetooth capability does not render the device out of compliance if device users have the ability to make Bluetooth associations to the device. Specific instructions or guidance for specific devices could be developed to ensure all implementations are compliant.

Voice/Voice over IP (VoIP)

Cellular voice transmissions are distinctly different at the technical level than Voice over IP (VoIP) transmissions using voice/video applications (e.g. FaceTime, Skype). The use of VoIP is not specifically granted the exemption identified in CJIS Security Policy Section 5.5.7.3.2. Agencies wishing to use capability of this type should ensure the specific technical implementation complies with the Policy on authentication and data encryption.

Chat/Text

Device integrated chat/texting applications and many common third party chat applications authenticate and are identified using embedded passwords or the device identifier only. These functions should not be considered secure or appropriate for transmission of CJI data. Texting functions that utilize a cellular service providers Short Message Service (SMS) or Multimedia Messaging Services (MMS) functions do not constitute a secure transmission medium. Third party applications utilizing appropriate encryption and authentication methods independent of the device password/PIN may provide a compliant solution where the device integrated utilities are will not provide a compliant solution.

Administrative Access

Local administrative access to the mobile device, regardless of device category should be restricted by some mechanism. For traditional operating systems, configuration of a separate administrative account other than that used for normal logins to the device is an acceptable method to ensure appropriate access permissions to the mobile user for which they are authorized. However for limited functionality mobile operating systems (e.g. Android, Apple iOS) internal permissions and accounts assume a single authorized device user with explicitly defined permissions. Those permissions may be modified through policy applied to the device, but are typically global to the device itself. As a result, to ensure appropriate separation of access permissions, it may be required to ensure specific applications or software on the device are configured with individual authentication methods to separate application data from ‘general user’ access. Without additional authentication at the application level, access to specific application data would be available to any user with the ability to unlock the device. This may be appropriate in some scenarios with a high degree of assurance that the device can only be accessed by a single user, but sufficiently stringent device passwords and short screen lock times may prove problematic for practical use of some device functions. An alternate method to ensure strict separation of ‘routine’ device functions which may be accessed by multiple individuals (e.g. phone function if loaned to someone for a critical call) is to ensure any method used to access or store CJI has a separate and more stringent authentication method configured with rules that make it impossible to use the same authentication credential (e.g. PIN/Password) on both the device authentication and the application or function with access to CJI.

Rooting/Jailbreaking

‘Rooting’ (Android OS) or ‘Jailbreaking’ (Apple iOS) refer to intentional modifications to the mobile device operating system in order to grant the device user or an installed application elevated control that would not normally exist on the device. The security model internal to the various mobile device architectures vary significantly, however the common effect of rooting or jailbreaking the devices is to bypass many or all of the built in security features. The security feature bypass may be universal to all device features and installed applications once completed. Intentionally rooting or jailbreaking mobile devices should be avoided in any scenario as it potentially defeats all built-in data access and segregation controls on the device. Additionally the rooting or jailbreaking process itself has a heightened risk of introducing malicious code as part of the process, and also substantially increases the risk for malware to infect the device through user action. Extreme caution should be used if software is being installed that requires the devices to be rooted or jailbroken for the software or application to function. This is inclusive of purported security software that requires a rooted or jailbroken device to function. For example, on both the Android and Apple iOS platforms, the built-in security features for data access and memory segmentation prevent the effective operation of ‘traditional’ anti-virus and intrusion detection/prevention software. Software or applications purporting to perform these functions but requiring rooting or jailbreaking of the device and may actually accomplish the anti-virus or IDS/IPS function but are also likely to significantly increase the overall risk associated to the device by effectively disabling most or all of the integrated security features. A careful risk-based assessment should be conducted by a trained security professional prior to allowing the operation of any rooted or jailbroken mobile devices regardless of intended use. Significant compensating controls would be required to return a rooted or jailbroken device to minimal compliance with most of the CJIS Security Policy and would likely not be a cost effective approach.

NOTE: There is a distinction between rooting a ‘stock’ Android installation vice the installation of a separately supported secure operating system. There are secure versions of Android available or that can be developed based on the open source Android source code and compiled for installation on a particular hardware device. Installation of a secure, supported mobile operating system that replaces the device original operating system may significantly enhance the security of the device and should not be confused with ‘rooting’ and Android installation. Due to the close integration of operating system security with hardware elements, and the proprietary nature of Apple source code, there are not currently separate ‘secure’ versions of the Apple iOS and it is unlikely they will be developed.

Identity and Authentication

Due to the technical methods used for identity and authentication on many limited functionality mobile operating systems, achieving compliance to CJIS Security Policy may require layering of identification and authentication mechanisms. With the complexity and large number of potential identity and authentication solutions in the mobile environment emphasis must be placed on designing secure identity management and authentication architecture prior to the selection of individual devices or applications. Failure to consider a robust identity and authentication scheme as part of system design or acquisition will significantly increase the risk of subsequent noncompliance with CJIS Security Policy and potential added costs for a remedial solution. Many identity and authentication schemes used by existing commercial applications may make claims that appear to be consistent with CJIS Security Policy Advanced Authentication requirements, however, extreme care must be taken to ensure the actual technical implementation is compliant with policy.

Utilizing Unique device Identification

Some commercial applications and features integrated with some mobile operating systems permit the mobile device to be uniquely identified in a cryptographically robust manner. Any authentication schema that considers the possession of the mobile device as a factor in uniquely identifying and authenticating a CJIS authorized user must also include factors beyond than mere possession of the device. Larger form factor devices that cannot be carried on the person of the authorized user should not rely on possession of the device as an identifying factor, but may still include identifying capability within the device to provide assurance that the device itself is an authorized device. This should still be coupled with multi-factor advanced authentication to the device itself or the application hosting CJI. Coupling unique device authentication with robust advanced authentication of the user provides a high degree of confidence that both the specific device and the operator of the device are correctly identified. Utilizing device unique identification in order to authorize initial connections from the remote device back to the CJI hosting system or enclave provides additional protection to the CJI hosting system to reduce the attack surface of the hosting system and should be considered a good practice, but not in itself an authentication mechanism for the device user.

Certificate Use

One method for uniquely identifying mobile devices is to place part of a public key pair on the device in the form of a public key certificate. While there is value to ensuring the device itself can authenticate to a system supplying CJI, and may provide a critical layer of identification or authentication in a larger scheme, a certificate alone placed on the device should not be considered valid proof that the device is being operated by an authorized CJIS user, only that the device itself is authorized to host CJIS users. Additional user identification and authentication should be used to supplement any device certificate installed. Using a PIN or password separate from the device login to ‘unlock’ the certificate from cryptographic storage within a secure application will provide an additional layer of security and may increase the confidence level the device is being used by the intended user. However, use of public/private key pairs or pre-shared encryption keys can be utilized as part of an architecture to protect against certain session hijacking or man-in-the-middle attacks a mobile device may be susceptible to if connected to public internet connections.

Certificate Protections

Any certificates or cryptographic keys stored on any mobile device should include protections against the certificate or key being extracted from the device. Additionally certificates or other keys stored on mobile devices that grant the device special access or unique identification should be configured for remote wipe on demand or self-deletion based on a number of unsuccessful login or access attempts. Alternatively, methods may be used to revoke or invalidate the unique certificate or keys associated with a device.

Minimum Password/Pin (Reference CJIS Security Policy Section 5.6.2.1)

The minimum password protections identified in the CJIS Security Policy may not be appropriate for the device PIN/password due to immediate access requirement for some device functions (e.g. phone function) secured by the device PIN/password and the difficulty to enter a complex password under emergency conditions on a small screen. In cases where the risk of a complex password on the device itself is deemed significant, a layered authentication approach may be necessary where CJI or access to CJI is protected via one or more additional layers of access control beyond the device PIN/password. In cases where the CJI or access to the CJI is cryptographically segregated from applications accessible using the device level PIN/Password (e.g. secure application or secure browser vice the built-in browser) the authentication mechanism for the secure application or browser may satisfy the CJIS Security Policy requirements if fully compliant as a stand-alone application.

Configuration Management

Due to the potential for inconsistent network access or monitoring capability on mobile devices, methods used to monitor and manage the configuration of traditional full-featured operating systems may not function properly on limited function mobile operating systems. Configuration Management systems in the mobile environment may be designed in order to duplicate some of the functions typically performed by traditional anti-malware systems that will not function properly on some mobile operating systems.

Mobile Device Management (MDM)/Enterprise Mobility Management (EMM)

MDM and EMM systems and applications coupled with device specific technical policy can provide a robust method for device configuration management if properly implemented. MDM capabilities include the application of mandatory policy settings on the device, detection of

unauthorized configurations or software/applications, detection of rooting/jailbreaking of the device, and many other security policy related functions. In many cases, the most cost effective way to achieve CJIS Security Policy compliance on mobile devices is the selection of MDM or EMM applications and infrastructure appropriate to the mobile operating systems and intended access to CJI on the mobile devices. MDM/EMM functions may be applicable to most of the CJIS Security Policy requirements and allow for significant compensating controls in areas where traditional methods of CJIS Security Policy compliance are not technically feasible. Section 5.5.7.3.3 of the CJIS Security Policy specifies the minimum functions required for MDM. However, careful selection of the MDM product will potentially provide a cost effective method for additional areas of compliance in the access, auditing, incident response, authentication, media protection and system integrity sections of the CJIS Security Policy.

Device Backups/Images

Device images and backups provide protection against data loss, but also provide a method to quickly recover a device after damage or potential compromise. Due to an inherently limited ability to access the internal file structure of mobile devices, it can be difficult to easily identify a device compromise or illicit modification of the device. Some device imaging and assessment software may provide a secondary forensic capability, especially if there is intent for the device to be used outside the United States.

Bring Your Own device (BYOD) employment

BYOD environments pose significant challenges to the management of secure device configurations. In many cases it may be impossible to apply effective security that is acceptable to the device owner or it may require extremely costly compensating controls to allow access to CJI on personally owned devices. While allowed by the CJIS Security Policy, agencies are advised to conduct a detailed cost analysis of the ancillary costs of compliance with CJIS Security Policy on personally owned devices when they are approved for use. In some cases, a BYOD user may agree to abide by the same device configurations and limitations as imposed on an agency owned device, but signed user agreements should still be in place to ensure the agency has a legal right to recover or clear the device of all data prior to device disposal or employee termination. In other cases, robust secure applications may provide acceptable levels of compliance in a BYOD environment for limited CJI access but application design and architecture should assume the device itself is un-trusted. If MDM/EMM software capable of detecting rooting or jailbreaking of the device is not installed, any CJIS or data access occurring from the device is at a substantially higher risk of compromise.

Configurations and tests

Common configurations specific to all employed mobile devices should be developed to ensure compliance. Configuration tests should be developed and executed on all versions of mobile devices under all possible connectivity scenarios to ensure CJIS Security Policy compliance under all expected operating conditions. Since mobile devices can expect to operate in different physical and network environments, testing and validating correct security functions is more critical than on fixed computing platforms. Additionally, security functions that function properly on one version of a mobile operating system on a particular device may not function in the same manner even on the same version on a different device or a different version on the same device.

Media Protection

Some mobile device hardware platforms include the ability to add removable storage in the form of memory cards. This function is primarily related to Android and Windows mobile platforms and is intentionally limited on Apple devices, but may be possible through certain application functions. While the Android platform performs robust cryptographic separation of data stores between applications within the ‘internal’ storage of the device, the Android OS does not provide secure separation of data stores on ‘external’ storage. Some Android hardware devices include additional storage hardwired inside the device that is classified by the operating system as external storage and the normal separation between applications accessing that storage is not applied. Each potential device considered for acquisition must be assessed regarding specific ‘external’ media protection requirements which may actually include built-in media or storage.

Protection of device connected media

As a result of the limited protection and encryption capabilities applied to device removable media and SIM cards for cellular provisioning that include onboard data storage, all externally removable media or memory should be handled consistently with the CJIS Security Policy on media protection.

Encryption for device media

While most mobile operating systems have the capability to encrypt internal storage, it may require specific device settings to be enabled. All mobile device storage should meet the encryption requirements identified for media in the CJIS Security Policy. Specific settings may need to be applied to ensure proper encryption is actually employed. Additionally, the device built-in encryption capability is typically tied to the device PIN or password. Depending on the device PIN or password requirements the integrated encryption may be easily bypassed by password guessing and appropriate consideration should be made to ensure additional encryption protected by advanced authentication methods be applied to all CJI.

Physical Protection

Due to small form factors and the fact that mobile devices are often stored in lower security areas and vehicles, physical protection of the devices must be considered in both policy and training. Physical protections will often be the responsibility of the assigned device user and physical protections typically inherited by individual information systems from a secure facility will not be available to mobile devices which will require compensating controls to achieve compliance.

Device Tracking/Recovery

MDM software as well as some integrated mobile operating system functions may allow tracking of stolen or lost devices via ‘always-on’ cellular data connections and the devices built-in GPS. Device tracking with WiFi only or ‘on-demand’ cellular access may not be reliable. Enabling device tracking capabilities, while not a replacement for secure storage, could be a compensating control used to substantially reduce overall device risk in some scenarios. Device tracking is not currently required in the CJIS Security Policy but should be applied to agency owned devices where possible as a risk mitigation factor. Enabling of device tracking on personally owned devices in a BYOD environment may raise employee privacy concerns and should be considered only for critical systems with the full knowledge of the employee and concurrence of the legal department. This is an enhanced risk that must be accepted for BYOD employments and should be considered

when allowing BYOD employment. Device tracking is available for both limited function mobile operating systems as well as traditional operating systems installed on laptop devices.

Access to device tracking software or applications within the organization should be controlled with limits and formal processes required to initiate a tracking action. It is advisable to include appropriate clauses in user agreements under what conditions and controls the organization applies to device tracking.

Devices utilizing unique device identification/certificates

Devices utilizing unique device identification or have installed certificates may require additional physical protection and/or additional incident handling steps in case of device loss in order to ensure the device unique identifier or certificate is immediately revoked or disabled. Additional physical protection rules or policy would be appropriate for any device which contains access mechanisms tied to the device.

System Integrity (CJIS Policy Section 5.10)

Managing system integrity on limited function mobile operating systems may require methods and technologies significantly different from traditional full-feature operating systems. In many cases the requirements of Section 5.10 of the CJIS Security Policy cannot be met with a mobile device without the installation of a third party MDM or EMM application and supporting server infrastructure.

Patching/Updates

MDM software may provide compliance to the Section 5.10.4.1 patch management requirements for particular platforms and software versions. However, devices without ‘always-on’ cellular connections may not be reachable for extended periods of time by the MDM or EMM solution either to report status or initiate patching. Supplementary or manual device accountability methods may need to be implemented to account for devices without persistent connections to ensure their patch and update state is current. Alternatively, some patches or system updates may not be practical over cellular connections and will require connection of devices to a WiFi network. Compliance with CJIS Security Policy requirements through purely technical means may not be practical and considerations should be made for aggressive management of devices through training and mandatory periodic connection of devices to organizationally managed WiFi networks.

TECHNOLOGY NOTE: Apple and Android based devices have different potential issues regarding device operating system updates. Apple maintains support for updating the operating system on Apple hardware for several device generations (typically 3-5 years) and provides a robust mechanism for system updates. However, updates to Android based systems are driven by the individual device manufacturer which may or may not support regular updates to current Android operating system versions. Additionally, different Android device vendors may offer updates/upgrades to the Android operating system on different schedules, which can complicate environments utilizing Android devices from multiple manufacturers.

Malicious code protection/Restriction of installed applications and application permissions

MDM or EMM software will typically allow restrictions on installed applications. One of the few effective attack vectors to compromise mobile operating systems is to manipulate the device user to install a malicious application. Even though the application may be restricted from accessing

other application data, it may have some access to common data stores on the device and access to device functions (e.g. GPS, microphone, and camera) that are undesirable. Unrestricted installation of applications by the device user could pose a significant risk to the device.

Malicious code protection using traditional virus scanning software is technically infeasible on most limited function mobile operating systems that are not rooted or jailbroken. The integrated data and program separations prevent any third party installed program from accessing or 'scanning' within another application data container. Even if feasible, power and storage limitations would be prohibitive in the effect on device battery life and storage capacity on most mobile devices. However, the cryptographic separation between applications and effective application virtualization technologies built into common mobile operating systems partially compensate for the lack of traditional virus scanning technologies. Appropriately configured MDM software is capable of checking the installed applications on the device and reporting the software inventory to a central management console in a matter analogous to traditional virus scan detection of unauthorized software. This behavior is analogous to the software inventory performed by anti-virus products and can provide a high degree of confidence that only known software or applications are installed on the device. While it is theoretically possible to bypass the application sandboxing and data segregation protections to compromise a mobile device through the web browser, the attack methods required are significantly more advanced than those required for a traditional full-featured operating system. Malicious code protections on the device web browser can be enforced through the use of a properly protected web proxy which the device is configured to use as a mandatory device policy. The most common method of malicious code installation is enticing the user to manually install the malicious app which can be mitigated on organizational devices using an MDM or other application installation restrictions which prevent the user from installing unauthorized or unknown applications. Mitigation of this issue within BYOD environments may not be possible and will present a significantly enhanced risk to the device.

TECHNOLOGY NOTE: In the particular area of application installation there is a significant difference between the behavior of Apple iOS and Android platforms. Apple cryptographically restricts the way applications will execute on the device and assigns mandatory application permissions when the application code is signed prior to release on the Apple App Store for distribution. Apps on the Apple platform must conform to Apple's policy on app behavior and cannot exceed their design permissions on access to common device functions once the app has been signed and distributed. However, the Apple method does not typically advertise the precise internal permissions granted to the app to the user prior to installation. At runtime, the app is required to request user permission to access certain device functions, and the user may agree or not agree, which may introduce risk if they are unaware of what they are agreeing to allow. Unsigned or un-trusted apps are cryptographically prevented from executing on non-jailbroken iOS devices. Apple provides a mechanism for organizations to distribute custom apps within an organization with equivalent protections but all receiving devices must have a special certificate installed that will only allow official App Store and the organization custom apps to execute.

Conversely, the Android platform, while also requiring app code signing, allows for self-signed code which can be distributed by means other than an official app store and execute on any Android device. Application permissions are presented to the user once at app installation but ramifications of agreement to certain app permissions may not be obvious to a non-technical user. Permissions in the Android model require user acceptance of all app requested permissions or the app is denied

installation, which can result in unwise user acceptance of excessive permissions in order to gain functionality provided by the app.

On either platform user installation of applications can significantly change the security state of the device. Applications may be able to transmit and receive data or share device common data with other devices over the network or local WiFi or Bluetooth connection. On either platform it is highly desirable to limit allowable applications to a pre-approved pool of apps via MDM or organizational App store structures and device policy. However, the risks associated with uncontrolled app installation is several orders of magnitude greater on Android based devices.

WARNING: Rooted or jailbroken devices are modified in such a manner that the built in protections against malicious code are effectively disabled. A rooted or jailbroken device would require significant and costly compensating controls to achieve compliance.

