Kentucky State Police – LINK/NCIC IT Security Policy

A Comprehensive Guide for CJI Security Compliance

**INSERT AGENCY NAME HERE**

**General**

Our agency relies on LINK/NCIC as an essential tool in its daily operations. This system enables officers to swiftly access records, conduct inquiries, and communicate with the broader criminal justice community. The real-time information provided by LINK/NCIC enhances our ability to respond to incidents effectively, ensuring a safer environment for both the public and our officers. As custodians of this powerful resource, we are committed to upholding the highest standards of data security and accuracy to maintain the integrity of the criminal justice system.

Procedures included in this policy:

1. CJIS, LINK, NCIC, NLETS
2. Auditing and Accountability
3. Incident Response
4. Identification and Authentication
5. Configuration Management
6. Media Protection
7. Personnel Security
8. System and Information Integrity
9. Access Control
10. Awareness and Training

|  |  |
| --- | --- |
| **Procedure** | **LINK/NCIC Policy** |
| **Name of Procedure** | **CJIS, LINK, NCIC, and NLETS** |
| **Policy Overview** | General Use and RestrictionRole and Responsibilities |
| **Applicable Parties** | **CJIS Users**: This includes any personnel who access Criminal Justice Information Systems, including full-access users and inquiry-only users.**Terminal Agency Coordinator (TAC)**: The individual responsible for overseeing CJIS System programs within the local agency and ensuring compliance with CJIS system policies.**Assistant Terminal Agency Coordinator (ATAC):** The person who assists the TAC and assumes the TAC duties if they are unavailable.**Local Agency Security Officer (LASO):** Responsible for ensuring the security of CJIS systems and hardware, including personnel screening and reporting security incidents.**Private Contractors/Vendor Personnel**: Any third-party personnel who provide services that involve access to CJIS systems or secure locations. |
| **Effective Date** | Highlight this text, then type effective date here |
| **Procedures** | * 1. **General Use and Restrictions**
1. CJIS Users and all criminal justice personnel must adhere to federal and state laws, regulations, procedures and policies established by the NCIC Advisory Policy Board, FBI/NCIC, NLETS, LINK, CJIS systems/programs, and CSA regarding system operation and the security and privacy of criminal justice and law enforcement information.
2. Our agency follows the LINK/NCIC Policy and CJIS Security Policy. These policies can be viewed at: <https://le.fbi.gov/cjis-division/cjis-security-policy-resource-center>, <https://link.ky.gov>, <https://kentuckystatepolice.ky.gov>.
3. Each CJIS user must continuously monitor the LINK/NCIC terminal while on duty.
4. The LINK, NCIC, and NLETS system shall not be used to send regional broadcast messages for the following purposes:
	1. Social announcements (e.g., holiday messages or retirements)
	2. Personnel recruitment
	3. Messages in which the complainant is solely interested in the recovery of property.
	4. Attempts to locate vehicles when no prosecution will be pursued.
	5. Excessively long messages
	6. Support or opposition of political, legislative bill, or labor issues
	7. Announcements of political, legislative, or labor-oriented meetings
	8. Request for information on salary, uniforms, personnel, or related matters
	9. Advertisement or sale of equipment
	10. Messages regarding wanted individuals or vehicles that can be entered into NCIC
	11. Requests for criminal history record information
	12. No reply-only-if-wanted (ROIWS) messages
	13. Solicitation of funds
	14. Training announcements identifying “for profit” companies providing training
5. The LINK/NCIC, NLETS, PII, and all CJIS systems shall be used strictly for official business and shall not be used for personal business or interests.
6. The N-Dex program, if utilized by authorized personnel must adhere to the N-Dex Policy and Procedure Operating Manual. The policy can be viewed at <https://www.fbi.gov>. A paper copy may be provided upon request.

**1.2 Roles and Responsibilities** **1.2.1 Terminal Agency Coordinator (TAC)**1. The TAC serves as the point of contact at the local agency for matters related to CJIS information access.
2. The TAC administers CJIS system programs within the local agency and ensure compliance with CJIS system policies.
3. The TAC will perform all TAC duties as outlined in the LINK Policy.
4. The TAC will complete any mandated TAC training.

**1.2.2 Assistant Terminal Agency Coordinator (ATAC)**1. The ATAC will assist with TAC duties and act as the TAC if the TAC is unable to perform those duties.
2. The ATAC will complete any mandated TAC training.

**1.2.3 Local Agency Security Officer (LASO)**1. Identify who is using the CSA-approved hardware, software, and firmware, and ensure no unauthorized individuals or processes have access to them.
2. Identify and document how the equipment is connected to the state system.
3. Ensure that personnel security screening procedures are being followed.
4. Ensure the approved and appropriate security measures are in place and functioning as expected.
5. Support policy compliance and ensure the CSA ISO is promptly informed of any security incidents.
6. The LASO will complete any mandated LASO Security and Privacy Training.

