CJIS Access, Maintenance, and Security

809.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidelines for the use, maintenance, and security of department systems that access Criminal Justice Information.

809.1.1 DEFINITIONS

Definitions related to this policy include:

Criminal Justice Information (CJI) - Data provided by FBI Criminal Justice Information Services (CJIS) that is necessary for law enforcement agencies to perform their mission and enforce the laws (e.g., biometric, identity history, person, organization, case/incident history data).

Security incident - Any incident that compromises the security of CJI or systems that access CJI. Examples include but are not limited to unauthorized use of legitimate code or credentials within department systems, email communications that contain malicious code, data breaches, signaling to external systems, and unauthorized exporting of information.

809.2 POLICY

It is the policy of the Louisville Police Department to maintain the security, confidentiality, and integrity of its information systems that access CJI by collaborating with appropriate state and federal agencies to implement the applicable established protocols.

809.3 CJIS COORDINATOR

The Chief of Police shall appoint a CJIS coordinator, who shall be responsible for the Louisville Police Department's adherence to FBI CJIS Security Policy requirements.

The CJIS coordinator shall establish procedures necessary to govern the department's use, maintenance, and security of systems that access CJI as described in this policy.

809.3.1 CJIS COORDINATOR RESPONSIBILITIES

The responsibilities of the CJIS coordinator include but are not limited to:

a. Coordinating with others, such as the information technology or legal departments, as appropriate, to maintain department compliance with FBI CJIS Security Policy requirements and the Colorado Bureau of Investigation (CBI).
b. Managing member accounts with access to CJI, including:
    1. Creating, enabling, modifying, disabling, and removing member accounts in accordance with this policy and the FBI CJIS Security Policy.
    2. Configuring member accounts in accordance with federal and state requirements (e.g., limiting unsuccessful login attempts).

3. Reviewing member accounts for compliance with legal and policy requirements at least annually.

c. Overseeing the maintenance, repair, and replacement of CJI systems and system components in accordance with manufacturer or vendor specifications and/or department requirements, including:
    1. Maintaining a list of organizations and personnel approved by the Chief of Police to perform maintenance on CJI systems.
    2. Approving, scheduling, documenting, and monitoring all maintenance and diagnostic activities, whether performed on-site, remotely, or off-site, and maintaining records.
    3. Verifying that non-escorted personnel performing maintenance on any CJI system or terminal possess the required access authorizations, and designating members who have the required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.
    4. Maintaining records for all system maintenance and diagnostic activities.
d. Monitoring department systems that have access to CJI to ensure compliance with applicable laws and this policy; developing processes to detect, identify, and correct flaws in software and firmware; and conducting security updates as necessary.
e. Providing for the security of hardware that includes provisions for the following:
    1. How hardware is to be brought into and taken out of department facilities
    2. Physical security of hardware within department facilities
    3. Physical security of areas containing network connections and transmission lines, including monitored access
f. Implementing and carrying out the department Incident Response Plan, including:
    1. Tracking and documenting all suspected or actual security incidents related to CJI in an appropriate manner.
    2. Directing annual testing of the department's information security incident response capabilities using tabletop or walk-through exercises, simulations, or other types of testing.
    3. Making the appropriate notifications outside of the Department (see the Records Maintenance and Release Policy for additional guidance).
    4. Providing information on security incidents to any third-party software developers or vendors as appropriate.
g. Protecting digital and non-digital media that contain CJI, including physical security, transportation, destruction/sanitization, and documentation requirements.
h. Developing and updating department information security and privacy literacy training and incident response training as required by policy.
i. Maintaining audit records in accordance with the established records retention schedule, but in no event for less than one year.
j. Managing the development, documentation, and dissemination of procedures for the following:
    1. Awareness and training
    2. Incident response
    3. Audit and accountability
    4. Access control
    5. Identification and authentication

6. Configuration management
7. Media protection
8. Physical and environmental protection
9. System and communications protection
10. System and information integrity
11. Maintenance
12. Security and privacy planning
13. Contingency planning
14. Risk assessment

k. Reviewing this policy and related procedures as required by the FBI CJIS Security Policy and proposing updates as needed to the Chief of Police.

809.4 MEMBER RESPONSIBILITIES

All members of the Department shall be committed to detecting information security incidents and making the appropriate notifications.

Any member who suspects that there may have been unauthorized access, disclosure, or other compromise of CJI shall report their suspicions in accordance with the Incident Response Plan within one hour of the discovery.