Firewall/IDS capability

Traditional device or “personal” firewalls as identified in CJIS Security Policy Section 5.10.4.4 may not be practical on limited function mobile device operating systems but significant compensating controls are available. By default, mobile device operating systems have a limited number of system services installed and carefully controlled network access. To a certain extent the mobile operating system performs similar effective functions as a personal firewall would perform on a general purpose operating system. Potential compensating controls for the five (5) personal firewall requirements specified in Section 5.10.4.4 are listed below:

1. Manage Program Access to the Internet: On agency controlled devices with an MDM, limiting the apps installed on the device will effectively perform the same function. Since no software or apps can be installed without MDM approval a robust approval process can effectively ensure internet access is only granted to approved apps. Built-in apps and functions can also be limited on network access by the MDM.
2. Block unsolicited requests to connect to the user device: Default configurations for mobile operating system platforms typically block incoming requests. It is possible to install an app that may ‘listen’ on the network and accept connections, but the same compensating control identified in item 1 will mitigate the likelihood of that occurring.
3. Filter incoming traffic by IP address or protocol: Protocol filtering effectively occurs due to the limited function of the operating sys long as no installed application opens network access ports. The mitigations in 1 effectively compensate for this control as well.
4. Filter incoming traffic by destination ports: Same as 3.
5. Maintain an IP traffic log: This may not be technically feasible on most mobile operating system platforms as maintaining this log would require access to lower level operating system functions that are not accessible unless the device is rooted or jailbroken. However, individual Apps that communicate over the network or accept connections from the network may permit logs of IP traffic associated to that application to be stored.

Spam Protection

Spam guards installed on corporate or organizational email systems may effectively accomplish the spam protection requirements for the CJIS Security Policy on mobile devices if properly configured to block spam before delivery to the device. If no upstream spam guard is installed on the mail server the mobile devices accesses, the device may not have adequate spam protection. Additionally access to internet based email (web mail) would need to be restricted to web mail with appropriate spam and/or antivirus protections to ensure compliance.

Periodic system integrity checks

One method to compensate for the technical infeasibility of traditional anti-virus and malicious code protection is to install an MDM that performs periodic system integrity checks that validate device configuration and status against an approved baseline. Deviations may provide indicators of potential device compromise or mis-configuration.

G.5 Administrator Accounts for Least Privilege and Separation of Duties

Administrator Accounts for Least Privilege and Separation of Duties

PURPOSE:

This appendix is provided to describe industry best security practices for assigning separate administrator accounts to support the concept of Least Privilege.

ATTRIBUTION:

- SANS, "The Critical Security Controls for Effective Cyber Defense", version 5.0
- NIST SP 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations", Revision 4 dated April 2013
- NIST SP 800-12, "An Introduction to Computer Security: The NIST Handbook" dated October 1995
- CNSSI-4009, "National Information Assurance (IA) Glossary", dated April 2010

DEFINITIONS:

Least Privilege – The principle that security architecture be designed to grant individual users and processes only the minimum accesses to system resources and authorizations required to perform their official duties or function.

Separation of Duties – The security principle requiring the division of roles and responsibilities so that a single individual cannot subvert a critical process or function.

SUMMARY:

The implementation of least privilege is accomplished by assigning user or process access to system resources based on operational or business needs. Thus, access is granted to only those resources required to perform assigned duties. For individuals who have multiple roles within the organization requiring varying levels privileges, this assignment of access can be challenging. Often times the agency will assign a single userid to the individual and elevate the privileges for that account based on the different roles. While it may seem logical to allow the user access to all

required resources using a single account, security vulnerabilities can be introduced into the system.

Associated with least privilege is separation of duties. This concept aids in maintaining the integrity of the system by preventing the abuse of elevated privileges for making unauthorized changes to the system. This objective essentially requires different individuals to perform separate functions with relation to (primarily) administrative duties. For instance, those with the ability to create and assign user access to system should not be able to access the audit logs that contain the evidence of the account actions.

USER ACCESS AND ACCOUNT MANAGEMENT:

Several factors influence the manner in which an agency implements and manages user access. Many times, the size of the agency and the technical expertise of the IT staff employed by the agency become primary drivers. Larger agencies with a broad base of technically savvy personnel normally have the ability to dedicate resources specifically to the administration and management of user access. This could translate to the use of multiple accounts for a single user performing duties requiring varying levels of access.

Smaller agencies with few or no technically experienced personnel will often assign single user accounts with the highest level of access required by users. Other smaller agencies may go as far as assigning every user an account with elevated privileges so there are no delays or problems requiring intervention by already overburdened system administrators. It is not uncommon for a smaller agency to outsource system administration duties.

Regardless of the size or resources of an organization, each agency should base the process for assigning access to system resources based on their operational requirements and a thorough risk assessment. To mitigate risk for accessing system resources, industry best security practices prescribe those individuals performing duties requiring elevated privileges be assigned a separate userid to be used in the performance of those duties. This account would be separate from a standard user account.

Why are some agencies unwilling to implement controls for least privilege? One common reason/perception is administrative overhead. There is a time factor for a system administrator to create user accounts and configure those accounts correctly based on the user's role. In larger agencies with many employees, this could add up to a significant impact on the system administrator(s) especially if there is a high level of turnover. Resources in some agencies may allow for a single system administrator dedicated strictly for account management. On the other end of the spectrum, in agencies with fewer employees, the impact may be more burdensome. While there are fewer user accounts to manage, a full-time system administrator for account

management may not be feasible. Those duties then become shared between a few people or added to the duties of a lone person.

Another reason may be the burden on system administrators to remember multiple userids and passwords. This could result in the user using the same password for each account or the user writing down the credentials for ease of remembrance. Additionally, an administrator could get the credentials mixed up between accounts causing an account lockout. This could then require system administrator intervention to reset or unlock the account.

Some agencies may feel that creating additional accounts reduces system resources. Depending on the size of the agency, this could be a concern. In most cases, the number of individuals that would require a secondary account would be minimal. The impact could be limited to a slight increase in disk space usage on the systems accessed by the system administrators with the separate accounts and perhaps the server housing the account information.

THREATS:

A primary goal of attackers is to gain administrative or root privileges on a network or system. Therefore, protection of credentials with that level of access is a key to preventing unauthorized access. Attackers may use many methods in attempts to gain unauthorized, privileged access to computer or network systems. There are two common techniques that take advantage of improperly managed administrative privileges.

Phishing Attacks

In this first method, consider a small organization with limited system administrative resources. Each user is assigned an account with elevated privileges that allows them to perform a myriad of duties including gaining access to critical system security resources. Because this is the only account the user has, normal non-administrative duties are also performed with administrative rights. While checking their email, the user is fooled into reading a message and opening a malicious attachment. Because the user's account has elevated privileges, malware is now installed on the system with elevated privileges. The malware could now allow the attacker to take over the system and install other malicious software such as key loggers, sniffers, or remote control applications. Other key system resources such as firewalls, routers, switches, or intrusion detection systems are now also compromised.

Password Brute Force Guessing / Cracking

The second method may not be as easy as the first and involves the guessing or cracking of passwords on the part of the attacker. Based on human nature, we tend to develop passwords that

are easy to remember and most likely contain some kind of information that is pertinent to us. Some passwords could be easily guessed with a minimal amount of social engineering or fact finding. Consider again an agency that assigns users a single account to perform all duties including those requiring elevated privileges. A user has created a password that, while meeting the requirements of the CJIS Security Policy, is comprised of easily guessed information about the user. An attacker has previously determined the userid and is now able to begin guessing the password. Upon success, the attacker will have unauthorized access to critical system resources.

MITIGATION:

The first step to implementing least privilege is to create separate user accounts for those individuals that require elevated privileges for their duties. These duties could include system or security administration, reviewing audit logs, backup administration, or configuring network devices (e.g. firewalls, routers). The passwords associated with these accounts should have a higher level of complexity than an account without elevated privileges. By disassociating the access levels required for system administration functions from an individual's "everyday use account", should a password be compromised, access would be limited to that of a user with non-elevated privileges.

Second is to implement procedures to ensure accounts with elevated privileges are used only for those duties requiring the higher level of access. This would mean disabling or blocking access to email, web browsers, and other external facing connections. While technical processes are the preferred method of preventing the misuse of accounts with elevated privileges, written policies can be used in situations where technology does not support that type of account management.

Several governance organizations recognize the importance of the security value of Least Privilege. The Payment Card Industry (PCI) includes requirements in their Data Security Standards (DSS). The National Institute of Standards and Technology (NIST) addresses the concept of Least Privilege in its Special Publication (SP) 800-53 rev. 4. While not considered a governance organization, the System Administration, Networking, and Security (SANS) Institute publishes a list of the top 20 security controls which includes "Controlled Use of Administrator Privileges" at number 12. Although the actual security controls or required implementation may slightly differ, the concept is consistent across the groups. The actual controls from NIST and SANS are included here in this appendix.

NIST CONSIDERATIONS FOR LEAST PRIVILEGE:

NIST Special Publication 800-53 rev. 4 includes controls required for all systems under the Federal Information Security Management Act. The publication specifies the guidance for Least Privilege in the control catalog under the Access Control (AC) family and specifically as AC-6. While the NIST requirements are not enforceable under the CJIS Security Policy, they were the genesis of

the Policy and do provide a sound security baseline that can be leveraged by the criminal and noncriminal justice community. AC-6 is a key control having several enhancements which, when implemented, bolster the overall security of the information system by reducing the risk of compromise through the misuse or misconfiguration of access to system resources.

AC-6 Least Privilege

Control: The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

Supplemental Guidance: Organizations employ least privilege for specific duties and information systems. The principle of least privilege is also applied to information system processes, ensuring that the processes operate at privilege levels no higher than necessary to accomplish required organizational missions/business functions. Organizations consider the creation of additional processes, roles, and information system accounts as necessary, to achieve least privilege. Organizations also apply least privilege to the development, implementation, and operation of organizational information systems. Related controls: AC-2, AC-3, AC-5, CM-6, CM-7, PL-2.

Control Enhancements:

(1) *LEAST PRIVILEGE | AUTHORIZE ACCESS TO SECURITY FUNCTIONS*

The organization explicitly authorizes access to [Assignment: organization-defined security functions (deployed in hardware, software, and firmware) and security-relevant information].

Supplemental Guidance: Security functions include, for example, establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters. Security-relevant information includes, for example, filtering rules for routers/firewalls, cryptographic key management information, configuration parameters for security services, and access control lists. Explicitly authorized personnel include, for example, security administrators, system and network administrators, system security officers, system maintenance personnel, system programmers, and other privileged users. Related controls: AC-17, AC-18, AC-19.

Control Enhancements:

(2) *LEAST PRIVILEGE | NON-PRIVILEGED ACCESS FOR NONSECURITY FUNCTIONS*

The organization requires that users of information system accounts, or roles, with access to [Assignment: organization-defined security functions or security-relevant information], use non-privileged accounts or roles, when accessing nonsecurity functions.

Supplemental Guidance: This control enhancement limits exposure when operating from within privileged accounts or roles. The inclusion of roles addresses situations where organizations implement access control policies such as role-based access control and where a change of role provides the same degree of assurance in the change of access authorizations for both the user and all processes acting on behalf of the user as would be provided by a change between a privileged and non-privileged account. Related control: PL-4.

(3) *LEAST PRIVILEGE | NETWORK ACCESS TO PRIVILEGED COMMANDS*

The organization authorizes network access to [Assignment: organization-defined privileged commands] only for [Assignment: organization-defined compelling operational needs] and documents the rationale for such access in the security plan for the information system.

Supplemental Guidance: Network access is any access across a network connection in lieu of local access (i.e., user being physically present at the device). Related control: AC-17.

(4) *LEAST PRIVILEGE | SEPARATE PROCESSING DOMAINS*

The information system provides separate processing domains to enable finer-grained allocation of user privileges.

Supplemental Guidance: Providing separate processing domains for finer-grained allocation of user privileges includes, for example: (i) using virtualization techniques to allow additional privileges within a virtual machine while restricting privileges to other virtual machines or to the underlying actual machine; (ii) employing hardware and/or software domain separation mechanisms; and (iii) implementing separate physical domains. Related controls: AC-4, SC-3, SC-30, SC-32.

(5) *LEAST PRIVILEGE | PRIVILEGED ACCOUNTS*

The organization restricts privileged accounts on the information system to [Assignment: organization-defined personnel or roles].

Supplemental Guidance: Privileged accounts, including super user accounts, are typically described as system administrator for various types of commercial off-the-shelf operating systems. Restricting privileged accounts to specific personnel or roles prevents day-to-day users from having access to privileged information/functions. Organizations may differentiate in the application of this control enhancement between allowed privileges for local accounts and for domain accounts provided organizations retain the ability to control information system configurations for key security parameters and as otherwise necessary to sufficiently mitigate risk. Related control: CM-6.

(6) *LEAST PRIVILEGE | PRIVILEGED ACCESS BY NON-ORGANIZATIONAL USERS*

The organization prohibits privileged access to the information system by non-organizational users.

Supplemental Guidance: Related control: IA-8.

(7) *LEAST PRIVILEGE | REVIEW OF USER PRIVILEGES*

The organization:

(a) Reviews [Assignment: organization-defined frequency] the privileges assigned to [Assignment: organization-defined roles or classes of users] to validate the need for such privileges; and

(b) Reassigns or removes privileges, if necessary, to correctly reflect organizational mission/business needs.

Supplemental Guidance: The need for certain assigned user privileges may change over time reflecting changes in organizational missions/business function, environments of operation, technologies, or threat. Periodic review of assigned user privileges is necessary to determine if the rationale for assigning such privileges remains valid. If the need cannot be revalidated, organizations take appropriate corrective actions. Related control: CA-7.

(8) *LEAST PRIVILEGE | PRIVILEGE LEVELS FOR CODE EXECUTION*

The information system prevents [Assignment: organization-defined software] from executing at higher privilege levels than users executing the software.

Supplemental Guidance: In certain situations, software applications/programs need to execute with elevated privileges to perform required functions. However, if the privileges required for execution are at a higher level than the privileges assigned to organizational users invoking such

applications/programs, those users are indirectly provided with greater privileges than assigned by organizations.

(9) *LEAST PRIVILEGE | AUDITING USE OF PRIVILEGED FUNCTIONS*

The information system audits the execution of privileged functions.

Supplemental Guidance: Misuse of privileged functions, either intentionally or unintentionally by authorized users, or by unauthorized external entities that have compromised information system accounts, is a serious and ongoing concern and can have significant adverse impacts on organizations. Auditing the use of privileged functions is one way to detect such misuse, and in doing so, help mitigate the risk from insider threats and the advanced persistent threat (APT). Related control: AU-2.

(10) *LEAST PRIVILEGE | PROHIBIT NON-PRIVILEGED USERS FROM EXECUTING PRIVILEGED FUNCTIONS*

The information system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.

Supplemental Guidance: Privileged functions include, for example, establishing information system accounts, performing system integrity checks, or administering cryptographic key management activities. Non-privileged users are individuals that do not possess appropriate authorizations. Circumventing intrusion detection and prevention mechanisms or malicious code protection mechanisms are examples of privileged functions that require protection from non-privileged users.

References: None.

Priority and Baseline Allocation:

P1	LOW Not Selected	MOD AC-6 (1) (2) (5) (9) (10)	HIGH AC-6 (1) (2) (3) (5) (9) (10)

**SYSTEM ADMINISTRATION, NETWORKING, AND SECURITY (SANS)
CONSIDERATION FOR LEAST PRIVILEGE:**

There are many negative factors that affect our cyber lives: massive data loss, intellectual property theft, credit card breaches, and identity theft just to name a few. Cyber defense is rapidly evolving to address the plethora of challenges we face. Defenders have access to a wide array of resources to combat those wishing to do harm. Ranging from the collection of vast amounts of intelligence data to security standards to training and certifications, security practitioners are well armed.

But can information overload actually worsen the problem? Organizations must decide, hopefully based on risk analysis, how to wade through all available resources and select those best suited to their own operating environment. The threats continue to evolve, the attackers become smarter, and user access more mobile. The cloud beckons and can provide reduced cost and infrastructure at a price of less control and accountability for vital information.

The SANS Institute publishes the “20 Critical Security Controls for Effective Cyber Defense”. This list of controls is the combined result of work by an international community to create, adopt, and support the controls. The components of the community provide insight, tools, information, and solutions into threats and adversaries. This list includes the control titled “Controlled Use of Administrative Privileges”. SANS describes this control as: *The process and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.*

Critical Security Control (CSC) 12: Controlled Use of Administrative Privileges

The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.

ID #	Description	Category
CSC 12---1	Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.	Quick win (<i>One of the “First Five”</i>)
CSC 12---2	Use automated tools to inventory all administrative accounts and validate that each person with administrative privileges on desktops, laptops, and servers is authorized by a senior executive	Quick win
CSC 12---3	Configure all administrative passwords to be complex and contain letters, numbers, and special characters intermixed, and with no dictionary words present in the password. Pass phrases containing multiple dictionary words, along with special characters, are acceptable if they are of a reasonable length.	Quick win

CSC 12---4	Before deploying any new devices in a networked environment, change all default passwords for applications, operating systems, routers, firewalls, wireless access points, and other systems to have values consistent with administration---level accounts.	<i>Quick win</i>
CSC 12---5	Ensure that all service accounts have long and difficult--- to--- guess passwords that are changed on a periodic basis, as is done for traditional user and administrative passwords.	<i>Quick win</i>
CSC 12---6	Passwords should be hashed or encrypted in storage. Passwords that are hashed should be salted and follow guidance provided in NIST SP 800---132 or similar guidance. Files containing these encrypted or hashed passwords required for systems to authenticate users should be readable only with super---user privileges.	<i>Quick win</i>
CSC 12---7	Utilize access control lists to ensure that administrative accounts are used only for system administration activities, and not for reading e---mail, composing documents, or surfing the Internet. Web browsers and e---mail clients especially must be configured to never run as administrator.	<i>Quick win</i>
CSC 12---8	Through policy and user awareness, require that administrators establish unique, different passwords for their administrative and non---administrative accounts. Each person requiring administrative access should be given his/her own separate account. Users should only use the Windows “administrator” or UNIX “root” accounts in emergency situations. Domain administration accounts should be used when required for system administration instead of local administrative accounts.	<i>Quick win</i>
CSC 12---9	Configure operating systems so that passwords cannot be re--- used within a timeframe of six months.	<i>Quick win</i>
CSC 12---10	Configure systems to issue a log entry and alert when an account is added to or removed from a domain administrators’ group, or when a new local administrator account is added on a system.	<i>Visibility/ Attribution</i>
CSC 12---11	Configure systems to issue a log entry and alert when unsuccessful login to an administrative account is attempted.	<i>Visibility/ Attribution</i>

CSC 12---12	Use multifactor authentication for all administrative access, including domain administrative access. Multi--- factor authentication can include a variety of techniques, to include the use of smart cards with certificates, One Time Password (OTP) tokens, and biometrics.	<i>Configuration/ Hygiene</i>
CSC 12---13 (NEW)	When using certificates to enable multi---factor certificate---based authentication, ensure that the private keys are protected using strong passwords or are stored in trusted, secure hardware tokens.	<i>Configuration/ Hygiene</i>
CSC 12---14	Block access to a machine (either remotely or locally) for administrator---level accounts. Instead, administrators should be required to access a system using a fully logged and non---administrative account. Then, once logged on to the machine without administrative privileges, the administrator should transition to administrative privileges using tools such as Sudo on Linux/UNIX, RunAs on Windows, and other similar facilities for other types of systems. Users would use their own administrative accounts and enter a password each time that is different than their user account.	<i>Configuration/ Hygiene</i>

Quick win: Implementation provides significant risk reduction without major financial, procedural, architectural, or technical changes to an environment, or that provide substantial and immediate risk reduction against very common attacks that most security-aware organizations prioritize these key controls.

Visibility / attribution: Measures to improve the process, architecture, and technical capabilities of organizations to monitor their networks and computer systems to detect attack attempts, locate points of entry, identify already-compromised machines, interrupt infiltrated attackers' activities, and gain information about the sources of an attack.