**1.2.4 User Agreements**1. This agency will maintain on file the appropriate and current user agreements:
	1. Between this agency and the Kentucky State Police.
	2. Between this agency and each respective satellite agency.
	3. Between this agency and each respective non-criminal justice agency (e.g., management control agreements between agencies and dispatch centers).
	4. If secondary dissemination is allowed, a secondary dissemination log must be kept.
2. This agency will implement and maintain on file the CJIS Security Addendum with each servicing private contractor/ vendor and Memorandum of Understanding (MOU’s) if required.

**1.2.5 CJI Access**1. All personnel who may have access to Criminal Justice Information (CJI) must submit fingerprints at an IdentoGo location immediately before CJIS access is granted. **(Note: There is no 10-day grace period.)**
2. This agency will ensure that the correct User Account Request form is sent to the ISO immediately prior to granting CJIS access.

**1.2.6 Terminal Operators, Inquiry-Only Users, and MDT Users**1. This agency will ensure that CJIS users complete the Security and Privacy Training Module before CJIS access is granted. This training is done through the nexTEST program on the CJIS LaunchPad for Full Access Users and MDT Inquiry-Only Users.
2. Full Access and MDT Inquiry-Only training must be completed by the access level deadline.
3. This agency will ensure that users complete recertification every year.
 |
| **Approved by / Date** | Highlight this text, then type name of person approving here | Highlight this text, then enter date of approval here |

|  |  |
| --- | --- |
| **Policy** | LINK/NCIC Policy |
| **Name of Procedure** | **Auditing and Accountability** |
| **Reference Number** | 2.0 |
| **Applicable Parties** | **CJIS Users**: This includes any personnel who access Criminal Justice Information Systems, including full-access users and inquiry-only users.**Terminal Agency Coordinator (TAC)**: The individual responsible for overseeing CJIS System programs within the local agency and ensuring compliance with CJIS system policies.**Assistant Terminal Agency Coordinator (ATAC)**: The person who assists the TAC and assumes the TAC duties if they are unavailable.**Local Agency Security Officer (LASO):** Responsible for ensuring the security of CJIS systems and hardware, including personnel screening and reporting security incidents.**Private Contractors/Vendor Personnel**: Any third-party personnel who provide services that involve access to CJIS systems or secure locations. |
| **Effective Date** | Highlight this text, then type effective date here |
| **Purpose** | To ensure that **Agency** resources and information systems are established with effective security controls and control enhancements that reflect applicable federal and state laws, Executive Orders, directives, regulations, policies, standards, and guidance. |
| **Procedures** | **2.1 HIGH-PRIORITY AUDITABLE EVENTS:**The agency, in cooperation with audits and IT, shall ensure the information system will generate audit records containing information that establishes what type of even occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the **Agency** of the individuals or subjects associated with the event. Additionally, the agency, in cooperation with audits and IT shall:Determine that the information system is capable of auditing the following events: * 1. **User Authentication and Access (AU-2, AU-4):**
	+ **Successful and Unsuccessful Login Attempts:** Log all attempts to access the system, capturing usernames, timestamps, and success/failure status. This helps identify unauthorized access attempts and potential account compromises.
	+ **Access to Sensitive CJI Records**: Log any time a user accesses, views, modifies, creates, deletes records containing highly sensitive CJI, such as:
		- **Incident/Case files**
		- **Motor vehicle and property records**
	+ **Use of Elevated Privileges**: Log any action performed by users with elevated privileges (e.g., system administrators). This includes changes to user accounts, system configuration, or access permissions.
	1. **System Changes and Configuration Management (AU-2, CM-6)**
	+ **Modifications to System Configurations**: Log changes to firewall rules, network settings, operating systems, application settings, and other critical system components.
	+ **Software Installations and Updates**: Log the installation of any new software, updates to existing software, and changes to system firmware.
	1. **Data Transfers and Sharing (AU-2, AU-4):**
	+ **CJI Queries and Retrievals:** Log all queries made to local, state, and national databases (e.g., NCIC, NICS). Capture the user, timestamp, search criteria, and retrieved data.
	+ **CJI Dissemination**: Log any time CJI is shared with external agencies or individuals, including the recipient, purpose of the disclosure, and authorization. Pay close attention to secondary dissemination where ethe recipient is not part of a pre-existing information exchange agreement.
1. **Security Events (AU-1, IR-6, Appendix J):**
	* **Intrusion Attempts**: Log suspected or confirmed security incidents such as unauthorized access attempts, malware infections, and denial-of-service attacks.
	* **Data Breaches**: Log any confirmed or suspected breaches of CJI confidentiality, including unauthorized access, disclosure, or data loss.
	1. **Additional Audit and Accountability Requirements:**
2. **Review and Updates**
	1. The agency shall review and update ethe audited events 30-60 days from the completion of the audit to finalize updates to audited events.
3. **Audit Storage Capacity**
	1. The agency shall ensure audit record storage capacity is large enough to:
		1. Retain records for legally required retention period (e.g., at least 1 year).
		2. Accommodate current and future data volumes
		3. Support system performance, accessibility, and backup requirements.
		4. Comply with all relevant security and regulatory standards.
4. **Transfer to Alternate Storage**
	1. The information/CAD system shall off-load audit records, in accordance with FBI CJIS Security Policy, onto a different system or media than the system being audited.
5. **Response to Audit Processing Failures:**The Information/CAD System shall:
6. Alert [**agency** defined personnel or roles] in the event of an audit.
7. Take the following additional actions: [**agency** defined actions to be taken processing failure; and (e.g., shut down information system, overwrite oldest audit records, stop generating audit records)].
8. **Audit Storage Capacity**
	1. The information/CAD system shall provide a warning to [**Agency** defined personnel, roles, and/or locations] immediately or within 15 minutes when allocated audit record storage volume reaches 75% or repository maximum audit record storage capacity.
9. **Real-time Alerts**
	1. **Audit Logging Process Failures (AU-5)**: The information/CAD system shall provide an alert **within one hour** to [**Agency** defined personnel, roles, and/or locations] when the following audit failure events occur:
		1. Software and hardware errors affecting the audit logging mechanisms
		2. Failures in audit log capturing mechanisms, preventing events from being recorded
		3. Reaching or exceeding audit log storage capacity, potentially leading to data loss or disruption of the logging process.
	2. **Protection of Audit Information (AU-9)**
		1. Unauthorized Access: Any attempts to access audit information without proper authorization.
		2. Modification: Any alterations made to audit records, setting, or tools without proper authorization.
		3. Deletion: Any attempts to delete audit information without proper authorization.
	3. **System Monitoring Alerts (SI-9):**
		1. This includes inappropriate or unusual activities with security or privacy implications, which could encompass failures impacting the following:
			1. Authentication systems
			2. Access control mechanisms
			3. Intrusion detection and prevention systems
			4. Malicious code protection
	4. Critical System Component Failures:

**Remember:**1. Coordinate the security audit function with other organizational entities requiring audits.
2. Provide a rationale for why the auditable events are deemed adequate to support after-the-fact investigations of security incidents.
3. Determine the events to be audited within the information system

**2. REVIEWS AND UPDATES**1. The Example Police Agency shall review and update the audited events [Agency-defined frequency].

**3. CONTENT OF AUDIT RECORDS**1. The information system shall generate audit records containing information that establishes the type of event, when and where it occurred, the source, the outcome, and the Agency of individuals associated with the event.

**4. ADDITIONAL AUDIT INFORMATION**1. The information system shall generate audit records containing the following additional information: [Agency-defined additional, more detailed information].

**5. AUDIT STORAGE CAPACITY**1. The information owner shall ensure audit record storage capacity is allocated in accordance with [Agency-defined audit record storage requirements].

**6. TRANSFER TO ALTERNATE STORAGE**1. The information system shall off-load audit records [Agency-defined frequency] onto a different system or media than the system being audited.

**7. RESPONSE TO AUDIT PROCESSING FAILURES**The information system shall:1. Alert [Agency-defined personnel or roles] in the event of an audit processing failure.
2. Take the following actions: [Agency-defined actions to be taken in case of failure, e.g., system shutdown, overwrite oldest records, stop generating records].

**8. AUDIT STORAGE CAPACITY WARNINGS**1. The information system shall provide a warning to [Agency-defined personnel, roles, and/or locations] within [Agency-defined time period] when allocated storage volume reaches [Agency-defined percentage] of maximum capacity.

**9. REAL-TIME ALERTS**1. The information system shall provide an alert in [Agency-defined real-time period] to [Agency-defined personnel, roles, and/or locations] when the following audit failure events occur: [Agency-defined audit failure events requiring real-time alerts].

**10. CONFIGURABLE TRAFFIC VOLUME THRESHOLDS**1. The information system shall enforce configurable network communication traffic volume thresholds, rejecting or delaying network traffic above those thresholds.

**11. SHUTDOWN ON FAILURE**1. The information system shall invoke a [full system shutdown, partial shutdown, or degraded operational mode] in the event of [Agency-defined audit failures], unless an alternate audit capability exists.

**12. AUDIT REVIEW, ANALYSIS, AND REPORTING**The information system owner shall:1. Review and analyze audit records [Agency-defined frequency] for indications of [Agency-defined inappropriate or unusual activity].
2. Report findings to [Agency-defined personnel or roles].

**13. PROCESS INTEGRATION**1. The information system owners shall ensure automated mechanisms are employed to integrate audit review, analysis, and reporting processes to support organizational processes for investigating and responding to suspicious activities.

**14. AUDIT REPOSITORIES**1. The information system owner shall ensure analysis and correlation of audit records across different repositories to gain situational awareness.

**15. AUDIT REDUCTION AND REPORT GENERATION**1. The information system shall provide audit reduction and report generation capability that:
	* Supports on-demand audit review, analysis, and reporting requirements.
	* Does not alter the original content or time ordering of audit records.

**16. AUTOMATIC PROCESSING**1. The information system shall process audit records for events of interest based on [Agency-defined audit fields].

**17. TIME STAMPS**The information system shall:1. Use internal system clocks to generate time stamps for audit records.
2. Record time stamps that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT), meeting [Agency-defined granularity of time measurement].

**18. SYNCHRONIZATION WITH AUTHORITATIVE TIME SOURCE**The information system shall:1. Compare internal clocks [Agency-defined frequency] with [Agency-defined authoritative time source].
2. Synchronize internal clocks when the time difference exceeds [Agency-defined time period].