Personally owned devices or systems and publicly accessible systems shall not be used to access, process, store, or transmit CJI.

809.5 SUPERVISOR RESPONSIBILITIES

Supervisors shall notify the CJIS coordinator when the account access of a member they supervise needs to be modified, disabled, or removed for any reason, such as resignation, termination, or change of duties.

809.6 MEMBER ACCOUNTS

Department accounts used to access CJI shall only be created upon approval of the Chief of Police or the authorized designee.

Member accounts shall be disabled within one week of any of the following:

a. The account has expired.
b. The account is no longer associated with a member.
c. The account is found to be in violation of this policy.
d. The account has been inactive for 90 calendar days.

If any threat to the confidentiality, integrity, or availability of CJI related to a specific member account is detected, the CJIS coordinator or designated member shall disable the account within 30 minutes of the discovery.

809.6.1 ACCESS AUTHORIZATION

Access authorization for systems transmitting, receiving, using, or storing CJI shall be based on the principle of least privilege as follows:

a. Members shall only be granted access authorizations that are necessary to accomplish assigned department tasks.
b. Accounts with security privileges shall only be authorized for members with an operational need for the privileges. Privileged functions shall be logged as they are executed.
c. Non-privileged members shall not be allowed to execute privileged functions.

809.6.2 ACCOUNT REVIEW ACTIVITIES

At least annually, the CJIS coordinator shall review member accounts for compliance with policy and applicable laws. The CJIS coordinator shall validate account privileges and remove or reassign them as necessary to accurately reflect the department mission and law enforcement needs.

809.7 MEDIA PROTECTION

Access to media containing CJI shall be restricted to authorized members and stored within physically secured locations or controlled areas, in accordance with the FBI CJIS Security Policy.

Digital media (e.g., flash drives, external or removable hard disk drives, compact discs) containing CJI shall be encrypted. Personally owned digital media devices or digital media devices with no identifiable owner shall not be used on department systems that store, process, or transmit CJI.

Non-digital media (e.g., paper files, printed pages, microfilm) containing CJI should be enclosed in an opaque folder or container if they are to be transported outside of physically secure locations or controlled areas. Media containing CJI shall not be left unattended outside of a physically secure location.

Transportation and transfers of media containing CJI shall be documented.

809.7.1 MEDIA DISPOSAL AND RELEASE

Digital media containing CJI shall be overwritten at least three times or degaussed (i.e., erased) prior to being disposed of, released from department control, or released for reuse. Inoperable digital media devices, such as hard drives or solid-state drives that cannot be accessed to overwrite the data, shall be physically destroyed. When non-digital media is no longer needed for investigative or security purposes, it shall be destroyed by crosscut shredding or incineration.

809.8 SYSTEM AND INFORMATION INTEGRITY

The integrity of department CJI systems shall be protected through the implementation of appropriate controls such as:

a. Flaw remediation.
b. System monitoring.

c. Security alerts, advisories, and directives.
d. Software, firmware, and information integrity controls.
e. Spam protection.

809.9 INCIDENT RESPONSE PLAN

INCIDENT RESPONSE POLICY.pdf

809.10 SECURITY AWARENESS TRAINING

Members with physical or electronic access to CJI or CJI systems shall complete security awareness training appropriate to their assigned roles and responsibilities and shall certify their understanding by signing a formal Security Awareness Training Acknowledgement. Training shall include information security and privacy literacy training, security incident response training, and a review of this policy and related procedures.

Security awareness training shall be completed prior to accessing any CJI data or system and at least annually thereafter. Additional training shall be completed as required following any changes to CJI systems and for any member involved in a security incident within 30 days of the event.

Individual training records shall be maintained in accordance with the established records retention schedule, but in no event for less than three years.

The department's CJIS training shall be reviewed for any necessary updates or changes annually and following any security incident or change in a CJI system or the FBI CJIS Security Policy.

809.11 SANCTIONS

Failure to adhere to policies and procedures pertaining to CJI shall result in disciplinary action, up to and including termination. Misuse of or failure to secure CJI may also result in temporary or permanent restrictions in the use of CJI. Intentional misuse of CJI may also be prosecutable under applicable laws.

Attachments

INCIDENT RESPONSE POLICY.pdf

Incident Response Policy

Purpose

The purpose of this policy is to outline the proper incident response procedures at Louisville Police Department] which are consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. These policies and procedures are in place to protect criminal justice information, systems, employees, Louisville Police Department, and the criminal justice community.