Configuration / hygiene: reduce the number and magnitude of security vulnerabilities and improve the operations of networked computer systems, with a focus on protecting against poor security practices by system administrators and end-users that could give an attacker an advantage.

SEPARATION OF DUTIES:

Separation of duties is another security control related to least privilege. Many of the same challenges faced by least privilege apply to this concept as well. Agency size and resources play a major in the implementation of separation of duties. As the name implies, some key functions should be separated between different individuals. The goal of this concept is to provide protection

against a single individual's ability to circumvent system security controls to gain unauthorized access or perform unauthorized actions without colluding with other individuals.

Simply put separation of duties entails distributing certain critical mission oriented functions or system administrative support functions amongst different individuals or roles. It also includes delineating information system support duties such as auditing, configuration control, or network security between different individuals.

As with least privilege, an agency's ability to implement separation of duties is typically based on financial and personnel resources. While a very large agency may have ready availability to those resources to ensure critical functions are spread across multiple individuals, a small agency probably does not have that luxury.

THREATS:

What effect can an individual with carte blanc access to all critical functions of a system have? Consider a single individual with the ability to install nefarious applications on a system (e.g. a keylogger). If this same individual also has the ability to edit any audit logs that would have recorded the actions of installing the software, those entries could be deleted and any evidence of the installation eliminated.

Perhaps a disgruntled system administrator wants to open a port on a firewall to allow a remote backdoor connection into the information system in order to siphon off criminal justice information. Because the perpetrator has access to the firewall and all logs, the port can be opened and the logs tampered with to eliminate records of the action.

As mentioned previously, the two concepts of least privilege and separation of duties are related. Additional threats are presented when a system administrator using a single account with unlimited elevated privileges across the information system uses that account to check email. In a successful phishing attack that compromises this account, the attacker now has unrestricted unauthorized access to all system resources and the ability to hide their tracks.

MITIGATION:

The primary method to avoid these situations is to configure system privileges and duties such that a single person is unable to effect questionable change to the system and then are able to erase any evidence of the change.

Technical configurations are most secure and sound enforceable policies compliment the technical solutions. When an information system does not support separating duties, strong policies help mitigate risk.

NIST CONSIDERATIONS FOR SEPARATION OF DUTIES:

NIST Special Publication 800-53 specifies the guidance for separation of duties in the control catalog under the Access Control (AC) family and specifically as AC-5. While the NIST requirements are not enforceable under the CJIS Security Policy, they were the genesis of the Policy and do provide a sound security baseline that can be leveraged by the criminal and noncriminal justice community. AC-5 is a relatively small control with no enhancements but it is significant in protecting the integrity of an information system.

AC-5 Separation of Duties

Control: The organization:

- a. Separates [*Assignment: organization-defined duties of individuals*];
- b. Documents separation of duties of individuals; and
- c. Defines information system access authorizations to support separation of duties.

Supplemental Guidance: Separation of duties addresses the potential for abuse of authorized privileges and helps to reduce the risk of malevolent activity without collusion. Separation of duties includes, for example: (i) dividing mission functions and information system support functions among different individuals and/or roles; (ii) conducting information system support functions with different individuals (e.g., system management, programming, configuration management, quality assurance and testing, and network security); and (iii) ensuring security personnel administering access control functions do not also administer audit functions. Related controls: AC-3, AC-6, PE-3, PE-4, PS-2.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P1	LOW Not Selected	MOD AC-5	HIGH AC-5

G.6 Encryption

Encryption

Purpose:

This paper was created to provide assistance and guidance on encryption types, methods, and to provide general best practices in the implementation of encryption.

Attribution:

- FIPS 140 – 2, Security Requirements for Cryptographic Modules (May 2001)
- FIPS 197, Advanced Encryption Standard (Nov 2001)
- NIST SP 800-111, Guide to Storage Encryption Technologies for End User Devices
- CNSSP-15, National Information Assurance Policy on the Use of Public Standards for Secure Sharing of Information among Security Systems
- CJIS Security Policy

Definitions and Terms:

Encryption – A form of cryptology that applies a cryptographic operation to provide confidentiality of (sensitive) information.

Decryption – The inverse cryptographic operation used to convert encrypted information back into a plaintext (readable) format.

Asymmetric Encryption – A type of encryption that uses key pairs for encryption. One key is used to encrypt a message and another key to decrypt the message. Asymmetric encryption is also commonly known as public key encryption.

Symmetric Encryption – A type of encryption where the same key is used to encrypt and decrypt a message. Symmetric encryption is also known as secret key encryption.

Hybrid encryption – A type of encryption where both asymmetric encryption and symmetric encryption keys are used creating what is referred to as cipher suites. In a hybrid solution the asymmetric encryption keys are used for client/server certificate exchange to provide session integrity while the symmetric encryption keys are used for bulk data encryption to provide data confidentiality.

Authorized User/Personnel - An individual, or group of individuals, who have been appropriately vetted through a national fingerprint-based record check and have been granted access to CJI.

Summary:

CJIS Security Policy encryption requirements are intended to provide protection of the sensitive data that is criminal justice information (CJI). The primary goal of encrypting CJI is to prevent unauthorized access to this sensitive data. Encryption is a great tool that can be applied to accomplish this protection and ensure compliance with the vast majority of the CJI requirements. CJIS Security Policy Section 5.10.1.2 details when encryption is required and provides information on the exceptions to the encryption requirement.

Achieving CJIS Security Policy Compliance:

To determine when encryption is required one must first read and understand CJIS Security Policy Section 5.9.1 Physically Secure Location. The reason for this is simple: encryption is not required while within a physically secure location. Conversely, whenever CJI is transmitted or stored (at rest) outside the boundaries of a physically secure location encryption may be required. The exact standards to which the data would be required to meet are detailed along with any exceptions in CJIS Security Policy Section 5.10.1.2.

Additionally, both security awareness training and personnel security requirements can be affected by whether or not CJI is encrypted. Requirements surrounding these Policy areas is determined by answering the following question: Who has unescorted access to unencrypted CJI?

Unless personnel is escorted, security awareness training is required as correlated with the access level needed by personnel as identified in CJIS Security Policy Section 5.2. Similarly, fingerprint-based background checks as detailed in CJIS Security Policy Section 5.12 may be required on individuals to permit unescorted access to CJI.

The intent of all these requirements is to limit access to CJI to only authorized personnel. CJIS Security Policy Appendix A: Terms and Definitions defines authorized user/personnel as an individual, or group of individuals, who have been appropriately vetted through a national fingerprint-based record check and have been granted access to CJI.

What is Encryption?

Encryption is the process of encoding messages or information in such a manner that only people with the knowledge or means to decrypt the message can do so. But how does this work?

In an encryption process, legible data, referred to as plaintext, is encrypted by applying a cipher (otherwise known as an encryption algorithm or crypto key) to the data. The data then becomes encrypted and is now referred to as ciphertext. The ciphertext is essentially unreadable until decrypted. The decryption process requires the process of applying the same algorithm (crypto key) to encrypt the data in an inverse manner to convert the data back into plaintext.

Encryption is important because it allows you to securely protect data that you don't want anyone else to have access to. Encryption has been used throughout history to send “secrets” securely by some form of obfuscation to a recipient. Businesses and enterprises use encryption to protect corporate secrets and sensitive employee data, such as payroll information and personally identifiable information (PII). Governments secure classified information with encryption. Additionally, individuals may use encryption to protect personal information, such as credit card data, banking information, and passwords to guard against things like identity theft.

It should be known that encryption may not always prevent the interception of data. If the stolen data is encrypted, though, it would be extremely difficult for any of the data to be decrypted without having the decryption key. While it may be possible to decrypt the message without possessing the key, it does require large computational resources, great skill, and lots of time to accomplish such a task. Exercising encryption along with key management policies is one of the best security practices that can be put into place with regard to sensitive data security and protection.

Types of Encryption:

Symmetric Encryption

Symmetric encryption is also commonly known as secret key encryption. Symmetric encryption is a form of cryptography utilizing a singular encryption key to guise an electronic message. Its data conversion uses a mathematical algorithm along with a secret key, which results in the inability to make sense out of a message. Symmetric encryption is a two-way algorithm because the mathematical algorithm is reversed when decrypting the message along with using the same secret key.

Symmetric encryption is most often used for data protection whether at rest or in transit, especially in bulk, due to the ease and speed with which the encryption can be implemented. The most common examples of symmetric algorithms are: AES and Triple-DES (3DES or TDEA).

How it works:

To encrypt and send a message to Jane, John does the following:

1. Generates a new symmetric key
2. Encrypts the message using this new symmetric key
3. Sends the message to Jane
4. Sends the encrypted symmetric key to Jane - out of band

To decrypt this ciphertext, Jane does the following:

1. Receives the encrypted message
2. Receives the symmetric key
3. Uses the symmetric key to decrypt the message

Asymmetric Encryption

Asymmetric encryption is also commonly known as public-key encryption. Asymmetric cryptography is cryptography in which a pair of keys, a public key and a private key, are used to encrypt and decrypt a message so that it arrives securely. Initially, a network user receives a public and private key pair from a certificate authority. Any other user who wants to send an encrypted message can get the intended recipient's public key from a public directory. They use this key to encrypt the message, and they send it to the recipient. When the recipient gets the message, they decrypt it with their private key, which no one else should have access to.

Creating Key Pairs:

Asymmetric encryption requires the use of algorithms of great computational complexity to create the key pairs. This is accomplished by using a large, random number that an algorithm is applied to which generates a pair of keys for use as asymmetric key algorithms (as shown in Figure 1 below).

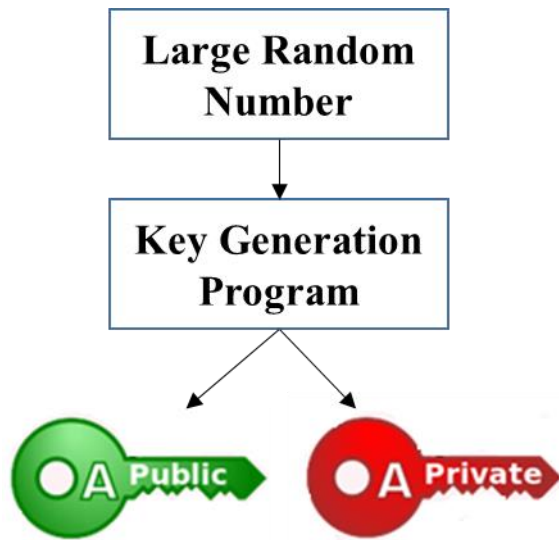


Figure 1 – Asymmetric key pair generation

Asymmetric encryption is most often used to encrypt a single message before transmission. The most common examples of asymmetric algorithms are: RSA and DSA.

How it works:

To encrypt and send a message to Jane, John does the following:

1. Obtains Jane's public key
2. Encrypts the message using Jane's public key
3. Sends the message to Jane

To decrypt this ciphertext, Jane does the following:

1. Receives the encrypted message
2. Uses her private key to decrypt the message

Advantages of Using Symmetric Encryption for Data Protection

Asymmetric encryption requires the use of algorithms with great computational complexity to create the key pairs, and therefore is not practical for large amounts of data. It is typically used for only for short messages. Also, asymmetric encryption must use a comparatively stronger key than symmetric key encryption to achieve the same level of protection as one key (public) will be published in the public directory for all to see.

Symmetric encryption is based on large, but simple algorithms which require less computation. Therefore, is much faster to create and use keys. This allows the same key to be used to encrypt and decrypt the message. So, data can be encrypted in real time. The (shared) key is sent to the recipient out of band so that it can be used to decrypt the data.

For the reasons stated above, symmetric key encryption is the preferred choice by both industry and government alike to encrypt large amounts of data (bulk encryption) simply due to the ease and real time encryption capabilities as detailed above. Additionally, a new key can be generated for every session, message transaction, etc., as desired. This means a sender won't have to use one key (public) to encrypt a message and have the recipient use another key (private) to decrypt the message.

Hybrid Encryption

Hybrid encryption solution exist where both asymmetric encryption and symmetric encryption keys are used to create what is referred to as cipher suites. In a hybrid solution the asymmetric encryption keys are used for client/server certificate exchange to provide session integrity while the symmetric encryption keys are used for bulk data encryption to provide data confidentiality.

Hybrid solutions are most often used by Internet browsers to protect data in transit. The most common examples of hybrid encryption are: TLS/SSL, PGP, IPSEC, and S/MIME.

How it works:

To encrypt a message to Jane in a hybrid cryptosystem, John does the following:

1. Obtains Jane's public key
2. Generates a new symmetric key
3. Encrypts the message using this new symmetric key
4. Encrypts the symmetric key using Jane's public key
5. Sends the message to Jane

To decrypt this hybrid cipher text, Jane does the following:

1. Receives the encrypted message
2. Receives the encrypted symmetric key
3. Uses her private key to decrypt the symmetric key
4. Uses the symmetric key to decrypt the message

Explaining Cipher Suites:

A cipher suite is a set of cryptographic algorithms used for the following:

- Protect information required to create shared keys (key exchange)
- Encrypt messages exchanged between clients and servers (bulk encryption)
- Generate message hashes and signatures to ensure the integrity of a message (message authentication)

Examples of Transport Layer Security (TLS) 1.2 Cipher Suites:

- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256

A cipher suite specifies one algorithm for each of the above tasks. For example, the TLS_RSA_WITH_AES_128_SHA256 cipher suite is used for TLS. The suite uses the RSA asymmetric algorithm for key exchange, AES with a 128-bit key for bulk data encryption, and SHA256 for message authentication.

Symmetric and Asymmetric Key Strength Comparison:

<u>Symmetric</u>		<u>Asymmetric</u>		
<u>Bits of security</u>	<u>Symmetric key algorithms</u>	<u>Finite-Field Cryptography (FFC)</u> <u>(e.g., DSA, D-H)</u> <u>Bits of security</u>	<u>Integer-Factorization Cryptography (IFC)</u> <u>(e.g., RSA)</u> <u>Bits of security</u>	<u>Elliptic-Curve Cryptography (ECC)</u> <u>(e.g., ECDSA)</u> <u>Bits of security</u>
<u>80</u>	<u>2TDEA18</u>	<u>Public key = 1024</u> <u>Private key = 160</u>	<u>Key size = 1024</u>	<u>Key size = 160-223</u>
<u>112</u>	<u>3TDEA</u>	<u>Public key = 2048</u> <u>Private key = 224</u>	<u>Key size = 2048</u>	<u>Key size = 224-255</u>
<u>128</u>	<u>AES-128</u>	<u>Public Key = 3072</u> <u>Private key = 256</u>	<u>Key size = 3072</u>	<u>Key size = 256-383</u>
<u>192</u>	<u>AES-192</u>	<u>Public key = 7680</u> <u>Private key = 384</u>	<u>Key size = 7680</u>	<u>Key size = 384-511</u>
<u>256</u>	<u>AES-256</u>	<u>Public key = 15360</u> <u>Private key = 512</u>	<u>Key size = 15360</u>	<u>Key size = 512+</u>

Figure 2 - Symmetric and asymmetric key strength comparison

As you can see in the chart provided above, the equivalent key strengths between symmetric and asymmetric key strengths do not necessarily correlate. There is a reason for this. As stated previously, asymmetric algorithms must use a comparatively stronger key than symmetric key encryption to achieve the same strength. The simplest explanation for this is because one of the keys is published to the public directory and can constantly be attacked by anyone with access to the directory. Therefore, the public key must be made of such strength that it can resist getting compromised while made public.

Federal Information Processing Standard (FIPS) 140-2 Explained

Origin of FIPS 140-2

On July 17, 1995, the National Institute of Standards and Technology (NIST) established the Cryptographic Module Validation Program (CMVP) to validate cryptographic modules to Federal Information Processing Standards (FIPS) Security Requirements for Cryptographic Modules, and other FIPS cryptography based standards. The CMVP is a joint effort between NIST and the Communications Security Establishment Canada (CSEC). FIPS 140-2, Security Requirements for Cryptographic Modules, was released on May 25, 2001 to supersede the original FIPS 140-1. Modules validated as conforming to FIPS 140-1 and FIPS 140-2 are accepted by the Federal Agencies of both countries for the protection of sensitive information.

What is FIPS 140-2?

Federal Information Processing Standard (FIPS) is a standard developed and recommended (often mandated) for use in federal-government-operated IT systems by the following two government bodies:

- The National Institute of Standards and Technology (NIST) in the United States
- The Communications Security Establishment (CSE) in Canada

FIPS 140-2 specifies the security requirements a cryptographic module must meet when utilized within a security system protecting sensitive information within information systems (computer and telecommunication systems). FIPS 140-2 specifies which encryption algorithms can be used and how encryption keys are to be generated and managed.

How does a product get certified?

Vendors of cryptographic modules can have their products tested by independent, accredited Cryptographic and Security Testing (CST) laboratories. The CST laboratories use the Derived Test

Requirements (DTR), Implementation Guidance (IG) and applicable CMVP programmatic guidance to test cryptographic modules against the applicable standards in a variety of implementations. The result of these tests are reported to NIST's Computer Security Division (CSD) and CSEC who jointly serve as the Validation Authorities for the program. These results are then reviewed and certificates would be issued if the results are determined to be acceptable.

What is the difference between being FIPS 140-2 compliant and being FIPS 140-2 certified?

It is common theme to discover a product is “FIPS compliant.” What does this mean, though? The difference between compliance and certification is not subtle. Certification requires a vast testing, verification, and validation process be performed by a CST laboratory as described in the previous section. Compliance is merely a claim stating the implementation of an encryption solution is done in accordance with the security policy related to the FIPS certification. Any claim of compliance would need to be validated and the corresponding certificate number would have to be known.

NIST has addressed related claims as shown below in their Frequently Asked Questions for the Cryptographic Module Validation Program:

A vendor makes the following claims of conformance to FIPS 140-2. Are they acceptable?

- The module has been designed for compliance to FIPS 140-2. <NO>
- Module has been pre-validated and is on the CMVP pre-validation list. <NO>
- The module will be submitted for testing. <NO>
- The module has been independently reviewed and tested to comply with FIPS 140-2. <NO>
- The module meets all the requirements of FIPS 140-2. <NO>
- The module implements FIPS Approved algorithms; including having algorithm certificates. <NO>
- The module follows the guidelines detailed in FIPS 140-2. <NO>
- The module has been validated and has received Certificate #XXXX. <YES>

A cryptographic module does not meet the requirements or conform to the FIPS 140-2 standard unless a reference can be made to the validation certificate number. The module used must also be the same version/part number as annotated on the validation certificate. Any other claims are not relevant.

To read more FAQs from NIST on FIPS certification, use the following NIST website link:
<http://csrc.nist.gov/groups/STM/cmvp/documents/CMVPFAQ.pdf>

Where can I learn more about FIPS 140-2?

For more information about the FIPS 140-2 standard, go to the following NIST website:
<http://csrc.nist.gov/cryptval/140-2.htm>

General Recommendations:

Encryption key management control is of paramount importance! Agencies should develop policies and procedures define and monitor the administrative tasks involved with protection, storage, organization, access controls and the lifecycle management of encryption keys. After all, encryption keys should not be accessible by just anyone. An encryption key management control process should ensure only authorized users have access to encryption keys. Key management is a best security practice and helps to ensure the confidentiality and integrity of CJI data and enforces key access control.

The CJIS Security Policy is a “living” document under constant review and receiving regular updates through the Advisory Policy Board (APB) process. Agencies need to always keep up to date on the latest requirements. These requirements can be found in CJIS Security Policy Section 5.10.1.2. Please contact the CJIS ISO Program anytime to address any questions or concerns about CJIS Security Policy requirements, the current APB status of CJIS Security Policy requirements, or if seeking general information or guidance.