**19. PROTECTION OF AUDIT INFORMATION**1. The information system shall protect audit information and tools from unauthorized access, modification, and deletion.

**20. ACCESS BY SUBSET OF PRIVILEGED USERS**1. The organization shall authorize access to audit management functions only to [Agency-defined subset of privileged users].

**21. AUDIT RECORD RETENTION**1. Information system owners shall retain audit records for [Agency-defined time period] to support investigations of security incidents and meet regulatory and organizational retention requirements.

**22. LONG-TERM RETRIEVAL CAPABILITY**1. Information system owners shall employ [Agency-defined measures] to ensure long-term audit records can be retrieved.

**23. AUDIT GENERATION**The information system shall:1. Provide audit record generation capability for auditable events defined by [Agency-defined information system components].
2. Allow [Agency-defined personnel or roles] to select which auditable events are audited.
3. Generate audit records for events with the content defined by [Agency-defined components].

**24. TIME-CORRELATED AUDIT TRAIL**1. The information system shall compile audit records from [Agency-defined components] into a system-wide audit trail time-correlated to within [Agency-defined tolerance level].

**25. STANDARDIZED FORMATS**1. The information system shall produce a system-wide audit trail composed of records in a standardized format.

**26. CHANGES BY AUTHORIZED INDIVIDUALS**1. The information system shall allow [Agency-defined individuals or roles] to change audit settings for [Agency-defined components] based on [Agency-defined event criteria] within [Agency-defined time thresholds].

**COMPLIANCE**Employees who violate this policy may be subject to disciplinary action, including discharge, as well as civil and criminal penalties. Non-employees, such as contractors, may face termination of contracts, denial of access to IT resources, and other penalties. |
| **Approved by / Date** | Highlight this text, then type name of person approving here | Highlight this text, then enter date of approval here |

|  |  |
| --- | --- |
| **Policy** | LINK/NCIC Policy |
| **Name of Procedure** | **Incident Response** |
| **Reference Number** | 3.0 |
| **Applicable Parties** | **CJIS Users**: This includes any personnel who access Criminal Justice Information Systems, including full-access users and inquiry-only users.**Terminal Agency Coordinator (TAC)**: The individual responsible for overseeing CJIS System programs within the local agency and ensuring compliance with CJIS system policies.**Assistant Terminal Agency Coordinator (ATAC)**: The person who assists the TAC and assumes the TAC duties if they are unavailable.**Local Agency Security Officer (LASO):** Responsible for ensuring the security of CJIS systems and hardware, including personnel screening and reporting security incidents.**Private Contractors/Vendor Personnel**: Any third-party personnel who provide services that involve access to CJIS systems or secure locations. |
| **Effective Date** | Highlight this text, then type effective date here |
| **Purpose** | The purpose of this policy is to establish a structured and efficient approach for detecting, reporting, responding to, and mitigating security incidents involving Criminal Justice Information (CJI). This ensures the confidentiality, integrity, and availability of CJI, compliance with FBI CJIS Security Policy, and the protection of criminal justice operations from unauthorized access or disruption.  |
| **Procedures** | **3.0 INCIDENT RESPONSE TRANING**The **Agency** shall:1. Provide incident response training to information system users consistent with their assigned roles and responsibilities:
	1. Immediately after assuming an incident response role or responsibility.
	2. When required by information system changes, and annually thereafter.
2. Incorporate simulated events into incident response training to facilitate effective response by personnel in crisis situations.
3. Employ automated mechanisms to provide a more thorough and realistic incident response training environment.

**3.1 INCIDENT RESPONSE TESTING**The [**AGENCY**] shall:1. Test the incident response capability for the information system annually using [Assignment: Agency-defined tests] to determine incident response effectiveness and document the results.
2. Coordinate incident response testing with **AGENCY** contacts responsible for related plans such as Business Continuity Plans, Contingency Plans, Disaster Recovery Plans, Continuity of Operations Plans, Crisis Communications Plans, Critical Infrastructure Plans, and Occupant Emergency Plans.

**3.2 INCIDENT HANDLING**The [**AGENCY**] shall:1. Implement an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.
2. Coordinate incident handling activities with contingency planning activities.
3. Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implement the resulting changes accordingly.

**3.3 INCIDENT MONITORING**The [**AGENCY**] shall:1. Employ automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information.

**3.4 INCIDENT REPORTING**The [**Agency**] shall:1. Require personnel to report suspected security incidents to the incident response capability immediately.
2. Report security incident information to [**AGENCY** authorities].

**3.5** **INCIDENT RESPONSE ASSISTANCE**The [**AGENCY**] shall:1. Provide an incident response support resource, integral to the incident response capability, that offers advice and assistance to users of the information system for handling and reporting security incidents.