Scope

This policy applies to all Louisville Police Department employees, contractors, temporary staff, and other workers at Louisville Police Department, with access to CJIS systems and/or data, sensitive and classified data, and media (i.e., general user; privileged user).

To ensure protection of CJI, Louisville Police Department shall:

(1) Designate an individual with security responsibilities to manage the development, documentation, and dissemination of the incident response policy and procedures.
(2) Review and update the current incident response policies and procedures annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI.

Policy

Training

Louisville Police Department has developed incident response training for all employees, contractors, temporary staff, and other workers at Louisville Police Department, with access to CJIS systems and/or data, sensitive and

classified data, and media (i.e., general user; privileged user). Various levels of training have been developed appropriately depending on employee or personnel type. This includes user training in identifying and reporting suspicious activities from external and internal sources, information on how to identify and respond to a breach, as well as how to report a breach.

A breach is defined as the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or a similar occurrence where a person other than an authorized user accesses or potentially accesses criminal justice information, personally identifiable information, or a CJI system; or an authorized user accesses or potentially accesses such information for other than authorized purposes.

Louisville Police Department shall review and update incident response training content **annually** and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI. Louisville Police Department shall provide incident response training to information system users consistent with assigned roles and responsibilities before authorizing access to the information system or performing assigned duties, when required by information system changes; and annually thereafter.

Louisville Police Department has developed incident response testing to evaluate the incident response procedures currently in place.

Incident Handling

An effective incident handling capability includes coordination among many organizational entities (e.g., mission or business owners, system owners, authorizing officials, human resources offices, physical security offices, personnel security offices, legal departments, risk executive [function], operations personnel, procurement offices).

Suspected security incidents include the receipt of suspicious email communications that can contain malicious code, while suspected supply chain incidents include the insertion of counterfeit hardware or malicious code into organizational systems or system components.

Louisville Police Department has implemented an incident handling capability for incidents discussed in the incident response plan.

The plan includes preparation, detection and analysis, containment, eradication, and recovery.

Incident Monitoring

Louisville Police Department tracks and documents all incidents that occur regarding the security of Criminal Justice Information (CJI) within Louisville Police Department. Documentation shall include:

(1) Maintaining records about each incident.
(2) The status of the incident.
(3) Evaluation of incident details, trends, and handling.

Incident Reporting

Louisville Police Department will promptly report incident information to the appropriate authorities within one hour after discovery. Louisville Police Department personnel shall be aware of the procedures for reporting the different types of events and weaknesses that might have an impact on the security of Louisville Police Department assets. If deemed an incident, Louisville Police Department personnel must notify the CSO.

Louisville Police Department personnel who:

(1) suspect a potential security breach or issue,
(2) become aware of any CJIS-related policy violation or potential violation, or
(3) realize that “something isn’t right” with computers, applications, or systems used for Louisville Police Department IT operations,

Shall notify their supervisor and tell them the issue; if their supervisor is unavailable, the person shall notify the next appropriate member in their chain-of-command.

Louisville Police Department Supervisors, upon notification by Louisville Police Department personnel:

Notify IT Director and the Local Agency Security Officer (LASO).

Notify Chief of Police, Deputy Chief, Division Commander and Administrative Services Manager.

Incident Response Assistance

Louisville Police Department has implemented incident response support resources, integral to the organizational incident response capability, that offer advice and assistance to users of the system for the handling and reporting of incidents.

Incident Response Plan

The following establishes an operational incident handling procedure for Louisville Police Department CJI and CJI systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; tracks, documents, and reports incidents to appropriate Louisville Police Department personnel and/or authorities.

Louisville Police Department shall:

(1) Revise the incident response plan/procedures to address system/organizational changes or problems encountered during implementation, execution, or testing.
(2) Distribute copies of the incident response plan/procedures to incident response personnel.
(3) Communicate incident response plan/procedure changes to incident response personnel and other organizational elements as needed.
(4) Track and document information system security incidents, retain and safeguard cyber security incident documentation as evidence for investigation, corrective actions, potential disciplinary actions, and/or

prosecution.

The IT Director (Current: Paulina Bennett) is the Louisville Police Department's point-of-contact for CJI security-related issues and will ensure the Incident Response reporting procedures are initiated at the local level.