G.7 Incident Response

Incident Response

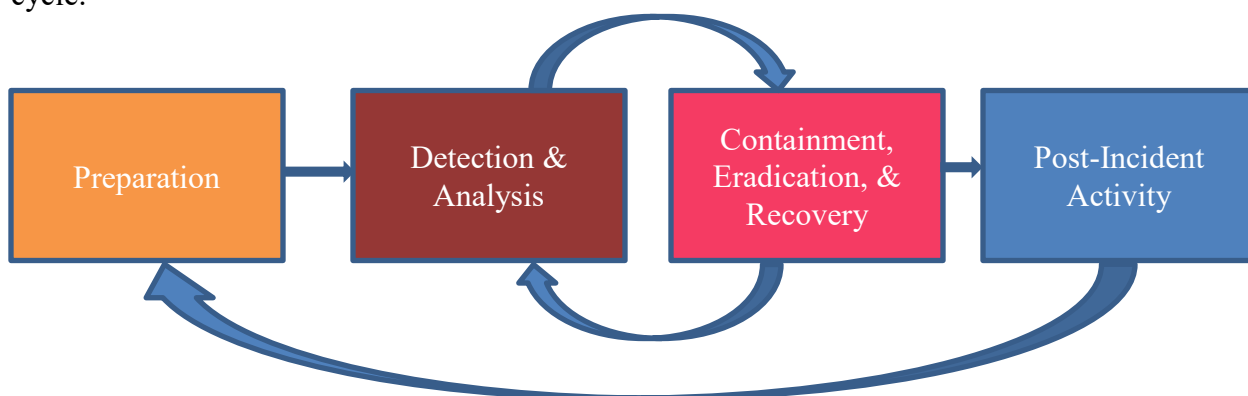
Introduction

Information technology (IT) security incident response is an important and critical component of information technology programs. Performing incident response effectively can be a complex undertaking – for that reason, establishing a successful incident response capability requires planning and resources. Everyone in an organization must be aware of IT security risks, threats, and actions to take in situations where an actual IT security incident has occurred. Even the best-secured and controlled environments can experience these security risks, threats, events, and incidents. This document provides guidelines for appropriate response to IT security incidents, and are independent of specific hardware platforms, operating systems, protocols, or applications.

The following example incidents are used to highlight appropriate actions during each phase:

- Malicious code execution
- Ransomware execution
- Denial of service attack
- Social Engineering
- Phishing

NIST Special Publication 800-61 rev. 2 outlines the “Incident Response Life Cycle” as a collection of phases – distinct sets of activities that will assist in the handling of a computer security incident, from start to finish. The following diagram explains the process flow of the incident response life cycle:



Preparation

The initial phase of the incident response life cycle, “Preparation”, involves establishing and training an incident response team, and acquiring the necessary tools and resources. A computer security incident may not have happened at this phase, but it is important to utilize all available knowledge and security measures to obtain the best posture for responding to potential future incidents. One of the most important preparation steps involves the collection, storage, and accessibility of event data and telemetry from hardware and software resources such as firewall logs, application logs, operating system logs, and other valuable sources of situational data, as well as the output of products that perform analysis on such data. Preventive measures to mitigate or eliminate future incidents are deployed during this phase, using industry best practices, data obtained from research and intelligence sources, and lessons learned from past incidents.

It is also imperative to prepare a list of contact information or notification methodologies to employ when an incident occurs, as well as notification and communication strategies within the team, with stakeholders, and with upper management and potentially other criminal justice and non-criminal justice agencies. This will help ensure that when incidents arise, the proper personnel and organizations are notified and kept informed of the circumstances regarding the incident.

Using the example incident categories outlined earlier, some overview into appropriate actions and activities for the Preparation phase can be given:

Malicious code execution

Preparation for incidents involving malicious code execution should initially involve user awareness of sources of malicious code. There are many potential sources of malicious code, such as web pages, emails, and removable media. The utilization and deployment of effective antivirus software, integrity-monitoring software, and intrusion detection and prevention software are effective measures to take to prepare for incidents involving malicious code execution.

Ransomware execution

Preparation phase activities for incidents involving ransomware execution are much the same as activities for malicious code execution, as ransomware is a specialized form of malware that encrypts potentially important or critical files, with the intention of coercing a victim to pay for a decryption key. Implementing a robust offline backup solution for these types of files is an important preparative action to take regarding the execution of ransomware. This will ensure that when ransomware attacks do happen, the mission impact is as minimal as possible and very little or no data is lost.

Denial of service attack

Denial of service attacks are given attention in the preparation phase. Defensive responses to denial of service attacks typically involve the use of a combination of attack detection and traffic classification and response tools, aiming to block traffic identified as abusive denial of service activity. Deploying solutions such as IDS/IPS devices and software, network hardware with rate-limiting capabilities (routers, switches, and firewalls), and upstream filtering devices at the system perimeter can mitigate for denial of service attacks.

Social Engineering

Preparation for social engineering attacks starts with user awareness training. Understanding and identifying attempts to obtain information in an unauthorized manner is crucial to thwarting these types of scenarios. Social engineering is the art of manipulating people to obtain information they may not be authorized to handle. Training and routinely testing users on potential social engineering scenarios and tactics, and providing training regarding appropriate responses to requests involving personal or otherwise sensitive information (for example, passwords or criminal justice information), is an effective way to ensure social engineering attacks never traverse past the preparation phase of the incident response life cycle.

Phishing

Like social engineering, preparation for phishing attacks is imperative. Phishing is a social engineering technique attackers employ to deceive users, in a fraudulent attempt to obtain sensitive information, or to gain unauthorized access to systems. Phishing is extremely widespread, and attackers disguising fraudulent scenarios in electronic communication such as email and instant messages are the most common. User awareness of these types of tactics is paramount to prepare for phishing attacks and schemes.

Detection and Analysis

The detection and analysis phase begins when a security incident has occurred. To understand when this phase begins, there must be a capability for an intelligent determination of circumstances constituting a security incident. Specialized knowledge and highly trained personnel are necessary for this step to be effective. Many organizations employ teams of personnel who are specifically trained to handle the intricacies of the incident response life cycle. The determination of a security incident can arise from one or several circumstances simultaneously – for example:

- Trained personnel manually reviewing collected event data for evidence of compromise
- Software applications analyzing events, trends, and patterns of behavior
- The observation of suspicious or anomalous activity on a computer system

The goals of this phase are:

- To detect whether a security incident occurred
- To determine the vector (i.e., method) of attack
- To determine the impact of the incident to the mission, systems, and personnel involved in the incident
- To obtain or create intelligence products regarding attack vectors and methodologies, especially when dealing with malicious code

Prioritization of incidents is also an important decision point in the incident response life cycle, as the circumstances regarding an incident can bring the situation to a critical level. There are three major impacts to consider when addressing priority of incidents:

- **Functional Impact:** the impact to business functionality
- **Information Impact:** the impact to confidentiality, integrity, and/or availability of criminal justice information
- **Recoverability:** the amount of time and resources that must be spent on recovering from an incident

Documentation regarding an incident should be thorough and applicable to the incident. This can be crucial in incidents that may lead to legal prosecution, as well as being invaluable to efficiently document, track, handle, manage, and resolve one or more incidents at the same time.

Using the example incident categories outlined earlier, some overview into appropriate actions and activities for the Detection and Analysis phase are given:

Malicious code execution

Detection of malicious code execution is often a primary job of host-based antivirus software. Having a capable and up-to-date antivirus solution installed on a system can detect known malicious code, as well as detect potentially malicious behaviors. The delivery of malicious code to a system can be detected by network traffic analysis and protection tools and hardware. Additionally, some malicious code may produce network traffic that is indicative of successful execution, exploitation, and/or compromise of a system. Solutions such as intrusion detection/prevention systems, Security Information and Event Management (SIEM) tools, and file integrity monitoring software can provide the necessary level of fidelity to make a determination of malicious code execution.

Knowing if or when a system is infected is not always immediately evident. Security controls may have been bypassed or even disabled by the malicious code. However, systems infected by malicious code or software (i.e. malware) can exhibit several indicators. These indicators include, but are not limited to:

Unexpected pop-up windows

- Slow start up and/or slow performance
- Suspicious hard drive activity including an unexpected lack of storage space
- Missing files
- Crashes and/or error messages
- Unexplained network activity
- Hijacked email

Analysis of malicious code can be performed in several ways. Static analysis of malicious code can be performed to determine the capabilities of the malicious code and generate actionable intelligence. Dynamic analysis of malicious code can be used to observe how the malicious code interacts with the system and what actions it performs and can often more rapidly determine the capabilities of malicious code. Both static and dynamic analysis can be performed manually, as well as in an automated fashion. Trained specialized personnel are crucial to the analysis of malicious code.

Ransomware execution

The detection of ransomware is identical to the detection of malicious code. Ransomware is specialized malicious code that encrypts potentially valuable files, generally with the intent to coerce a victim to pay a ransom for the possibility of the decryption of those files. Host-based antivirus solutions can also detect these threats, and network traffic analysis and protection tools and hardware can be used to prevent the successful execution of ransomware. SIEM tools and file integrity monitoring software can also detect the execution of ransomware.

Analysis of ransomware is identical to the analysis of malicious code, and the same intelligence can be determined in the same fashion as with the analysis of malicious code. The most obvious sign that ransomware has affected a system is the existence of encrypted files, the disappearance of certain types of files, and/or the presence of “ransom notes” on the system, which contain instructions for payment to obtain a decryption key, which may or may not be legitimate.

Denial of service attack

Denial of service (DoS) attacks are often detected at the perimeter of an organization but can also be detected within the organization as well. Often, from a user’s perspective, the signs of a DoS attack appear to be network performance or administrative maintenance related issues such as slow or broken network connections or down websites. Additionally, an administrator may notice ping time outs, event logs overflowing or alerts from network monitoring systems as issues that may identify a DoS attack. Intrusion detection and prevention software and platforms can detect denial of service attacks, as well as some network monitoring hardware and appliances, such as web application filters, routers,

firewalls, and switches. Devices targeted by denial of service attacks can also detect the attacks in some instances, if they have the capabilities to determine explicit attack activity versus normal network traffic.

Analysis of denial of service attacks include the determination of the source traffic, the protocols used to generate the traffic, the service(s) targeted by the attack, and the potential impacts of the attack. Network monitoring devices can often provide these types of data, with the exception of potential impacts of denial of service attacks on systems.

Social Engineering

Detection of social engineering attacks is primarily based on the situational awareness of the individual targeted by social engineering. Given that social engineering is a broad topic that can involve the manipulation and exploitation of people in control of an information system, user awareness of social engineering attempts is crucial. If the target has security awareness training in detecting attempts to gain information or access in an unapproved manner, social engineering is easier to detect.

Analysis of social engineering attacks will generally rely on the recollection abilities of or documentation taken by the targets of the attack. Social engineering may not occur on an information system and may be completely carried out in-person. If the target can recollect or produce documentation regarding the social engineering attempt, the motivation and desired access can potentially be determined. For successful social engineering attempts, recollection and documentation of the attempt is crucial to determining the level of unauthorized access that was obtained.

Phishing

Detection of phishing attacks generally will first occur at an organization's email point of presence. Some organizations still run their own email servers, and many have migrated to cloud solutions. Having an on-premise email server or server farm or cluster will require additional functionality to detect phishing attempts. For example, the header content of the email will need to be read, as well as the content inside the body of the email, to check for potentially malicious content and potentially falsified data that may indicate a phishing email. Many cloud email providers have built this capability into their email solutions, but it is still possible for users to receive phishing emails, as attacker tactics and capabilities evolve daily. The most effective detection of phishing comes from heightened situational awareness of potential attacks. Validating the source of the email can uncover potential phishing attempts.

Analysis of phishing attacks involves examination of email headers, as well as contents of the body of the email. The body of the email may contain malicious content, attachments, or links to suspicious or malicious content. Manual or automated analysis activities can be

performed on the email content. Analysis of these elements should be performed by trained specialized personnel to generate intelligence and aid with the determination of indicators of compromise.

Containment, Eradication, and Recovery

Containment activities for computer security incidents involve decision-making and the application of strategies to help control attacks and damage, cease attack activities, or reduce the impact or damage caused by the incident. Often, this requires intelligence gathered by the detection and analysis phases of the incident – for example, identification of affected hosts, identification of attacking hosts or attackers, identification of malware and its capabilities, and identification and monitoring of attacker communication channels can be invaluable to the implementation of containment activities. In most cases, it is important to introduce containment solutions all at once, as attackers may escalate their attack activity if deployment of the strategy is delayed.

Eradication efforts for a computer security incident involve removal of latent threats from systems (such as malware on the system and user accounts that may have been created), identifying and mitigating potential vulnerabilities or misconfigurations that may have been exploited, and identification of other hosts that may have been affected within the organization.

Recovery efforts for incidents involve restoration of affected systems to normal operation. This may include actions like restoring systems from backups, rebuilding systems from an agency-approved baseline, replacing compromised files with clean versions, installing patches, changing passwords, and increasing network perimeter and host-based security.

Compromised hosts are often attacked during these phases, as attackers try to regain their foothold on compromised systems or systems on the same network or others in the logical vicinity.

Malicious code execution

Containment activities for malicious code execution involve the logical or physical isolation of the host from the attacker's control and from any mission services or systems that would be impacted by the compromised host. This may include putting the host in a restricted VLAN, using firewalls to block traffic, disconnecting it from the network completely, shutting it down, or disabling functionality. Exercise caution as malicious code may have capabilities to take further actions on a host in case communications with a command and control server are severed. It is important to understand the capabilities of the malicious code before taking containment actions.

Eradication activities include the removal of malicious code from the system. This may be as simple as removing files, configuration rules, accounts, and other persistent items that the malicious code utilizes to function and maintain a presence on the system. This phase

also involves the discovery and removal of indicators of compromise on other systems, if applicable. It is imperative to remediate vulnerabilities that may have been exploited during eradication as well.

Recovery from malicious code execution generally is similar across many environments. Rebuilding the system from a clean baseline or restoring files from backup are typical activities that help restore the functionality of the system to continue the mission. Changing system passwords, installing patches, implementing tighter network access control, and ensuring appropriate levels of logging fidelity of the information system are integral parts of the recovery process.

Ransomware execution

Containment for ransomware execution should be as swift and immediate as possible, as ransomware can execute and spread to accessible media at a rapid pace. Considering files are being encrypted or have already been encrypted, immediate action should be taken to logically or physically isolate the system by disconnecting network connectivity. It is up to the system owner whether to take the risk in powering off the system, as valuable forensic artifacts may be destroyed in the process, but it will halt the execution of the ransomware and protect potentially valuable files. Please note that containment of active ransomware execution is one of the only circumstances where measures such as immediate shutdown are recommended.

Eradication of ransomware does not need to occur in most circumstances, as the entire goal of ransomware is to encrypt files and leave “recovery” instructions to extort victims. The vast majority of ransomware will delete itself once encryption of files is complete, but it is possible that some ransomware is persistent and can remain on the system. If this is the case, analysis should be performed on the ransomware to determine its capabilities, and eradication activities will proceed in an identical fashion to malicious code execution eradication activities.

Recovery from ransomware execution involves restoring encrypted files from backup and may involve the rebuilding of an entire system depending on the extent of the encryption from the ransomware. If a robust offline backup solution for hosts is not present or not utilized on a regular basis, the loss of potentially valuable data may be incredibly costly in several areas to repair, to include man-hours, revenue, and business products, data, and intelligence.

Denial of service attack

Containment of denial of service attacks involve the modification of access control where the attack is occurring. For example, if a web or application server is experiencing a denial of service attack, the system itself, as well as network monitoring devices, should be

examined to determine the source of the attack traffic. Once the source of the traffic is identified, modifications to access controls or rate-limiting features such as firewall access controls lists (ACLs) and web application filters can be employed to block the traffic. Care must be taken to determine if the observed traffic is actually intentional malicious denial of service traffic, versus heavy legitimate network traffic. Implementing access control mechanisms or rate-limiting features may negatively affect the mission of the system. It is also important to note that manual containment in this fashion may not be entirely effective, as attackers can circumvent the ACL by changing the attacking IP address, protocol, or other attribute of the connection.

Eradication is not necessarily applicable in denial of service scenarios, unless a vulnerability or misconfiguration is being exploited to cause the denial of service condition. If this is the case, take steps to remediate the vulnerability or misconfiguration.

Recovery actions depend on the available resources of the information system. For example, on-premise load balancers can be used to distribute the traffic, whether legitimate or malicious, to other less-burdened systems. Many cloud providers and content delivery networks also have denial of service mitigation capabilities. It may also be prudent to increase the resources (memory, processing capacity) of internet-facing systems so that they can handle larger amounts of traffic simultaneously.

Social Engineering

Containment regarding social engineering attacks is dependent upon the information or access that was provided to the attacker. For example, if an attacker gained access to an account on a system following a social engineering attempt, the account should be administratively disabled and all sources of event data regarding that account should be immediately collected. If sensitive data was divulged to the attacker, the impact of the exposure of that data should be examined and mitigating activity should be initiated to determine or reduce the damage of the spread of the information.

Eradication regarding social engineering attacks also depends on the information or access provided to the attacker. Removing or limiting the provided access is a pertinent eradication action. If the information provided is a credential to a system, disable and remove the credential from the system. Eradication may also involve the physical detainment or removal of personnel from a site.

Recovery actions for social engineering attacks are dependent on the information or access provided to the attacker. Additionally, security awareness training is an appropriate recovery action to ensure staff understands the threats of social engineering.

Phishing

Containment of phishing activity is tied very closely to the identification and analysis of the phishing activity. Understanding the tactics of the phishing attacker is paramount to deploying containment activities. Activities include, but are not limited to, administratively blocking sender email addresses and IPs, blocking potential malicious content in email via a web proxy, communicating with potential recipients, and implementation of email content or hyperlink blacklisting if possible. Phishing attacks can also include attempts to have users execute malicious code on systems, where containment activities regarding malicious code will be applicable.

Eradication of phishing attacks include the administrative removal of the emails from email systems, as well as eradication actions for malicious code if applicable.

Recovery from phishing attacks can include:

- Implementation and enforcement of the Domain Keys Identified Mail (DKIM) email authentication method, which can mitigate the possibility that attackers can send spoofed email
- Implementation and enforcement of Sender Policy Framework (SPF) to control and stop sender forgeries
- Implementation and enforcement of Domain-based Message Authentication, Reporting, and Conformance (DMARC), which enables message senders to indicate that their messages are protected with SPF and/or DKIM

Additionally, if malicious code is present in the phishing attack, recovery actions regarding malicious code may be applicable.

Post-Incident Activity

Post-incident activities occur after the detection, analysis, containment, eradication, and recovery from a computer security incident. Arguably one of the most important phases of incident response, post-incident activities involve the reflection, compilation, and analysis of the activities that occurred leading to the security incident, and the actions taken by those involved in the security incident, including the incident response team. Some of the important items to consider:

- Exactly what happened, and at what times?
- How well did staff and management perform in dealing with the incident?
- What information was needed sooner?
- Were any steps or actions taken that might have inhibited the recovery?
- What would the staff and management do differently the next time a similar incident occurs?

- How could information sharing with other organizations have been improved?
- What corrective actions can prevent similar actions in the future?
- What precursors or indicators should be watched for in the future to detect similar incidents?
- What additional tools or resources are needed to detect, analyze, and mitigate future incidents?