**3.6** **INCIDENT RESPONSE PLAN**The [**AGENCY**] shall:1. Maintain an incident response plan that:
2. Provides the **Agency** with a roadmap for implementing its incident response capability.
3. Describes the structure of the incident response capability.
4. Provides a high-level approach for how the incident response capability fits into the overall **Agency**.
5. Meets the unique requirements of the **Agency**, which relate to mission, size, structure, and functions.
6. Defines reportable incidents.
7. Provides metrics for measuring the incident response capability within the **Agency**.
8. Defines the resources and management support needed to effectively maintain and mature an incident response capability.
9. Is reviewed and approved by [**AGENCY** **HEAD**].
10. Distribute copies of the incident response plan to [**AGENCY** incident response personnel (identified by name and/or by role)].
11. Review the incident response plan annually.
12. Update the incident response plan to address system changes or problems encountered during plan implementation, execution, or testing.
13. Communicate incident response plan changes to [Agency-defined incident response personnel (identified by name and/or by role)].
14. Protect the incident response plan from unauthorized disclosure and modification.
15. **AGENCY** will report all security incidents to KSP Information Security Officer.

**COMPLIANCE**Employees who violate this Incident Response Policy may be subject to appropriate disciplinary action up to and including discharge, as well as civil and criminal penalties. Non-employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to IT resources, and other actions, as well as civil and criminal penalties. |
| **Approved by / Date** | Highlight this text, then type name of person approving here | Highlight this text, then enter date of approval here |

|  |  |
| --- | --- |
| **Policy** | LINK/NCIC Policy |
| **Name of Procedure** | **Identification and Authentication** |
| **Reference Number** | 4.0  |
| **Applicable Parties** | **CJIS Users**: This includes any personnel who access Criminal Justice Information Systems, including full-access users and inquiry-only users.**Terminal Agency Coordinator (TAC)**: The individual responsible for overseeing CJIS System programs within the local agency and ensuring compliance with CJIS system policies.**Assistant Terminal Agency Coordinator (ATAC)**: The person who assists the TAC and assumes the TAC duties if they are unavailable.**Local Agency Security Officer (LASO):** Responsible for ensuring the security of CJIS systems and hardware, including personnel screening and reporting security incidents.**Private Contractors/Vendor Personnel**: Any third-party personnel who provide services that involve access to CJIS systems or secure locations. |
| **Effective Date** | Highlight this text, then type effective date here |
| **Supporting Documentation** |  |
| **Procedures** |  **4.1 IDENTIFICATION AND AUTHENTICATION****AGENCY** shall:1. Ensure that information systems uniquely identify and authenticate users or processes acting on behalf of [**AGENCY**] users.
2. Ensure that information systems implement multi-factor authentication for network access to privileged accounts.
3. Ensure that information systems implement multi-factor authentication for network access to non-privileged accounts.
4. Ensure that information systems implement multi-factor authentication for local access to privileged accounts.
5. Ensure that information systems implement replay-resistant authentication mechanisms for network access to privileged accounts.
6. Ensure that information systems implement multi-factor authentication for remote access to privileged and non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access and the device utilizes a cryptographic strength mechanisms that protects the primary authentication token (secret key, private key or one-time password) against compromise by protocol threats including: eavesdropper, replay, online guessing, verifier impersonation and man-in-the-middle attacks.
7. Ensure that information systems accept and electronically verify **Agency** Verification (PIV) credentials.

**4.2 DEVICE IDENTIFICATION AND AUTHENTICATION****AGENCY** shall:1. Ensure that information systems uniquely identify and authenticate all devices before establishing a network connection.

**4.3** **IDENTIFIER MANAGEMENT****AGENCY**, through **Agency** information systems owners, shall:1. Ensure that the [**AGENCY**] manages information system identifiers by receiving authorization from [**Agency** defined personnel or roles] to assign an individual, group, role, or device identifier.
2. Select an identifier that identifies an individual, group, role, or device.
3. Assign the identifier to the intended individual, group, role, or device.
4. Prevent reuse of identifiers for 90 days.
5. Disable the identifier after 30 days of inactivity.

**4.4 AUTHENTICATOR MANAGEMENT****AGENCY** shall:1. Manage information system authenticators by verifying, as part of the initial authenticator distribution, the **Agency** of the individual, group, role, or device receiving the authenticator.
2. Establish initial authenticator content for authenticators defined by the organization.
3. Ensure that authenticators have sufficient strength of mechanism for their intended use.
4. Establish and implement administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators.
5. Change default content of authenticators prior to information system installation.
6. Establish minimum and maximum lifetime restrictions and reuse conditions for authenticators.
7. Change/refresh authenticators every 90 days.
8. Protect authenticator content from unauthorized disclosure and modification.
9. Require individuals and devices to implement specific security safeguards to protect authenticators.
10. Change authenticators for group/role accounts when membership to those account changes.
11. Ensure that information systems, for password-based authentication enforce minimum password complexity that must not contain the user's entire Account Name value or entire Full Name value.
12. Ensure passwords must contain characters from three of the following five categories:
13. Uppercase characters of European languages (A through Z, with diacritic marks, Greek and Cyrillic characters);
14. ii. Lowercase characters of European languages (a through z, sharp-s, with diacritic marks, Greek and Cyrillic characters);
15. Base 10 digits (0 through 9);
16. Non-alphanumeric characters ~!@#$%^&\*\_-+=`|\(){}[]:;"'<>,.?/; and
17. Any Unicode character that is categorized as an alphabetic character, but is not uppercase or lowercase. This includes Unicode characters from Asian languages.
18. Require passwords to have a minimum length of 8 characters.
19. Enforce at least one changed character when new passwords are created.
20. Store and transmit only cryptographically-protected passwords.
21. Enforce password minimum and maximum lifetime restrictions of one day and 120 days respectively.
22. Prohibit password reuse for 12 generations.
23. Allow the use of a temporary password for system logons with an immediate change to a permanent password.
24. Ensure that information system, for PKI-based authentication, validates certifications by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information.
25. Enforce authorized access to the corresponding private key.
26. Map the authenticated **Agency** to the account of the individual or group.
27. Implement a local cache of revocation data to support path discovery and validation in case of inability to access revocation information via the network.
28. Require that the registration process to receive [**Agency** defined types of and/or specific authenticators] be conducted in person or by a trusted third party before [**Agency** defined registration authority] with authorization by [**Agency** defined personnel or roles].
29. Ensure that the information system, for hardware token-based authentication, employs mechanisms that satisfy [CSA defined token quality requirements].