Procedures for Reporting Information Security Events:

Louisville Police Department will promptly report incident information to the appropriate authorities. CJI-related security events and weaknesses associated with information systems shall be communicated in a manner allowing timely corrective action to be taken. Louisville Police Department personnel shall be aware of the procedures for reporting the different types of events and weaknesses that might have an impact on the security of Louisville Police Department assets. Louisville Police Department personnel are required to report any information security events and weaknesses as quickly as possible to the security point-of-contact identified above.

Reporting Procedures for Suspected and Actual Security Breaches for all Louisville Police Department Personnel:

*As required, an incident response team will be formed and implemented for Louisville Police Department

Louisville Police Department personnel who:

(1) suspect a potential security breach or issue,
(2) become aware of any CJIS-related policy violation or potential violation, or
(3) realize that "something isn't right" with computers, applications, or systems used for Louisville Police Department business,

Shall notify their supervisor and tell them the issue; if their supervisor is unavailable, the person shall notify the next appropriate member in their chain-of-command.

Louisville Police Department Supervisors, upon notification by Louisville Police Department personnel:

Notify IT Director (Current: Paulina Bennett) Local Agency Security Officer (LASO).

Notify Chief of Police, Deputy Chief, Division Commander and Administrative Services Manager.

The designated LASO (or Compliance Officer) shall:

(1) Compile information needed for completing an IT Security Incident Response Form (also attached in Word & PDF).
(2) Identify the suspected cause of the incident (name, virus, etc.). Determine and note if antivirus software was running and up to date at the time of infection (if applicable).
(3) Determine how and when the problem was first identified.
(4) Note if local IT staff have been notified / determine if they are involved.
(5) Determine the number of workstations infected/affected.
(6) Determine if any other equipment or the network is infected.
(7) Determine proposal of action plan for removal.

These questions must be answered before the action plan for removal is implemented:

(1) Will infected workstations be re-imaged before reconnection?
(2) When was the last update of signature files?
(3) When was the last operating system update?
(4) Was any CJIS data or personal identification information compromised?

The system component will remain disconnected from the CJI network(s) until Paulina Bennett is certain Louisville Police Department systems are free from virus infection.

Incident Response Team

An incident response team may be formed to include positions below that are deemed necessary by Louisville Police Department to respond to security incidents effectively. These roles are not mandatory, and may not

be needed in every situation, but may be beneficial in maintaining the security of Louisville Police Department. One individual may fill multiple roles within the agency.

- **Incident Response Manager/Team Lead:**
  This person is responsible for coordinating the overall incident response efforts, managing team members, and ensuring that the incident response plan is executed effectively.
- **Incident Analyst/Investigator:**
  This role involves analyzing and investigating security incidents, identifying the root cause, and determining the extent of the compromise. Incident analysts use various tools and techniques to gather evidence, perform forensic analysis, and provide recommendations for containment and eradication.
- **Threat Intelligence Analyst:**
  These individuals monitor and analyze threat intelligence sources to identify potential threats, vulnerabilities, and indicators of compromise (IOCs). They provide insights into the evolving threat landscape and help the team proactively detect and respond to emerging security incidents.
- **Forensics Expert:**
  A forensic expert specializes in digital forensics and is responsible for gathering, analyzing, and preserving digital evidence related to security incidents. They have in-depth knowledge of forensic tools and techniques and help in legal and investigative processes.
- **IT/Network Administrator:**
  Network and system administrators play a crucial role in incident response by providing technical expertise to contain, isolate, and remediate affected systems. They assist in system restoration, patching vulnerabilities, and implementing security controls.
- **Communications Coordinator:**
  This person handles internal and external communications related to security incidents. They liaise with stakeholders, coordinate notifications, and ensure timely and accurate communication throughout the incident response process.
- **Legal/Compliance Representative:**
  Depending on the nature of the incident, having a legal or

compliance representative on the team is important to address any legal or regulatory implications. They provide guidance on legal requirements, data breach notification laws, and ensure compliance during the incident response process.

- **Public Relations/Corporate Communications:**
  In case of high-profile or public incidents, a member from the public relations or corporate communications team may be involved in managing public messaging, media relations, and reputation management.
- **External Experts/Consultants:**
  In certain situations, organizations may engage external experts or consultants with specialized knowledge or skills to assist in incident response. These experts may include incident response consultants, cybersecurity consultants, or legal advisors.