Smaller incidents, and those that are similar to others that have been well documented, do not necessarily need much focus in this phase of incident response. Larger and less-understood security incidents should be the focus of a comprehensive post-mortem evaluation that outlines many of the items listed above and should include personnel that can have a direct impact on or are directly affected or responsible for the involved systems.

Post-incident activities such as these also help to serve as training opportunities for all parties involved in the incident, from victims, to system administration personnel, to incident responders.

Malicious code execution

Post-incident activities for malicious code execution generally will follow similar patterns. A timeline of activity should have been prepared using digital forensic data collected during the detection and analysis phases of the incident. This timeline should include all affected systems and times of all activities and actions taken during the incident. Steps that victims and system administrators may have taken during the course of the incident, as well as in close proximity to the time range of the incident, are valuable items to document and discuss. Any deviation from organizational policy should be noted and taken as training items or assigned consequences in accordance with organizational policies. It may also be pertinent to ensure that appropriate information and intelligence sharing was performed during and after the incident occurred. Corrective actions that may have prevented the execution of malicious code, such as antivirus solutions, restrictions on where executables can run, tightened permissions, and script blockers for browsers, should be considered as a mitigation for the risks posed by malicious code threats. Web proxy blocks from information discovered during analysis can be utilized to ensure that malicious hosts are not contacted.

Ransomware execution

Post-incident activities for ransomware execution include all the activities involved with malicious code execution, with the addition of ensuring the functionality of a robust offline backup solution. An offline backup solution ensures that backup data is kept inaccessible to ransomware threats and is available if ransomware is successfully executed. A functional and frequent (such as daily incremental and weekly full) backup process helps ensure that business continuity is maintained in the event of issues and incidents.

Denial of service attack

Denial of service post-incident activities should include a timeline of traffic activities, as well as organizational responses to the attack traffic as well as the timeline of any business impacts and the damage associated with the impacts. Any attack precursors should be investigated and noted, and intelligence implemented to notify personnel and potentially take action as soon as attack traffic is observed. Impacts on affected systems should be noted, and a consensus should be reached on whether the systems should be upgraded or supplemented with load-balancing capabilities.

Social Engineering

Post-incident activities for social engineering incidents should include a timeline that includes all applicable activities, such as points of contact, narratives from the parties involved, CCTV footage (if applicable), system and network log files, and physical access control logging data. If unauthorized access was obtained, the impact of the access should be assessed and mitigating factors should be identified for inclusion to reduce the risk of future incidents (such as multifactor authentication, physical locks, greater CCTV coverage, improved physical access control, etc.). Security awareness training should be imperative if policy was breached, and information or access was given to unauthorized parties.

Phishing

Phishing post-incident activities should also include a timeline of actions taken since the phishing email was received, to include descriptions of the type of phishing campaign observed (malicious code, financial exploitation, credential harvesting, etc.), malicious attachments contained (if any), malicious or suspicious links in the body of emails, as well as narratives from recipients of the email and any potential victims, either self-reported or discovered through email, network, or host-based monitoring. If malicious code was included in the campaign, typical post-incident activities involving malicious code should be considered as well. Training opportunities can often arise from phishing attacks, whether successful or not, that can be valuable in giving employees better situational awareness regarding phishing.

The CJIS Security Policy requires each agency with access to CJI to establish operational incident handling procedures (i.e. a local policy). Gleaning from the requirements in Section 5.3 Incident Response, the local policy may include the following elements:

- Overall incident handling procedures. This section describes and identifies the processes used locally how the agency successfully prepares for, manages, and recovers from an incident. It includes sections on:
 - Preparation
 - Detection and Analysis
 - Containment

- Recovery
 - User response activities
- How the agency performs incident reporting. This section describes the process of notifying internal and external partners when an incident has occurred and how the incident is documented. It includes sections on:
 - Internal and external points of contact
 - Required tracking and reporting documents
 - Escalation procedures
- Incident management procedures. This section describes the agency's approach to a consistent and repeatable approach to managing incidents. It includes sections on:
 - Roles and responsibilities
 - Incident-related information collection
 - Updating policies with lessons learned
 - Collection of evidence
 - Incident response training
 - Document and artifact retention

G.8 Secure Coding

Secure Coding

This appendix documents a source of information on best practices and standards for secure coding. With the increased use of software products and the rapid pace of modern software development, it is essential to discover and resolve insecure software risks. The mitigations and guidelines to reduce these common risks can be found in secure coding best practices.

Understanding how software applications work can be a daunting thing; however, it could be key to know if data security is in jeopardy. Awareness of secure coding practices allows an agency to review potential vendors and their products prior to purchase and implementation. It also empowers the agency with the knowledge of the questions to ask a vendor of how the software was developed and whether the vendor uses secure coding practices or standards.

Additionally, the information in this appendix can provide a path forward for agencies with the internal capability to produce “in-house” software applications. By implementing security during the code writing process, security is “baked in” and there is more trust the software will aid in protecting the information it processes.

Open Web Application Security Project (OWASP) Foundation

The OWASP Foundation is a not-for-profit charitable organization focused on improving the security of software. OWASP operates as a community of like-minded professionals to provide unbiased and practical information about application security (AppSec) through software tools and documentation. These materials are available under a free and open software license, which can be located at the link below.

https://www.owasp.org/index.php/Main_Page

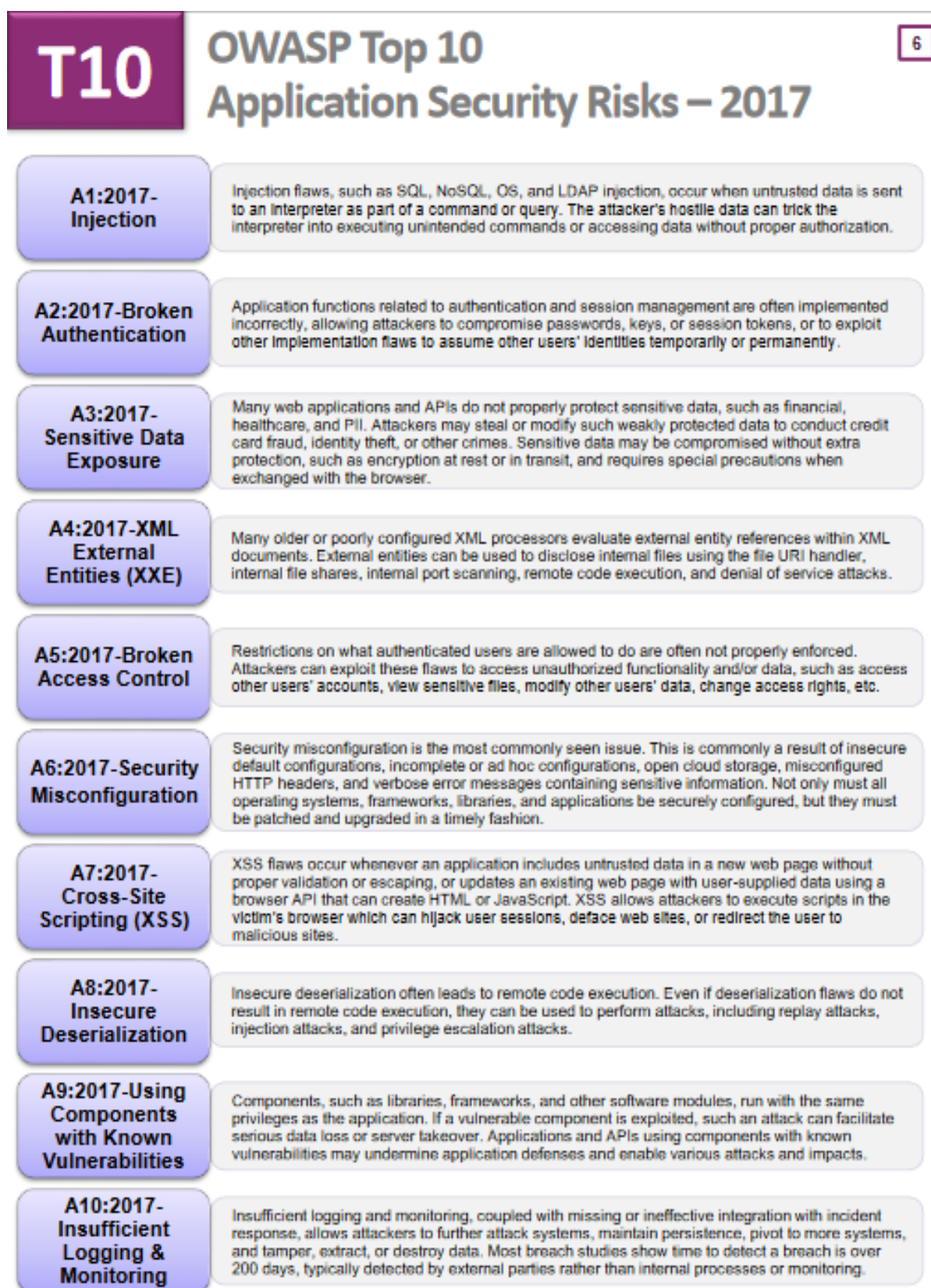
Software is becoming increasingly complex and connected, and the difficulty of achieving application security increases exponentially. The rapid pace of modern software development processes makes the most common risks essential to discover and resolve quickly and accurately.

The OWASP Foundation publishes the Top 10 Application Security Risks, which focus on the most serious web application security risks. The OWASP Top 10 is based primarily on 40 plus data submissions from firms that specialize in application security and an industry survey that was completed by over 500 individuals. This data spans vulnerabilities gathered from hundreds of organizations and over 100,000 real world applications and application program interfaces (API). The Top 10 items are selected and prioritized according to this data, in combination with consensus estimates of exploitability, detectability, and impact.

A primary aim of the OWASP Top 10 is to educate developers, designers, architects, managers, and organizations about the consequences of the most common and most important web application security weaknesses. The Top 10 provides basic techniques to protect against these high risks problem areas, and provides guidance on a path forward.

The OWASP Top 10 focuses on identifying the most serious web application security risks for a broad array of organizations. For each of these risks, generic information about likelihood and technical impact using the following simple ratings scheme, which is based on the OWASP Risk Rating Methodology.

Figure G.8-A



Each organization is unique, and so are the threat actors for that organization, their goals, and the impact of any breach. It is critical to understand the risk to your organization based on applicable threat agents and business impacts.

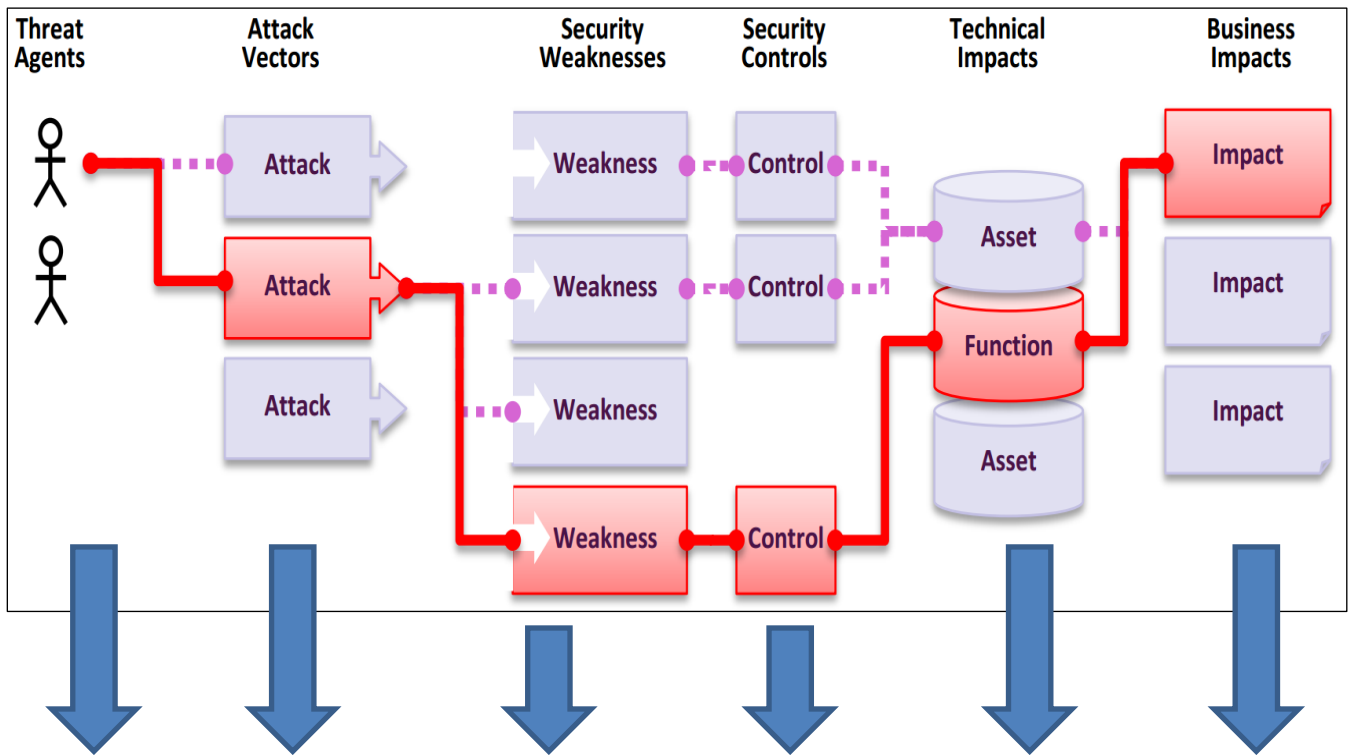
Application Security Risks

The figures immediately below illustrate the path of a sample threat beginning with the threat agent and ending with the target or affected business resource. Various paths are available but the agent would normally select the path of least resistance which would be the most vulnerable and with the fewest number of effective security controls.

The sample risk matrix can be used to assign in the various aspects of potential vulnerability. Each column corresponds to a phase in the attack process. In the matrix, a lower value represents less risk and is more desirable.

Concerning secure coding practices, when security is built-in during code development, vulnerabilities can be identified and controls included reducing the overall risk to information processed by the code.

Figure G.8-B Sample Threat Path



Threat Agents	Exploitability	Weakness Prevalence	Weakness Detectability	Technical Impacts	Business Impacts
App Specific	EASY: 3	WIDESPREAD: 3	EASY: 3	SEVERE: 3	App / Business Specific
	AVERAGE: 2	COMMON: 2	AVERAGE: 2	MODERATE: 2	
	DIFFICULT: 1	UNCOMMON: 1	DIFFICULT: 1	MINOR: 1	

Figure G.8-C General Risk Matrix

To understand these risks for a particular application or organization, you must consider your own specific threat agents and business impacts. Even severe software weaknesses may not present a serious risk if there are no threat agents in a position to perform the necessary attack or the business impact is negligible for the assets involved. The following table presents a summary of the 2017 Top 10 Application Security Risks, and the risk factors that have been assigned to each risk.

Figure G.8-D Top 10 Risk Factor Summary

RISK							Score
	Threat Agents	Exploitability	Prevalence	Detectability	Technical	Business	
A1:2017-Injection	App Specific	EASY: 3	COMMON: 2	EASY: 3	SEVERE: 3	App Specific	8.0
A2:2017-Authentication	App Specific	EASY: 3	COMMON: 2	AVERAGE: 2	SEVERE: 3	App Specific	7.0
A3:2017-Sens. Data Exposure	App Specific	AVERAGE: 2	WIDESPREAD: 3	AVERAGE: 2	SEVERE: 3	App Specific	7.0
A4:2017-XML External Entities (XXE)	App Specific	AVERAGE: 2	COMMON: 2	EASY: 3	SEVERE: 3	App Specific	7.0
A5:2017-Broken Access Control	App Specific	AVERAGE: 2	COMMON: 2	AVERAGE: 2	SEVERE: 3	App Specific	6.0
A6:2017-Security Misconfiguration	App Specific	EASY: 3	WIDESPREAD: 3	EASY: 3	MODERATE: 2	App Specific	6.0
A7:2017-Cross-Site Scripting (XSS)	App Specific	EASY: 3	WIDESPREAD: 3	EASY: 3	MODERATE: 2	App Specific	6.0
A8:2017-Insecure Deserialization	App Specific	DIFFICULT: 1	COMMON: 2	AVERAGE: 2	SEVERE: 3	App Specific	5.0
A9:2017-Vulnerable Components	App Specific	AVERAGE: 2	WIDESPREAD: 3	AVERAGE: 2	MODERATE: 2	App Specific	4.7
A10:2017-Insufficient Logging&Monitoring	App Specific	AVERAGE: 2	WIDESPREAD: 3	DIFFICULT: 1	MODERATE: 2	App Specific	4.0

Whether you are new to web application security or already very familiar with these risks, the task of producing a secure web application or fixing an existing one can be difficult. If you have to manage a large application portfolio, this task can be daunting.

To help organizations, developers, testers and managers reduce their application security risks in a cost-effective manner; OWASP has produced numerous free and open resources that you can use to address application security in your organization. The following are some of the many resources OWASP has produced to help organizations produce secure web applications and APIs.

Get Started:

- Document all applications and associated data assets.
- Larger organizations should consider implementing a Configuration Management Database (CMDB).
- Establish an application security program to conduct analysis to define key improvement areas and an execution plan.

Risk Based Portfolio Approach:

- Identify the protection needs of your application portfolio from a business perspective.
- Establish a common risk-rating model with a consistent set of likelihood and impact factors reflective of your organization's tolerance for risk.
- Measure and prioritize all applications and APIs and add results to CMDB.

Enable with a Strong Foundation:

- Establish a set of policies and standards that provide an application security baseline for all development teams to adhere to.
- Define a common set of reusable security controls that complement these policies and standards and provide design and development guidance on their use.

Integrate Security into Existing Processes:

- Define and integrate secure implementation and verification activities into existing development and operational processes.
 - Activities include threat modeling, secure design and design review, secure coding and code review, penetration testing, and remediation.

Application Security Requirements - to produce a secure web application, you must define what secure means for that application.

- [Application Security Verification Standard \(ASVS\):](https://www.owasp.org/index.php/ASVS)
<https://www.owasp.org/index.php/ASVS>
- [OWASP Secure Software Contract Annex:](https://www.owasp.org/index.php/OWASP_Secure_Software_Contract_Annex)
https://www.owasp.org/index.php/OWASP_Secure_Software_Contract_Annex

Application Security Architecture - retrofitting security into your applications and APIs, it is far more cost effective to design the security in from the start.

- OWASP Prevention Cheat Sheets:

https://www.owasp.org/index.php/OWASP_Cheat_Sheet_Series

Standard Security Controls - building strong and usable security controls is difficult. Using a set of standard security controls radically simplifies the development of secure applications and APIs.

- OWASP Proactive Controls:
https://www.owasp.org/index.php/OWASP_Proactive_Controls

Secure Development Lifecycle - to improve the process your organization follows when building applications and APIs, organizations formulate and implement a strategy for software security that is tailored to the specific risks facing their organization.

- OWASP Software Assurance Maturity Model (SAMM):
https://www.owasp.org/index.php/OWASP_SAMM_Project
- OWASP Application Security Guide for CISOs:
https://www.owasp.org/index.php/Application_Security_Guide_For_CISOs

Application Security Education – hands-on learning about vulnerabilities to help educate developers on web application security.

- OWASP Education Project:
https://www.owasp.org/index.php/Category:OWASP_Education_Project
- OWASP WebGoat:
<https://www.owasp.org/index.php/WebGoat>
- OWASP Broken Web Application Project:
https://www.owasp.org/index.php/OWASP_Broken_Web_Applications_Project

Understand the Threat Model – be sure to understand the priorities when it comes to threat model.