**4.5 AUTHENTICATOR FEEDBACK****Agency** shall:1. Ensure that information systems obscure feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

**4.6 CRYPTOGRAPHIC MODULE AUTHENTICATION****Agency** shall:1. Ensure that information systems implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable state and federal laws, directives, policies, regulations, standards, and guidance for such authentication.

**7. IDENTIFICATION AND AUTHENTICATION****Agency** shall:1. Ensure that information systems uniquely identify and authenticate non-Agency users or processes acting on behalf of non-Agency users.
2. Ensure that information systems accept and electronically verify Personal ID Agency Verification (PIV) credentials from other government agencies.
3. Ensure that information systems accept only Federal Agency, Credential, and Access Management (FICAM) Trust Framework Solutions initiative approved third-party credentials
4. Ensure that the organization employs only FICAM-approved information system components in [**Agency** defined information systems] to accept third- party credentials.
 |
| **Approved by / Date** | Highlight this text, then type name of person approving here | Highlight this text, then enter date of approval here |

|  |  |
| --- | --- |
| **Policy** | LINK/NCIC Policy |
| **Name of Procedure** | **Configuration Management** |
| **Reference Number** | 5.0 |
| **Applicable Parties** | **CJIS Users**: This includes any personnel who access Criminal Justice Information Systems, including full-access users and inquiry-only users.**Terminal Agency Coordinator (TAC)**: The individual responsible for overseeing CJIS System programs within the local agency and ensuring compliance with CJIS system policies.**Assistant Terminal Agency Coordinator (ATAC)**: The person who assists the TAC and assumes the TAC duties if they are unavailable.**Local Agency Security Officer (LASO):** Responsible for ensuring the security of CJIS systems and hardware, including personnel screening and reporting security incidents.**Private Contractors/Vendor Personnel**: Any third-party personnel who provide services that involve access to CJIS systems or secure locations. |
| **Effective Date** | Highlight this text, then type effective date here |
| **Purpose** | To ensure that **Agency** resources and information systems are established with effective security controls and control enhancements that reflect applicable federal and state laws, Executive Orders, directives, regulations, policies, standards, and guidance. |
| **Procedures** | This policy is applicable to all **Agency** and users of IT resources and assets.**5.1 BASELINE CONFIGURATION****Agency** shall:1. Develop, document, and maintain under configuration control, a current baseline configuration of information systems.
2. Review and update the baseline configuration of the information system annually.
3. Review and update the baseline configuration of the information system when required and as an integral part of information system component installations and upgrades.
4. Retain one previous version of baseline configurations of information systems to support rollback.
	1. **CONFIGURATION CHANGE CONTROL**

**Agency** shall:1. Determine the types of changes to the information system that are configuration-controlled.
2. Review proposed configuration-controlled changes to the information system and approve or disapprove such changes with explicit consideration for security impact analyses.
3. Document configuration change decisions associated with the information system.
4. Implement approved configuration-controlled changes to the information system.
5. Retain records of configuration-controlled changes to the information system for a minimum of one year.
6. Audit and review activities associated with configuration-controlled changes to the information system.
7. Coordinate and provide oversight for configuration change control activities through [Agency defined configuration change control element (e.g., committee, board)] that convenes [Agency defined frequency]; [Agency defined configuration change conditions].
8. Test, validate, and document changes to the information system before implementing the changes on the operational system.
	1. **SECURITY IMPACT ANALYSIS**

**Agency** shall:1. Analyze changes to the information system to determine potential security impacts prior to change implementation.
	1. **ACCESS RESTRICTIONS FOR CHANGE**

**Agency** shall:1. Define, document, approve, and enforce physical and logical access restrictions associated with changes to the information system.
	1. **CONFIGURATION SETTINGS**

**Agency** shall:1. Establish and document configuration settings for information technology products employed within the information system using [Agency defined security configuration checklists lists available at https://checklists.nist.gov] that reflect the most restrictive mode consistent with operational requirements.
2. Implement the configuration settings.
3. Identify, document, and approve any deviations from established configuration settings for [Agency defined information system components] based on CJIS Security Policy requirements.
4. Monitor and control changes to the configuration settings in accordance with policies and procedures.