- OWASP Testing Guide:
https://www.owasp.org/index.php/OWASP_Testing_Project
- [Application Security Verification Standard \(ASVS\):](https://www.owasp.org/index.php/ASVS)
<https://www.owasp.org/index.php/ASVS>

Testing Strategies – choose the simplest, fastest, most accurate technique to verify each requirement.

- OWASP Security Knowledge Framework:
https://www.owasp.org/index.php/OWASP_Security_Knowledge_Framework

- [Application Security Verification Standard \(ASVS\):
https://www.owasp.org/index.php/ASVS](https://www.owasp.org/index.php/ASVS)

APPENDIX H SECURITY ADDENDUM

The following pages contain:

The legal authority, purpose, and genesis of the Criminal Justice Information Services Security Addendum (H2-H4);

An example of a contract addendum (H-5);

The Security Addendum itself (H6-H7);

The Security Addendum Certification page (H8).

**FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES
SECURITY ADDENDUM**

**Legal Authority for and Purpose and Genesis of the
Security Addendum**

Traditionally, law enforcement and other criminal justice agencies have been responsible for the confidentiality of their information. Accordingly, until mid-1999, the Code of Federal Regulations Title 28, Part 20, subpart C, and the National Crime Information Center (NCIC) policy paper approved December 6, 1982, required that the management and exchange of criminal justice information be performed by a criminal justice agency or, in certain circumstances, by a noncriminal justice agency under the management control of a criminal justice agency.

In light of the increasing desire of governmental agencies to contract with private entities to perform administration of criminal justice functions, the FBI sought and obtained approval from the United States Department of Justice (DOJ) to permit such privatization of traditional law enforcement functions under certain controlled circumstances. In the Federal Register of May 10, 1999, the FBI published a Notice of Proposed Rulemaking, announcing as follows:

1. Access to CHRI [Criminal History Record Information] and Related Information, Subject to Appropriate Controls, by a Private Contractor Pursuant to a Specific Agreement with an Authorized Governmental Agency To Perform an Administration of Criminal Justice Function (Privatization). Section 534 of title 28 of the United States Code authorizes the Attorney General to exchange identification, criminal identification, crime, and other records for the official use of authorized officials of the federal government, the states, cities, and penal and other institutions. This statute also provides, however, that such exchanges are subject to cancellation if dissemination is made outside the receiving departments or related agencies. Agencies authorized access to CHRI traditionally have been hesitant to disclose that information, even in furtherance of authorized criminal justice functions, to anyone other than actual agency employees lest such disclosure be viewed as unauthorized. In recent years, however, governmental agencies seeking greater efficiency and economy have become increasingly interested in obtaining support services for the administration of criminal justice from the private sector. With the concurrence of the FBI's Criminal Justice Information Services (CJIS) Advisory Policy Board, the DOJ has concluded that disclosures to private persons and entities providing support services for criminal justice agencies may, when subject to appropriate controls, properly be viewed as permissible disclosures for purposes of compliance with 28 U.S.C. 534.

We are therefore proposing to revise 28 CFR 20.33(a)(7) to provide express authority for such arrangements. The proposed authority is similar to the authority that already exists in 28 CFR 20.21(b)(3) for state and local CHRI systems. Provision of CHRI under this authority would only be permitted pursuant to a specific agreement with an authorized governmental agency for the purpose of providing services for the administration of criminal justice. The agreement would be required to incorporate a security addendum approved by the Director of the FBI (acting for the Attorney General). The security

addendum would specifically authorize access to CHRI, limit the use of the information to the specific purposes for which it is being provided, ensure the security and confidentiality of the information consistent with applicable laws and regulations, provide for sanctions, and contain such other provisions as the Director of the FBI (acting for the Attorney General) may require. The security addendum, buttressed by ongoing audit programs of both the FBI and the sponsoring governmental agency, will provide an appropriate balance between the benefits of privatization, protection of individual privacy interests, and preservation of the security of the FBI's CHRI systems.

The FBI will develop a security addendum to be made available to interested governmental agencies. We anticipate that the security addendum will include physical and personnel security constraints historically required by NCIC security practices and other programmatic requirements, together with personal integrity and electronic security provisions comparable to those in NCIC User Agreements between the FBI and criminal justice agencies, and in existing Management Control Agreements between criminal justice agencies and noncriminal justice governmental entities. The security addendum will make clear that access to CHRI will be limited to those officers and employees of the private contractor or its subcontractor who require the information to properly perform services for the sponsoring governmental agency, and that the service provider may not access, modify, use, or disseminate such information for inconsistent or unauthorized purposes.

Consistent with such intent, Title 28 of the Code of Federal Regulations (C.F.R.) was amended to read:

§ 20.33 Dissemination of criminal history record information.

- a) Criminal history record information contained in the Interstate Identification Index (III) System and the Fingerprint Identification Records System (FIRS) may be made available:
 - 1) To criminal justice agencies for criminal justice purposes, which purposes include the screening of employees or applicants for employment hired by criminal justice agencies.
 - 2) To noncriminal justice governmental agencies performing criminal justice dispatching functions or data processing/information services for criminal justice agencies; and
 - 3) To private contractors pursuant to a specific agreement with an agency identified in paragraphs (a)(1) or (a)(6) of this section and for the purpose of providing services for the administration of criminal justice pursuant to that agreement. The agreement must incorporate a security addendum approved by the Attorney General of the United States, which shall specifically authorize access to criminal history record information, limit the use of the information to the purposes for which it is provided, ensure the security and confidentiality of the information consistent with these regulations, provide for sanctions, and contain such other provisions as the Attorney General may require. The power

and authority of the Attorney General hereunder shall be exercised by the FBI Director (or the Director's designee).

This Security Addendum, appended to and incorporated by reference in a government-private sector contract entered into for such purpose, is intended to insure that the benefits of privatization are not attained with any accompanying degradation in the security of the national system of criminal records accessed by the contracting private party. This Security Addendum addresses both concerns for personal integrity and electronic security which have been addressed in previously executed user agreements and management control agreements.

A government agency may privatize functions traditionally performed by criminal justice agencies (or noncriminal justice agencies acting under a management control agreement), subject to the terms of this Security Addendum. If privatized, access by a private contractor's personnel to NCIC data and other CJIS information is restricted to only that necessary to perform the privatized tasks consistent with the government agency's function and the focus of the contract. If privatized the contractor may not access, modify, use or disseminate such data in any manner not expressly authorized by the government agency in consultation with the FBI.

EXAMPLE OF A CONTRACT ADDENDUM

AMENDMENT NO. ____ TO THE CONTRACT BETWEEN
[PARTY NO. 1] AND [PARTY NO. 2], ENTERED INTO [DATE]

[Name of Law Enforcement Agency] and [Party No. 2], upon notification and pursuant to Paragraph/Section No. ____ [the amendment clause of the original contract] of that certain contract entered into by these parties on [date][and entitled "____"], hereby amend and revise the contract to include the following:

1. Access to and use of criminal history record information and other sensitive information maintained in [state and] FBI-managed criminal justice information systems by [private party] are subject to the following restrictions:

- a.
- b.
- c.

and

d. The Security Addendum appended hereto, which is incorporated by reference and made a part thereof as if fully appearing herein.

This amendment is effective the ____ day of _____, 20__.

On behalf of [Party No. 1]: _____

[Name]

[Title]

Date

On behalf of [Party No. 2]: _____

[Name]

[Title]

FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES
SECURITY ADDENDUM

The goal of this document is to augment the CJIS Security Policy to ensure adequate security is provided for criminal justice systems while (1) under the control or management of a private entity or (2) connectivity to FBI CJIS Systems has been provided to a private entity (contractor). Adequate security is defined in Office of Management and Budget Circular A-130 as “security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.”

The intent of this Security Addendum is to require that the Contractor maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

This Security Addendum identifies the duties and responsibilities with respect to the installation and maintenance of adequate internal controls within the contractual relationship so that the security and integrity of the FBI's information resources are not compromised. The security program shall include consideration of personnel security, site security, system security, and data security, and technical security.

The provisions of this Security Addendum apply to all personnel, systems, networks and support facilities supporting and/or acting on behalf of the government agency.

1.00 Definitions

1.01 Contracting Government Agency (CGA) - the government agency, whether a Criminal Justice Agency or a Noncriminal Justice Agency, which enters into an agreement with a private contractor subject to this Security Addendum.

1.02 Contractor - a private business, organization or individual which has entered into an agreement for the administration of criminal justice with a Criminal Justice Agency or a Noncriminal Justice Agency.

2.00 Responsibilities of the Contracting Government Agency.

2.01 The CGA will ensure that each Contractor employee receives a copy of the Security Addendum and the CJIS Security Policy and executes an acknowledgment of such receipt and the contents of the Security Addendum. The signed acknowledgments shall remain in the possession of the CGA and available for audit purposes. The acknowledgement may be signed by hand or via digital signature (see glossary for definition of digital signature).

3.00 Responsibilities of the Contractor.

3.01 The Contractor will maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed and all subsequent versions), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

4.00 Security Violations.

4.01 The CGA must report security violations to the CJIS Systems Officer (CSO) and the Director, FBI, along with indications of actions taken by the CGA and Contractor.

4.02 Security violations can justify termination of the appended agreement.

4.03 Upon notification, the FBI reserves the right to:

- a. Investigate or decline to investigate any report of unauthorized use;
- b. Suspend or terminate access and services, including telecommunications links. The FBI will provide the CSO with timely written notice of the suspension. Access and services will be reinstated only after satisfactory assurances have been provided to the FBI by the CGA and Contractor. Upon termination, the Contractor's records containing CHRI must be deleted or returned to the CGA.

5.00 Audit

5.01 The FBI is authorized to perform a final audit of the Contractor's systems after termination of the Security Addendum.

6.00 Scope and Authority

6.01 This Security Addendum does not confer, grant, or authorize any rights, privileges, or obligations on any persons other than the Contractor, CGA, CJA (where applicable), CSA, and FBI.

6.02 The following documents are incorporated by reference and made part of this agreement: (1) the Security Addendum; (2) the NCIC 2000 Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20. The parties are also subject to applicable federal and state laws and regulations.

6.03 The terms set forth in this document do not constitute the sole understanding by and between the parties hereto; rather they augment the provisions of the CJIS Security Policy to provide a minimum basis for the security of the system and contained information and it is understood that there may be terms and conditions of the appended Agreement which impose more stringent requirements upon the Contractor.

6.04 This Security Addendum may only be modified by the FBI, and may not be modified by the parties to the appended Agreement without the consent of the FBI.

6.05 All notices and correspondence shall be forwarded by First Class mail to:

Information Security Officer

Criminal Justice Information Services Division, FBI

1000 Custer Hollow Road

Clarksburg, West Virginia 26306

**FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES
SECURITY ADDENDUM**

CERTIFICATION

I hereby certify that I am familiar with the contents of (1) the Security Addendum, including its legal authority and purpose; (2) the NCIC Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20, and agree to be bound by their provisions.

I recognize that criminal history record information and related data, by its very nature, is sensitive and has potential for great harm if misused. I acknowledge that access to criminal history record information and related data is therefore limited to the purpose(s) for which a government agency has entered into the contract incorporating this Security Addendum. I understand that misuse of the system by, among other things: accessing it without authorization; accessing it by exceeding authorization; accessing it for an improper purpose; using, disseminating or re-disseminating information received as a result of this contract for a purpose other than that envisioned by the contract, may subject me to administrative and criminal penalties. I understand that accessing the system for an appropriate purpose and then using, disseminating or re-disseminating the information received for another purpose other than execution of the contract also constitutes misuse. I further understand that the occurrence of misuse does not depend upon whether or not I receive additional compensation for such authorized activity. Such exposure for misuse includes, but is not limited to, suspension or loss of employment and prosecution for state and federal crimes.

Printed Name/Signature of Contractor Employee

Date

Printed Name/Signature of Contractor Representative

Date

Organization and Title of Contractor Representative

APPENDIX I REFERENCES

White House Memo entitled “Designation and Sharing of Controlled Unclassified Information (CUI)”, May 9, 2008

[CJIS RA] *CJIS Security Policy Risk Assessment Report*; August 2008; For Official Use Only; Prepared by: Noblis; Prepared for: U.S. Department of Justice, Federal Bureau of Investigation, Criminal Justice Information Services Division, 1000 Custer Hollow Road, Clarksburg, WV 26306

[CNSS Instruction No. 4009] *National Information Assurance (IA) Glossary*; Committee on National Security Systems (CNSS) Instruction No. 4009; 26 April 2010

[FBI SA 8/2006] *Federal Bureau of Investigation, Criminal Justice Information Services, Security Addendum*; 8/2006; Assistant Director, Criminal Justice Information Services, FBI, 1000 Custer Hollow Road, Clarksburg, West Virginia 26306

[FISMA] *Federal Information Security Management Act of 2002*; House of Representatives Bill 2458, Title III–Information Security

[FIPS 199] *Standards for Security Categorization of Federal Information and Information Systems*; Federal Information Processing Standards Publication, FIPS PUB 199; February 2004

[FIPS 200] *Minimum Security Requirements for Federal Information and Information Systems*; Federal Information Processing Standards Publication, FIPS PUB 200; March 2006

[FIPS 201] *Personal Identity Verification for Federal Employees and Contractors*; Federal Information Processing Standards Publication, FIPS PUB 201-1

[NIST SP 800–14] *Generally Accepted Principles and Practices for Securing Information Technology Systems*; NIST Special Publication 800–14

[NIST SP 800–25] *Federal Agency Use of Public Key Technology for Digital Signatures and Authentication*; NIST Special Publication 800–25

[NIST SP 800–30] *Risk Management Guide for Information Technology Systems*; NIST Special Publication 800–36

[NIST SP 800–32] *Introduction to Public Key Technology and the Federal PKI Infrastructure*; NIST Special Publication 800–32

[NIST SP 800–34] *Contingency Planning Guide for Information Technology Systems*; NIST Special Publication 800–34

[NIST SP 800–35] *Guide to Information Technology Security Services*; NIST Special Publication 800–35

[NIST SP 800–36] *Guide to Selecting Information Technology Security Products*; NIST Special Publication 800–36

[NIST SP 800–39] *Managing Risk from Information Systems, An Organizational Perspective*; NIST Special Publication 800–39

[NIST SP 800–40] *Procedures for Handling Security Patches*; NIST Special Publication 800–40

- [NIST SP 800–44] *Guidelines on Securing Public Web Servers*; NIST Special Publication 800–44
- [NIST SP 800–45] *Guidelines on Electronic Mail Security*; NIST Special Publication 800–45, Version 2
- [NIST SP 800–46] *Security for Telecommuting and Broadband Communications*; NIST Special Publication 800–46
- [NIST SP 800–48] *Wireless Network Security: 802.11, Bluetooth, and Handheld Devices*; NIST Special Publication 800–48
- [NIST SP 800–52] *Guidelines on the Selection and Use of Transport Layer Security*; NIST Special Publication 800–52
- [NIST SP 800–53] *Recommended Security Controls for Federal Information Systems*; NIST Special Publication 800–53, Revision 2
- [NIST SP 800–53A] *Guide for Assessing the Security Controls in Federal Information Systems, Building Effective Security Assessment Plans*; NIST Special Publication 800–53A
- [NIST SP 800–58] *Security Considerations for Voice over IP Systems*; NIST Special Publication 800–58
- [NIST SP 800–60] *Guide for Mapping Types of Information and Information Systems to Security Categories*; NIST Special Publication 800–60, Revision 1, DRAFT
- [NIST SP 800–63–1] *Electronic Authentication Guideline*; NIST Special Publication 800–63–1; DRAFT
- [NIST SP 800–64] NIST Special Publication 800–64
- [NIST SP 800–66] *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA)*; NIST Special Publication 800–66
- [NIST SP 800–68] *Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist*; NIST Special Publication 800–68
- [NIST SP 800–70] *Security Configuration Checklists Program for IT Products*; NIST Special Publication 800–70
- [NIST SP 800–72] *Guidelines on PDA Forensics*; NIST Special Publication 800–72
- [NIST SP 800–73] *Integrated Circuit Card for Personal Identification Verification*; NIST Special Publication 800–73; Revision 1
- [NIST SP 800–76] *Biometric Data Specification for Personal Identity Verification*; NIST Special Publication 800–76
- [NIST SP 800–77] *Guide to IPSec VPNs*; NIST Special Publication 800–77
- [NIST SP 800–78] *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*; NIST Special Publication 800–78
- [NIST SP 800–81] *Secure Domain Name System (DNS) Deployment Guide*; NIST Special Publication 800–81
- [NIST SP 800–84] *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*; NIST Special Publication 800–84

- [NIST SP 800–86] *Guide to Integrating Forensic Techniques into Incident Response*; NIST Special Publication 800–86
- [NIST SP 800–87] *Codes for the Identification of Federal and Federally Assisted Agencies*; NIST Special Publication 800–87
- [NIST SP 800–96] *PIV Card / Reader Interoperability Guidelines*; NIST Special Publication 800–96
- [NIST SP 800–97] *Guide to IEEE 802.11i: Robust Security Networks*; NIST Special Publication 800–97
- [NIST SP 800–121] *Guide to Bluetooth Security*, NIST Special Publication 800-121
- [NIST SP 800–124] *Guidelines on Cell Phone and PDA Security*, NIST Special Publication 800-124
- [NIST SP 800-125] *Guide to Security for Full Virtualization Technologies*; NIST Special Publication 800-125
- [NIST SP 800–144] *Guidelines on Security and Privacy in Public Cloud Computing*; NIST Special Publication 800-144
- [NIST SP 800–145] *The NIST Definition of Cloud Computing*; NIST Special Publication 800-145
- [NIST SP 800–146] *Cloud Computing Synopsis and Recommendations*; NIST Special Publication 800-146
- [OMB A–130] *Management of Federal Information Resources*; Circular No. A–130; Revised; February 8, 1996
- [OMB M–04–04] *E-Authentication Guidance for Federal Agencies*; OMB Memo 04–04; December 16, 2003
- [OMB M–06–15] *Safeguarding Personally Identifiable Information*; OMB Memo 06–15; May 22, 2006
- [OMB M–06–16] *Protection of Sensitive Agency Information*; OMB Memo 06–16; June 23, 2006
- [OMB M–06–19] *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*; OMB Memo 06–19; July 12, 2006
- [OMB M–07–16] *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*; OMB Meme 07–16; May 22, 2007
- [Surviving Security] *Surviving Security: How to Integrate People, Process, and Technology*; Second Edition; 2004
- [USC Title 5, Section 552] *Public information; agency rules, opinions, orders, records, and proceedings*; United States Code, Title 5 - Government Agency and Employees, Part I - The Agencies Generally, Chapter 5 - Administrative Procedure, Subchapter II - Administrative Procedure, Section 552. Public information; agency rules, opinions, orders, records, and proceedings

[USC Title 44, Section 3506] *Federal Information Policy*; 01/02/2006; United States Code,
Title 44 - Public Printing and Documents; Chapter 35 - Coordination of
Federal Information Policy; Subchapter I - Federal Information Policy, Section
3506

APPENDIX J NONCRIMINAL JUSTICE AGENCY SUPPLEMENTAL GUIDANCE

This appendix is not intended to be used in lieu of the CJIS Security Policy (CSP) but rather should be used as supplemental guidance specifically for those Noncriminal Justice Agencies (NCJA) with access to Criminal Justice Information (CJI) as authorized by legislative enactment or federal executive order to request civil fingerprint-based background checks for licensing, employment, or other noncriminal justice purposes, via their State Identification Bureau (SIB) and/or Channeling agency. Examples of the target audience for the Appendix J supplemental guidance include school boards, banks, medical boards, gaming commissions, alcohol and tobacco control boards, social services agencies, pharmacy boards, etc.

The CSP is the minimum standard policy used by both criminal and noncriminal justice agencies requiring access to CJI maintained by the FBI CJIS Division. The essential premise of the CSP is to provide appropriate controls to protect the full lifecycle of CJI, whether at rest or in transit. The CSP provides guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of CJI. This Policy applies to every individual—contractor, private entity, noncriminal justice agency representative, or member of a criminal justice entity—with access to, or who operate in support of, criminal justice services and information.

For those NCJAs new to the CSP and Advisory Policy Board (APB) auditing process (all NCJAs will be periodically audited by the CJIS Systems Agency (CSA)/SIB and may be included in a sampling of triennial audits conducted by the FBI) it is strongly recommended that each system processing CJI should be individually reviewed to determine which CSP requirements may apply. In the interim however this supplemental guidance provides a minimum starting point that every NCJA processing CJI can immediately put into place. Once the broader array of security controls are gleaned for a specific system, agencies can then leverage the (already implemented) controls described in this appendix as a launching pad towards full policy compliance.

The following information is organized to provide the section and section title within the CSP, along with a brief summary and background on the guidance itself. For the specific “shall” statement please go to the referenced section within the main body of the CSP.

General CJI Guidance

The following information provides NCJAs guidance to maintain security compliance when setting up any system capable of sending and/or receiving CJI:

a. 3.2.9 – Local Agency Security Officer (LASO)

It is the responsibility of the CJIS Systems Officer (CSO) to ensure each agency having access to CJI has someone designated as the Local Agency Security Officer (LASO) per CSP Section 3.2.2(2e).

The LASO serves as the primary point of contact (POC) between the local NCJA and their respective CSA CSO or Information Security Officer (ISO) who interfaces with the FBI CJIS Division. The LASO actively represents their agency in all matters pertaining to information security, disseminates information security alerts and other material to their constituents, maintains information security documentation (including system configuration data), assists with Information Security audits of hardware and

procedures, and keeps the CSA (i.e., CSO or ISO) informed as to any information security needs and problems.

b. 5.1.1.6 – Agency User Agreements

When an NCJA (private or public) is permitted to request civil fingerprint-based background checks, with the full consent of the individual to whom a background check is taking place, for noncriminal justice functions as authorized pursuant to federal law or state statute approved by the U.S. Attorney General, the information received from the background check, such as criminal history record information (CHRI) or personally identifiable information (PII), must be protected as CJI. In order to receive access to CJI the NCJA must enter into a signed written agreement, i.e., an agency user agreement, with the appropriate signatory authority of the CSA, SIB, or authorized agency providing the CJI access. An example of a NCJA (private) is a local bank. An example of a NCJA (public) is a county school board.

Note 1: The CSA, SIB, or authorized agency providing the CJI access term should be part of the agency user agreement.

Note 2: Any NCJA that directly accesses FBI CJIS must allow the FBI to periodically test the ability to penetrate the FBI's network through the external network connection or system.

c. 5.1.3 – Secondary Dissemination

Secondary dissemination is the promulgation of CJI from a releasing agency to an authorized recipient agency that has not been previously identified in a formal information exchange agreement.

If CHRI is released to another authorized agency, that is not part of the releasing agency's primary information exchange agreement(s), the releasing agency must log such dissemination.

d. 5.2.1.1 – All Personnel (Security Awareness Training)

Basic security awareness training is required for all personnel who have access to CJI within six months of initial assignment, and biennially thereafter. CSP Section 5.2.1.1 describes the topics that must be addressed within baseline security awareness training for all authorized personnel with access to CJI.

Note: The CSO/SIB may accept the documentation of the completion of security awareness training from another agency. Accepting such documentation from another agency means that the accepting agency assumes the risk that the training may not meet a particular requirement or process required by federal, state, or local laws.

e. 5.3 – Incident Response

CSP Section 5.3 assists agencies with response and reporting procedures for accidental and malicious computer and network attacks. The requirements within Section 5.3 will help NCJAs with:

- (i) Establishing an operational incident handling capability for agency information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and,
- (ii) Tracking, documenting, and reporting incidents to appropriate agency officials and/or authorities.

CSP Section 5.3.1 describes the requirements for reporting security events and describes the responsibilities of the FBI CJIS Division and the CSA ISO.

CSP Section 5.3.2 describes the requirements for managing security incidents, to include: incident handling and the collection of evidence.

CSP Section 5.3.3 describes the requirement for an agency to ensure general incident response roles responsibilities are included as part of required security awareness training.

CSP Section 5.3.4 describes the requirement for an agency to track and document information system security incidents on an ongoing basis.

Note 1: CSA ISOs serve as the POC on security-related issues for their respective agencies and must ensure LASOs institute the CSA incident response reporting procedures at the local level. The CSA ISO shall maintain completed security incident reporting forms until the subsequent FBI triennial audit or until legal action (if warranted) is complete; whichever time-frame is greater.

Note 2: CSP Appendix F contains a sample incident notification letter for use when communicating the details of an incident to the FBI CJIS ISO.

f. 5.4 – Auditing and Accountability

CSP Section 5.4 assists agencies in assessing the inventory of components that compose their information systems to determine which security controls are applicable to the various components and implement required audit and accountability controls.

CSP Section 5.4.1 describes the required parameters for agencies to generate audit records and content for defined events and periodically review and update the list of agency-defined auditable events.

CSP Section 5.4.2 describes the requirement for agencies to provide alerts to appropriate agency officials in the event of an audit processing failure, such as software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.

CSP Section 5.4.3 describes the requirements for audit review/analysis frequency and to designate an individual or position to review/analyze information system audit records for indications of inappropriate or unusual activity, investigate suspicious activity or suspected violations, to report findings to appropriate officials, and to take necessary actions.

CSP Section 5.4.4 describes the requirement to establish information system time stamp parameters for use in audit record generation.

CSP Section 5.4.5 describes the requirement to protect audit information and audit tools from modification, deletion and unauthorized access.

CSP Section 5.4.6 describes the requirement for an agency to retain audit records for at least one (1) year.

Note: The agency will continue to retain audit records for longer than one (1) year until it is determined they are no longer needed for administrative, legal, audit, or other operational purposes - for example, retention and availability of audit records relative

to Freedom of Information Act (FOIA) requests, subpoena, and law enforcement actions.

CSP Section 5.4.7 describes the requirements for logging National Crime Information Center (NCIC) and Interstate Identification Index (III) transactions. A log must be maintained for a minimum of one (1) year on all NCIC and III transactions. The III portion of the log will clearly identify both the operator and the authorized receiving agency. III logs must also clearly identify the requester and the secondary recipient. The identification on the log will take the form of a unique identifier that shall remain unique to the individual requester and to the secondary recipient throughout the minimum one (1) year retention period.

g. 5.8 – Media Protection

CJIS Security Policy Section 5.8 assists agencies to document and implement media protection policy and procedures required to ensure that access to electronic and physical media in all forms is restricted to authorized individuals for securely handling, transporting and storing media.

“Electronic media” is electronic storage media, such as memory devices in laptops and computers (hard drives) and any removable, transportable digital memory media, such as magnetic tape or disk, optical disk, flash drives, external hard drives, or digital memory card. “Physical media” refers to CJI in physical form, e.g. printed documents, printed imagery, etc.

CSP Section 5.8.1 describes the requirement for agencies to securely store electronic and physical media within physically secure locations or controlled areas and restrict access to electronic and physical media to authorized individuals. If physical and personnel restrictions are not feasible then the data must be encrypted per CSP Section 5.10.1.2.

CSP Section 5.8.2 describes the requirements for agencies to protect and control both electronic and physical media during transport outside of controlled areas and restrict the activities associated with transport of such media to authorized personnel. The agency is responsible for implementing controls to protect electronic media containing CJI while in transport (physically moved from one location to another) to help prevent compromise of the data. Encryption, as defined in CSP Section 5.10.1.2, is the optimal control; however, if encryption of the data isn’t possible then each agency must institute other controls to ensure the security of the data.

CSP Section 5.8.3 describes the requirements for agencies to maintain written documentation of the steps taken to sanitize or destroy electronic media. Agencies must sanitize (electronically overwrite the data at least three times) or degauss electronic media prior to disposal or release for reuse by unauthorized individuals. This sanitization or destruction needs to be witnessed or carried out only by authorized personnel. Inoperable electronic media must be destroyed (cut up, shredded, etc.).

CSP Section 5.8.4 describes the requirements for physical media to be securely disposed of when no longer required, using established formal procedures. Physical media must be destroyed by shredding or incineration. This disposal or destruction needs to be witnessed or carried out only by authorized personnel.

h. 5.9 Physical Protection

CSP Section 5.9 explains the physical protection policy and procedures that are required to ensure CJI and information system hardware, software, and media are physically protected through access control measures.

CSP Section 5.9.1 details the requirements for establishing a Physically Secure Location - a facility, a criminal justice conveyance, an area, a room, or a group of rooms within a facility with both the physical and personnel security controls sufficient to protect CJI and associated information systems. Sections 5.9.1.1 – 5.9.1.8 describe the physical control requirements that must be implemented in order to establish a physically secure location.

CSP Section 5.9.2 details the requirements for establishing a Controlled Area. The controlled area is an area, a room, or a storage container established for the purpose of day-to-day CJI access, storage, or processing in the event an agency is unable to meet all of the controls required for establishing a physically secure location. Access to the controlled area needs to be restricted to only authorized personnel whenever CJI is processed. The CJI material needs to be locked away when unattended to prevent unauthorized and unintentional access. Additionally, the encryption standards of CSP Section 5.10.1.2 apply to the electronic storage (i.e. data “at rest”) of CJI.

i. 5.11 – Formal Audits

CSP Section 5.11 explains the formal audit process to help agencies understand the audit procedures.

CSP Section 5.11.1 details the requirements for compliance and security audits by the FBI CJIS Division. The FBI CJIS Division is authorized to conduct audits, once every three (3) years as a minimum, to assess agency compliance with applicable statutes, regulations and policies.

The CJIS Audit Unit (CAU) will conduct triennial audits of each CSA in order to verify compliance with applicable statutes, regulations and policies. This audit includes a sample of Criminal Justice Agency (CJA) and NCJAs, in coordination with the SIB.

Note 1: Audits may be conducted on a more frequent basis if the audit reveals that an agency has not complied with applicable statutes, regulations and policies.

Note 2: The FBI CJIS Division has the authority to conduct unannounced security inspections and scheduled audits of Contractor facilities.

CSP Section 5.11.2 describes the requirements for the CSA to triennially audit all CJAs and NCJAs with direct access to the state system, establish a process to periodically audit all NCJAs with access to CJI, establish the authority to conduct unannounced security inspections and scheduled audits of Contractor facilities.

CSP Section 5.11.3 describes the requirement that all agencies with access to CJI must permit an inspection team to conduct an appropriate inquiry and audit of any alleged security violations. The inspection team, appointed by the APB, will include at least one representative of the CJIS Division. All results of the inquiry and audit will be reported to the APB with appropriate recommendations.

Agencies located within states having passed legislation authorizing or requiring civil fingerprint-based background checks for personnel with access to criminal history record

information for the purposes of licensing or employment need to follow the guidance in Section 5.12 (referenced below).

j. 5.12 – Personnel Security

CSP Section 5.12 provides agencies the security terms and requirements as they apply to all personnel who have unescorted access to unencrypted CJI, including individuals with only physical or logical access to devices that store, process or transmit unencrypted CJI.

CSP Section 5.12.1 details the minimum screening requirements for all individuals requiring unescorted access to unencrypted CJI.

CSP Section 5.12.2 describes the requirement for an agency to immediately terminate CJI access for an individual upon termination of employment.

CSP Section 5.12.3 describes the requirement for an agency to review CJI access authorizations and initiate appropriate actions (such as closing and establishing accounts and changing system access authorizations) whenever personnel are reassigned or transferred to other positions within the agency.

CSP Section 5.12.4 describes the requirement for an agency to employ a formal sanctions process for personnel failing to comply with established information security policies and procedures.

Agencies located within states that have not passed legislation authorizing or requiring civil fingerprint-based background checks are exempted from this requirement until such time as appropriate legislation has been written into law.

The following scenarios are intended to help the reader identify areas within the CSP that NCJAs may often come across. Each scenario should be reviewed for applicability in conjunction with the above General CJI Guidance section. The specific requirements found with the CSP are not shown; however specific sections are referenced along with a requirements summary.

Hard Copy CJI Storage and Accessibility

When an NCJA receives CJI via a paper copy from a CJA and stores the paper within a locked file cabinet, the NCJA should, in addition to the General CJI Guidance, focus on compliance with policy section:

a. 4.2.4 – Storage

When storing CJI, appropriate administrative, technical, and physical safeguards must be implemented to ensure the security and confidentiality of the information.

Electronic CJI Storage and Accessibility – Controlled Area

When an NCJA creates an electronic copy of CJI (e.g. scanning a document or creation of a spreadsheet) and subsequently stores this static CJI on either a local hard drive or shared network drive in a controlled area for indirect access by Authorized Recipients, the NCJA should, in addition to the General CJI Guidance, focus on compliance with policy section:

a. 5.5.2.4 (3) – Access Control – Encryption

CSP Section 5.5.2.4 item 3 – Encryption describes the requirement for utilizing encryption as the primary access control mechanism which is necessary in this situation. Encrypted information can only be read by personnel possessing the

appropriate cryptographic key (e.g., passphrase) to decrypt. Refer to Section 5.10.1.2 for specific encryption requirements.

Electronic CJI Storage and Accessibility – Physically Secure Location

When an NCJA receives or creates an electronic copy of CJI and subsequently stores this CJI within a Records Management System (RMS), located within a physically secure location that may be queried by Authorized Recipients, the NCJA should, in addition to the General CJI Guidance, focus on compliance with policy sections:

a. **5.5 – Access Control**

CSP Section 5.5 describes the requirements and parameters for utilizing access control mechanisms for restricting CJI access (such as the reading, writing, processing and transmission of CJIS information) and the modification of information systems, applications, services and communication configurations allowing access to CJI to only authorized personnel.

b. **5.6 – Identification and Authentication**

CSP Section 5.6 describes the requirements and parameters agencies must implement to validate and authenticate the identity of information system users and processes acting on behalf of users the identities prior to granting access to CJI or agency information systems/services that process CJI.

c. **5.7 – Configuration Management**

CSP Section 5.7 describes the requirements for implementing access restrictions that will only permit authorized and qualified individuals access to information system components for purposes of initiating changes, including upgrades, and modifications.

CSP Section 5.7.1 describes the requirements for implementing the concept of least privilege (5.7.1.1) and for developing and maintaining network diagrams (5.7.1.2) that detail how the RMS is interconnected and protected within the network. See Appendix C for sample network diagrams.

CSP Section 5.7.2 details the requirement for agencies to protect the system documentation from unauthorized access consistent with the provisions described in Section 5.5 Access Control.

d. **5.10 – System and Communications Protection and Information Integrity**

CSP Section 5.10 details the requirements for network infrastructures within physically secure locations through establishment of system and communication boundary and transmission protection safeguards that assist in securing an agency's environment, even when virtualized. In addition, this section describes the requirements for providing the capability to ensure system integrity through the detection and protection against unauthorized changes to software and information for applications, services, and information systems.

Use Case Scenarios

1. Indirect Access to Criminal Justice Information (CJI) Stored on a Network Server

A county board of education is converting all employee records, including background check information containing CJI, to an electronic format. The records will be scanned from hard copy to electronic files and placed on network server that has indirect access to CJI and is located in a secure data center within the board of education offices. The data center meets all the requirements to be labeled a physically secure location as defined in Section 5.9.1 of the CSP.

Keeping in mind the scenario as described, an authorized user needs access to an employee's electronic record. This user is not located in the secure data center and will have to use remote access to access the file. The user is therefore required to provide identification and authentication credentials to prove they are an authorized user. To access the record, the user is prompted to enter their unique username and password. Because the record resides on a system with indirect access to CJI (does not allow the user to query a state or national criminal record repository), AA is not required to access the record.

NOTE: If the Authorized User has direct access to CJI (the ability to query a state or national criminal record repository) in the above scenario, AA would be required.

2. Encryption for Data at Rest (Exemption for FIPS 140-2 Certified Encryption)

A county board of education is converting all employee records, including background check information containing CJI, to an electronic format. The records will be scanned from hard copy to electronic files and placed on network server that is not located in a secure data center. Because the data center does not meet the requirements of a physically secure location, as defined in Section 5.9.1 of the CSP, the files, at rest (in storage) on the server, are required to be encrypted.

To prevent unauthorized access, the IT staff has decided to encrypt the entire folder that contains the files. They will use a product that provides an advanced encryption standard (AES) encryption algorithm at 256 bit strength to comply with the CSP and employ a CSP compliant passphrase to lock the folder's encryption. When an authorized user needs to access an employee's record, they access the folder on the server and are prompted to enter the designated passphrase to decrypt (unlock) the folder. The user can then access all files within the folder.

NOTE: Whenever authorized personnel no longer require access to the encrypted folder, the passphrase must be changed to prevent future access by that user.

APPENDIX K CRIMINAL JUSTICE AGENCY SUPPLEMENTAL GUIDANCE

This appendix is not intended to be used in lieu of the CJIS Security Policy (CSP) but rather should be used as supplemental guidance specifically for those Criminal Justice Agencies (CJA) that have historically not been subject to audit under the CJIS Security Policy guidelines. The target audience typically gains access to CJI via fax, hardcopy distribution or voice calls; does not have the capability to query state or national databases for criminal justice information; and may have been assigned an originating agency identifier (ORI) but is dependent on other agencies to run queries on their behalf. This guidance is not intended for criminal justice agencies covered under an active information exchange agreement with another agency for direct or indirect connectivity to the state CJIS Systems Agency (CSA) – in other words those agencies traditionally identified as “terminal agencies”.

The CSP is the minimum standard policy used by both criminal and noncriminal justice agencies requiring access to criminal justice information (CJI) maintained by the FBI CJIS Division. The essential premise of the CSP is to provide appropriate controls to protect the full lifecycle of CJI, whether at rest or in transit. The CSP provides guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of CJI. This Policy applies to every individual—contractor, private entity, noncriminal justice agency representative, or member of a criminal justice entity—with access to, or who operate in support of, criminal justice services and information.

For those CJAs new to the CSP it is strongly recommended that each system processing CJI should be individually reviewed to determine which CSP requirements may apply. In the interim however this supplemental guidance provides a minimum starting point that every CJA processing CJI can immediately put into place. Once the broader array of security controls are gleaned for a specific system, agencies can then leverage the (already implemented) controls described in this appendix as a launching pad towards full policy compliance.

The following information is organized to provide the section and section title within the CSP, along with a brief summary and background on the guidance itself. For the specific “shall” statement please go to the referenced section within the main body of the CSP.

General CJI Guidance

The following information provides CJAs guidance to maintain security compliance when setting up any system capable of sending and/or receiving CJI:

a. 3.2.9 – Local Agency Security Officer (LASO)

It is the responsibility of the CJIS Systems Officer (CSO) to ensure each agency having access to CJI has someone designated as the Local Agency Security Officer (LASO) per CSP Section 3.2.2(2e).