**5.6 LEAST FUNCTIONALITY****Agency** shall:* 1. Configure the information system to provide only essential capabilities.
	2. Review the information system quarterly to identify unnecessary and/or non-secure functions, ports, protocols, and services.
	3. Disable functions, ports, protocols, and services within the information system deemed to be unnecessary and/or non-secure.
	4. Prevent program execution in accordance with policies regarding software program usage and restrictions and rules authorizing the terms and conditions of software program usage.
	5. Identify software programs not authorized to execute on information systems.
	6. Employ an allow-all, deny-by-exception policy to prohibit the execution of unauthorized software programs on the information system.
	7. Review and update the list of unauthorized software programs annually.
	8. **INFORMATION SYSTEM COMPONENT INVENTORY**

**Agency** shall:1. Develop and document an inventory of information system components that:
2. Reflects the current information system accurately.
3. Includes all components within the authorization boundary of the information system.
4. Is at the level of granularity deemed necessary for tracking and reporting.
5. Includes information deemed necessary to achieve effective information system component accountability.
6. Review and update the information system component inventory for a minimum of one year.
7. Update the inventory of information system components as an integral part of component installations, removals, and information system updates.
8. Employ automated mechanisms quarterly to detect the presence of unauthorized hardware, software, and firmware components within the information system.
9. Take the following actions when unauthorized components are detected:
10. Disable network access by such components, or
11. Isolate the components and notifies the Chief Information Officer and system owner.
12. Verify that all components within the authorization boundary of the information system are not duplicated in other information system component inventories.
	1. **CONFIGURATION MANAGEMENT PLAN**

IT shall develop, document, and implement a configuration management plan for the information system that:1. Addresses roles, responsibilities, and configuration management processes and procedures.
2. Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items.
3. Defines the configuration items for the information system and places the configuration items under configuration management.
4. Protects the configuration management plan from unauthorized disclosure and modification.
	1. **SOFTWARE USAGE RESTRICTIONS**

**Agency** shall:1. Use software and associated documentation in accordance with contract agreements and copyright laws.
2. Track the use of software and associated documentation protected by quantity licenses to control copying and distribution.
3. Control and document the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.
	* 1. **USER-INSTALLED SOFTWARE**

**Agency** shall:1. Establish policies governing the installation of software by users.
2. Enforce software installation policies through controlling privileged access and blocking the execution of files using policy applied by directory service and/or application whitelisting.
3. Monitor policy compliance monthly.
 |
| **Approved by / Date** | Highlight this text, then type name of person approving here | Highlight this text, then enter date of approval here |

|  |  |
| --- | --- |
| **Policy** | LINK/NCIC Policy |
| **Name of Procedure** | **Media Protection** |
| **Reference Number** | 6.0 |
| **Applicable Parties** | **CJIS Users**: This includes any personnel who access Criminal Justice Information Systems, including full-access users and inquiry-only users.**Terminal Agency Coordinator (TAC)**: The individual responsible for overseeing CJIS System programs within the local agency and ensuring compliance with CJIS system policies.**Assistant Terminal Agency Coordinator (ATAC)**: The person who assists the TAC and assumes the TAC duties if they are unavailable.**Local Agency Security Officer (LASO):** Responsible for ensuring the security of CJIS systems and hardware, including personnel screening and reporting security incidents.**Private Contractors/Vendor Personnel**: Any third-party personnel who provide services that involve access to CJIS systems or secure locations. |
| **Effective Date** | Highlight this text, then type effective date here |
| **Purpose** | To ensure that **Agency** resources and information systems are established with effective security controls and control enhancements that reflect applicable federal and state laws, Executive Orders, directives, regulations, policies, standards, and guidance. |
| **Procedures** | * 1. **MEDIA ACCESS:**

IT through direction from **Agency** shall:1. Restrict access to [Agency defined types of digital and/or non-digital media] to [Agency identified staff].
2. Mark information system media indicating the distribution limitations, handling caveats, and applicable security markings of digital and non-digital information media.
	1. **MEDIA STORAGE**

**Agency** shall:1. Specify staff to physically control and securely store media within defined controlled areas.
2. Protect information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.
	1. **MEDIA TRANSPORT**

**Agency** Shall:* 1. Protect and control media during transport outside of controlled areas.
	2. Maintain accountability for information system media during transport outside of controlled areas.
	3. Document activities associated with the transport of information system media.
	4. Restrict the activities associated with the transport of information system media to authorized personnel.
	5. **MEDIA SANITIZATION**

**Agency** shall:* 1. Sanitize prior to disposal, release out of organizational control, or release for reuse in accordance with applicable federal and CSA standards and policies.
	2. Employ sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.
	3. **MEDIA USE**