The LASO serves as the primary point of contact (POC) between the local CJA and their respective CSA CSO or Information Security Officer (ISO) who interfaces with the FBI CJIS Division. The LASO actively represents their agency in all matters pertaining to information security, disseminates information security alerts and other material to their constituents, maintains information security documentation (including system configuration data), assists with Information Security audits of hardware and procedures, and keeps the CSA (i.e., CSO or ISO) informed as to any information security needs and problems.

b. 5.1.1.3 – Criminal Justice Agency User Agreements

Any CJA receiving access to CJI must enter into a signed agreement with the CSA providing the access. The agreement specifies the services and systems the agency will access. It must also specify all pertinent governance policies to which the agency must adhere.

c. 5.1.3 – Secondary Dissemination

Secondary dissemination is the promulgation of CJI from a releasing agency to an authorized recipient agency that has not been previously identified in a formal information exchange agreement.

If CHRI is released to another authorized agency, that is not part of the releasing agency's primary information exchange agreement(s), the releasing agency must log such dissemination.

d. 5.2 – Security Awareness Training

Basic security awareness training is required for all personnel who have access to CJI within six months of initial assignment, and biennially thereafter. CSP Section 5.2.1.1 describes the topics that must be addressed within baseline security awareness training for all authorized personnel with access to CJI.

CSP Section 5.2.1.2 describes the topics required to be discussed for personnel that have both physical and logical access to CJI. These topics are covered in addition to the ones addressed in basic security awareness training.

CSP Section 5.2.1.3 describes topics to be covered for those personnel assigned information technology roles. Topics covered in this section are in addition to the topics addressed in Sections 5.2.1.1 and 5.2.1.2.

Note: The CSO may accept the documentation of the completion of security awareness training from another agency. Accepting such documentation from another agency means that the accepting agency assumes the risk that the training may not meet a particular requirement or process required by federal, state, or local laws.

e. 5.3 – Incident Response

CSP Section 5.3 assists agencies with response and reporting procedures for accidental and malicious computer and network attacks. The requirements within Section 5.3 will help CJAs with:

- (iii) Establishing an operational incident handling capability for agency information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and,
- (iv) Tracking, documenting, and reporting incidents to appropriate agency officials and/or authorities.

CSP Section 5.3.1 describes the requirements for reporting security events and describes the responsibilities of the FBI CJIS Division and the CSA ISO.

CSP Section 5.3.2 describes the requirements for managing security incidents, to include: incident handling and the collection of evidence.

CSP Section 5.3.3 describes the requirement for an agency to ensure general incident response roles responsibilities are included as part of required security awareness training.

CSP Section 5.3.4 describes the requirement for an agency to track and document information system security incidents on an ongoing basis.

Note 1: CSA ISOs serve as the POC on security-related issues for their respective agencies and must ensure LASOs institute the CSA incident response reporting procedures at the local level. The CSA ISO shall maintain completed security incident reporting forms until the subsequent FBI triennial audit or until legal action (if warranted) is complete; whichever time-frame is greater.

Note 2: CSP Appendix F contains a sample incident notification letter for use when communicating the details of an incident to the FBI CJIS ISO.

f. 5.4 – Auditing and Accountability

CSP Section 5.4 assists agencies in assessing the inventory of components that compose their information systems to determine which security controls are applicable to the various components and implement required audit and accountability controls.

CSP Section 5.4.1 describes the required parameters for agencies to generate audit records and content for defined events and periodically review and update the list of agency-defined auditable events.

CSP Section 5.4.2 describes the requirement for agencies to provide alerts to appropriate agency officials in the event of an audit processing failure, such as software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.

CSP Section 5.4.3 describes the requirements for audit review/analysis frequency and to designate an individual or position to review/analyze information system audit records for indications of inappropriate or unusual activity, investigate suspicious activity or suspected violations, to report findings to appropriate officials, and to take necessary actions.

CSP Section 5.4.4 describes the requirement to establish information system time stamp parameters for use in audit record generation.

CSP Section 5.4.5 describes the requirement to protect audit information and audit tools from modification, deletion and unauthorized access.

CSP Section 5.4.6 describes the requirement for an agency to retain audit records for at least one (1) year.

Note: The agency will continue to retain audit records for longer than one (1) year until it is determined they are no longer needed for administrative, legal, audit, or other operational purposes - for example, retention and availability of audit records relative to Freedom of Information Act (FOIA) requests, subpoena, and law enforcement actions.

CSP Section 5.4.7 describes the requirements for logging National Crime Information Center (NCIC) and Interstate Identification Index (III) transactions. A log must be maintained for a minimum of one (1) year on all NCIC and III transactions. The III portion of the log will clearly identify both the operator and the authorized receiving agency. III logs must also clearly identify the requester and the secondary recipient.

The identification on the log will take the form of a unique identifier that shall remain unique to the individual requester and to the secondary recipient throughout the minimum one (1) year retention period.

g. 5.8 – Media Protection

CJIS Security Policy Section 5.8 assists agencies to document and implement media protection policy and procedures required to ensure that access to digital and physical media in all forms is restricted to authorized individuals for securely handling, transporting and storing media.

“Digital media” is electronic storage media, such as memory devices in laptops and computers (hard drives) and any removable, transportable digital memory media, such as magnetic tape or disk, optical disk, flash drives, external hard drives, or digital memory card. “Physical media” refers to CJI in physical form, e.g. printed documents, printed imagery, etc.

CSP Section 5.8.1 describes the requirement for agencies to securely store digital and physical media within physically secure locations or controlled areas and restrict access to electronic and physical media to authorized individuals. If physical and personnel restrictions are not feasible then the data must be encrypted per CSP Section 5.10.1.2.

CSP Section 5.8.2 describes the requirements for agencies to protect and control both digital and physical media during transport outside of controlled areas and restrict the activities associated with transport of such media to authorized personnel. The agency is responsible for implementing controls to protect electronic media containing CJI while in transport (physically moved from one location to another) to help prevent compromise of the data. Encryption, as defined in CSP Section 5.10.1.2, is the optimal control; however, if encryption of the data isn’t possible then each agency must institute other controls to ensure the security of the data.

CSP Section 5.8.3 describes the requirements for agencies to maintain written documentation of the steps taken to sanitize or destroy digital media. Agencies must sanitize (electronically overwrite the data at least three times) or degauss electronic media prior to disposal or release for reuse by unauthorized individuals. This sanitization or destruction needs to be witnessed or carried out only by authorized personnel. Inoperable electronic media must be destroyed (cut up, shredded, etc.).

CSP Section 5.8.4 describes the requirements for physical media to be securely disposed of when no longer required, using established formal procedures. Physical media must be destroyed by shredding or incineration. This disposal or destruction needs to be witnessed or carried out only by authorized personnel.

h. 5.9 Physical Protection

CSP Section 5.9 explains the physical protection policy and procedures that are required to ensure CJI and information system hardware, software, and media are physically protected through access control measures.

CSP Section 5.9.1 details the requirements for establishing a Physically Secure Location - a facility, a police vehicle, an area, a room, or a group of rooms within a facility with both the physical and personnel security controls sufficient to protect CJI and associated information systems. Sections 5.9.1.1 – 5.9.1.8 describe the physical control requirements that must be implemented in order to establish a physically secure location.

CSP Section 5.9.2 details the requirements for establishing a Controlled Area. The controlled area is an area, a room, or a storage container established for the purpose of day-to-day CJI access, storage, or processing in the event an agency is unable to meet all of the controls required for establishing a physically secure location. Access to the controlled area needs to be restricted to only authorized personnel whenever CJI is processed. The CJI material needs to be locked away when unattended to prevent unauthorized and unintentional access. Additionally, the encryption standards of CSP Section 5.10.1.2 apply to the electronic storage (i.e. data “at rest”) of CJI.

i. 5.10 – System and Communications Protection and Information Integrity

CSP Section 5.10 explains the technical safeguards ranging from boundary and transmission protection to security an agency’s virtualized environment.

CSP Section 5.10.1.2 details the requirements for the encryption of CJI whether in transit or at rest. FIPS 140-2 certification is required when CJI is in transit outside a physically secure location. When at rest outside a physically secure location, encryption methods can use Advanced Encryption Standard (AES) at 256 bit strength or a FIPS 140-2 certified method.

CSP Section 5.10.3 explains the use of virtualization and partitioning when processing CJI in a virtual environment. A virtualized environment can be configured such that those parts of the system which process CJI are either physically or virtually separated from those that do not.

CSP Section 5.10.4 explains system and information integrity policy and procedures. This includes areas such as patch management, malicious code protection, and spam and spyware protection.

j. 5.11 – Formal Audits

CSP Section 5.11 explains the formal audit process to help agencies understand the audit procedures.

CSP Section 5.11.1 details the requirements for compliance and security audits by the FBI CJIS Division. The FBI CJIS Division is authorized to conduct audits, once every three (3) years as a minimum, to assess agency compliance with applicable statutes, regulations and policies.

The CJIS Audit Unit (CAU) will conduct triennial audits of each CSA in order to verify compliance with applicable statutes, regulations and policies. This audit includes a sample of Criminal Justice Agency (CJA) and NCJAs, in coordination with the SIB.

Note 1: Audits may be conducted on a more frequent basis if the audit reveals that an agency has not complied with applicable statutes, regulations and policies.

Note 2: The FBI CJIS Division has the authority to conduct unannounced security inspections and scheduled audits of Contractor facilities.

CSP Section 5.11.2 describes the requirements for the CSA to triennially audit all CJAs and NCJAs with direct access to the state system, establish a process to periodically audit all NCJAs with access to CJI, establish the authority to conduct unannounced security inspections and scheduled audits of Contractor facilities.

CSP Section 5.11.3 describes the requirement that all agencies with access to CJI must permit an inspection team to conduct an appropriate inquiry and audit of any alleged security violations. The inspection team, appointed by the APB, will include at least one

representative of the CJIS Division. All results of the inquiry and audit will be reported to the APB with appropriate recommendations.

k. 5.12 – Personnel Security

CSP Section 5.12 provides agencies the security terms and requirements as they apply to all personnel who have unescorted access to unencrypted CJI, including individuals with only physical or logical access to devices that store, process or transmit unencrypted CJI.

CSP Section 5.12.1 details the minimum screening requirements for all individuals requiring unescorted access to unencrypted CJI.

CSP Section 5.12.2 describes the requirement for an agency to immediately terminate CJI access for an individual upon termination of employment.

CSP Section 5.12.3 describes the requirement for an agency to review CJI access authorizations and initiate appropriate actions (such as closing and establishing accounts and changing system access authorizations) whenever personnel are reassigned or transferred to other positions within the agency.

CSP Section 5.12.4 describes the requirement for an agency to employ a formal sanctions process for personnel failing to comply with established information security policies and procedures.

l. 5.13 – Mobile Devices

When access to CJI using mobile devices such as laptops, smartphones, and tablets is authorized, CSP Section 5.13 explains the controls required to manage those devices to ensure the information remains protected.

The following scenarios are intended to help the reader identify areas within the CSP that CJAs may often come across. Each scenario should be reviewed for applicability in conjunction with the above “General CJI Guidance” section. The specific requirements found with the CSP are not shown; however specific sections are referenced along with a requirements summary.

Hard Copy CJI Storage and Accessibility

When CJI is received in hard copy and the agency stores the paper within a locked file cabinet, the CJA should, in addition to the “General CJI Guidance”, focus on compliance with policy section:

a. 4.2.4 – Storage

When storing CJI, appropriate administrative, technical, and physical safeguards must be implemented to ensure the security and confidentiality of the information.

Electronic CJI Storage and Accessibility – Controlled Area

When an agency creates an electronic copy of CJI (e.g. scanning a document or creation of a spreadsheet) and subsequently stores this static CJI on either a local hard drive or shared network drive in a controlled area for indirect access by Authorized Recipients, the agency should, in addition to the “General CJI Guidance”, focus on compliance with policy section:

a. 5.5.2.4 (3) – Access Control Mechanisms – Encryption

CSP Section 5.5.2.4 item 3, Encryption – This describes the requirement for utilizing encryption as the primary access control mechanism which is necessary in this

situation. Encrypted information can only be read by personnel possessing the appropriate cryptographic key (e.g., passphrase) to decrypt. Refer to Section 5.10.1.2 for specific encryption requirements.

Electronic CJI Storage and Accessibility – Physically Secure Location

When an agency receives or creates an electronic copy of CJI and subsequently stores this CJI within a Records Management System (RMS), located within a physically secure location that may be queried by Authorized Recipients, the agency should, in addition to the “General CJI Guidance”, focus on compliance with policy sections:

a. **5.5 – Access Control**

CSP Section 5.5 describes the requirements and parameters for utilizing access control mechanisms for restricting CJI access (such as the reading, writing, processing and transmission of CJIS information) and the modification of information systems, applications, services and communication configurations allowing access to CJI to only authorized personnel.

b. **5.6 – Identification and Authentication**

CSP Section 5.6 describes the requirements and parameters agencies must implement to validate and authenticate the identity of information system users and processes acting on behalf of users the identities prior to granting access to CJI or agency information systems/services that process CJI.

c. **5.7 – Configuration Management**

CSP Section 5.7 describes the requirements for implementing access restrictions that will only permit authorized and qualified individuals access to information system components for purposes of initiating changes, including upgrades, and modifications.

CSP Section 5.7.1 describes the requirements for implementing the concept of least privilege (5.7.1.1) and for developing and maintaining network diagrams (5.7.1.2) that detail how the RMS is interconnected and protected within the network. See Appendix C for sample network diagrams.

CSP Section 5.7.2 details the requirement for agencies to protect the system documentation from unauthorized access consistent with the provisions described in Section 5.5 Access Control.

d. **5.10 – System and Communications Protection and Information Integrity**

CSP Section 5.10 details the requirements for network infrastructures within physically secure locations through establishment of system and communication boundary and transmission protection safeguards that assist in securing an agency’s environment, even when virtualized. In addition, this section describes the requirements for providing the capability to ensure system integrity through the detection and protection against unauthorized changes to software and information for applications, services, and information systems.

Use Case Scenarios

1. Indirect Access to Criminal Justice Information (CJI) Stored on a Network Server

A county court scans hard copy case documents containing CJI into an electronic format. The documents are placed on a network server which is located in a secure data center within the court offices. The data center meets all the requirements to be labeled a physically secure location as defined in Section 5.9.1 of the CSP.

Keeping in mind the scenario as described, an authorized user needs access to case documents. This user is not located in the secure data center and will have to use remote access to access the file. The user is therefore required to provide identification and authentication credentials to prove they are an authorized user. To access the documents, the user is prompted to enter their unique username and password. Because the documents reside on a system with indirect access to CJI (does not allow the user to query a state or national criminal record repository), AA is not required for access to the documents.

NOTE: If the Authorized User has direct access to CJI (the ability to query a state or national criminal record repository) in the above scenario, AA would be required.

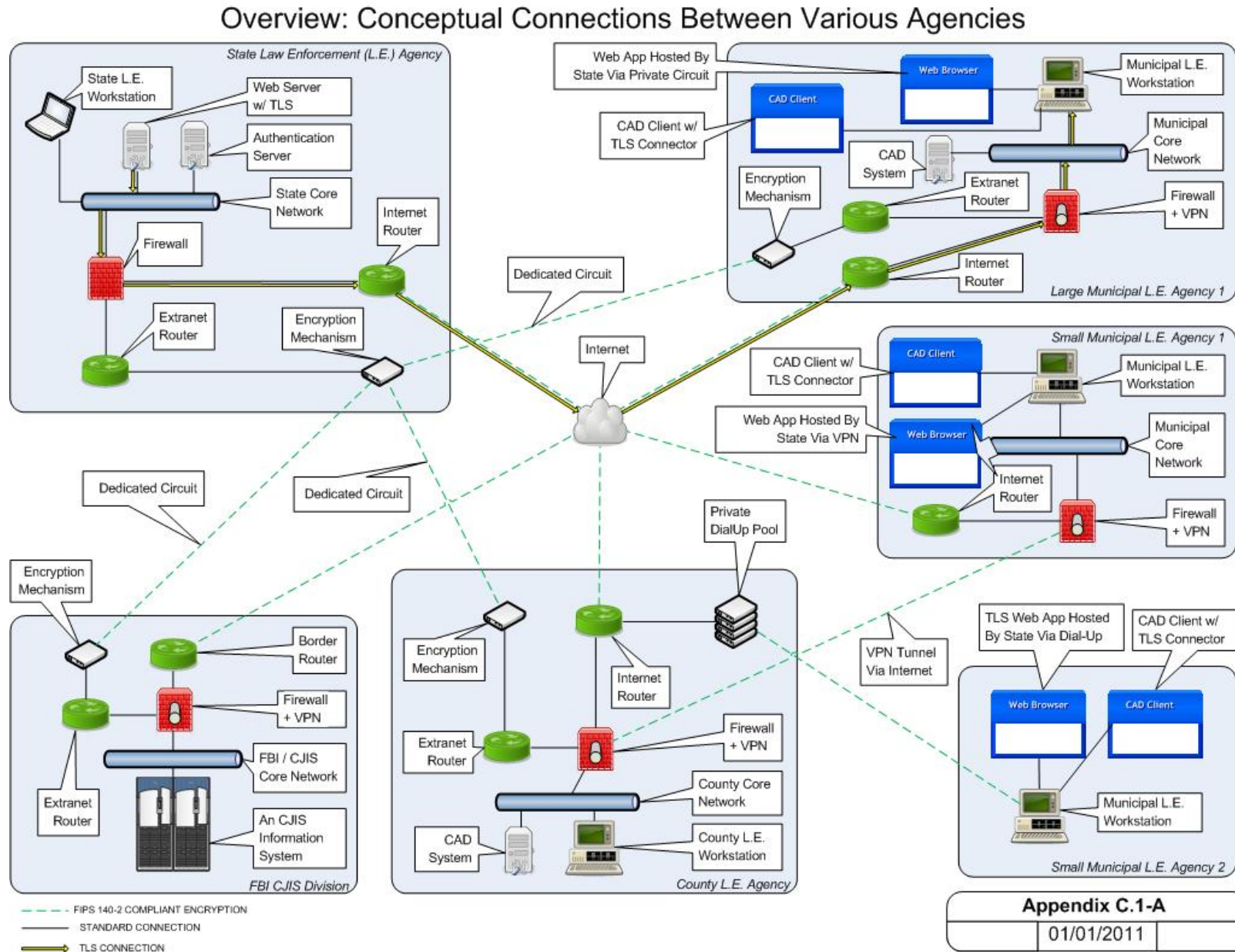
2. Encryption for Data at Rest (Exemption for FIPS 140-2 Certified Encryption)

A county court scans hard copy case documents containing CJI in an electronic format. The documents are placed on a network server which is not located in a secure data center. Because the data center does not meet the requirements of a physically secure location, as defined in Section 5.9.1 of the CSP, the files, at rest (in storage) on the server, are required to be encrypted.

To prevent unauthorized access, the IT staff has decided to encrypt the entire folder that contains the files. They will use a product that provides an advanced encryption standard (AES) algorithm at 256 bit strength to comply with the CSP and employ a CSP compliant passphrase to lock the folder's encryption. When an authorized user needs to access to the case documents, they access the folder on the server and are prompted to enter the designated passphrase to decrypt (unlock) the folder. The user can then access all files within the folder. Additionally, because the documents reside on a system with indirect access to CJI (does not allow the user to query a state or national criminal record repository), AA is not required for access to the documents.

NOTE: Whenever authorized personnel no longer require access to the encrypted folder, the passphrase must be changed to prevent future access by that user.

Figure C-1-A Overview: Conceptual Connections Between Various Agencies



T

—