**Agency** shall:Prohibit the use of [Agency defined types of information system media] on Agency owned equipment using unapproved security safeguards.  |
| **Approved by / Date** | Highlight this text, then type name of person approving here | Highlight this text, then enter date of approval here |

|  |  |
| --- | --- |
| **Policy** | LINK/NCIC Policy |
| **Name of Procedure** | **Personnel Security Policy** |
| **Reference Number** | 7.0  |
| **Applicable Parties** | **CJIS Users**: This includes any personnel who access Criminal Justice Information Systems, including full-access users and inquiry-only users.**Terminal Agency Coordinator (TAC)**: The individual responsible for overseeing CJIS System programs within the local agency and ensuring compliance with CJIS system policies.**Assistant Terminal Agency Coordinator (ATAC)**: The person who assists the TAC and assumes the TAC duties if they are unavailable.**Local Agency Security Officer (LASO):** Responsible for ensuring the security of CJIS systems and hardware, including personnel screening and reporting security incidents.**Private Contractors/Vendor Personnel**: Any third-party personnel who provide services that involve access to CJIS systems or secure locations. |
| **Effective Date** | Highlight this text, then type effective date here |
| **Purpose** | To ensure that **Agency** resources and information systems are established with effective security controls and control enhancements that reflect applicable federal and state laws, Executive Orders, directives, regulations, policies, standards, and guidance. |
| **Procedures** | This policy is applicable to all **Agency** and users of IT resources and assets.* 1. **POSITION RISK DESIGNATION**

**Agency** shall:* 1. Assign a risk designation to all positions.
	2. Establish screening criteria for individuals filling those positions.
	3. Review and update position risk designations annually.
	4. **PERSONNEL SCREENING**

IT and **Agency** system and application owners shall:* 1. Screen individuals prior to authorizing access to the information systems.
	2. Rescreen individuals according to recommendation of CJIS Security Policy.
	3. Ensure personnel screening and rescreening activities reflect applicable state and federal laws, directives, regulations, policies, standards, guidance, and specific criteria established for the risk designations of assigned positions.
	4. **PERSONNEL TERMINATION**

**Agency** shall, upon termination of individual employment:* 1. Disable information system access within time period, as defined in the FBI CJIS Security Policy.
	2. Terminate/revoke any authenticators/credentials associated with the individual.
	3. Conduct exit interviews that include a discussion of the following:
		1. Retrieve all security-related information system-related property.
		2. Retain access to information and information systems formerly controlled by terminated individual.
		3. Notify [Agency defined personnel or roles] within 1 business day.

Information system-related property includes, for example, hardware authentication tokens, system administration technical manuals, keys, identification cards, and building passes. Exit interviews ensure that terminated individuals understand the security constraints imposed by being former employees and that proper accountability is achieved for information system-related property. Security topics of interest at exit interviews can include, for example, reminding terminated individuals of nondisclosure agreements and potential limitations on future employment. Exit interviews may not be possible for some terminated individuals.The Agency shall:* 1. Notify terminated individuals of applicable, legally binding post-employment requirements for the protection of information.
	2. Require terminated individuals to sign an acknowledgment of post-employment requirements as part of the termination process as directed by Counsel and Human Resources (HR).
	3. Employ automated mechanisms to notify [Agency defined personnel or roles] upon termination of an individual.
	4. **PERSONNEL TRANSFER**

**Agency** shall:1. Review and confirm ongoing operational need for current logical and physical access authorizations to information systems/facilities when individuals are reassigned or transferred to other positions.
2. Initiate transfer or reassignment notification according to LINK Provisions and Guidelines.
3. Modify access authorization as needed to correspond with any changes in operational need due to reassignment or transfer.
4. Notify [Agency defined personnel] immediately or **no later** than 1 business day of transfer.

This control applies when reassignments or transfers of individuals are permanent or of such extended durations as to make the actions warranted.* 1. **ACCESS AGREEMENTS**

**Agency** shall:1. Develop and document access agreements for information systems.
2. Review and update the access agreements annually.
3. Ensure that individuals requiring access to information and information systems:
4. Sign appropriate access agreements prior to being granted access.
5. Re-sign access agreements to maintain access to information systems when access agreements have been updated or in accordance with LINK Provisions and Guidelines.

Access agreements include, for example, nondisclosure agreements, acceptable use agreements, rules of behavior, and conflict-of-interest agreements. * 1. **THIRD-PARTY PERSONNEL SECURITY**

**Agency** shall:* 1. Establish and document personnel security requirements including security roles and responsibilities for third-party providers.
	2. Require third-party providers to comply with personnel security policies and procedures established by the **Agency**.
	3. Require third-party providers to notify [**Agency** defined personnel] of any personnel transfers or terminations of third-party personnel who possess credentials and/or badges, or who have information system privileges within [**Agency** defined time period].
	4. Monitor provider compliance.

Third-party providers include, for example, service bureaus, contractors, and other organizations providing information system development, information technology services, outsourced applications, and network and security management. * 1. **PERSONNEL SANCTIONS**

IT and HR shall:1. Employ a formal sanction process for individuals failing to comply with established information security policies and procedures
2. Notify [Agency defined personnel] immediately or within 1 business day when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.

Sanction processes reflect applicable state and federal laws, directives, regulations, policies, standards, and guidance. Sanctions processes are described in access agreements and can be included as part of general personnel policies and procedures for those organizations. Employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to IT resources, and other actions as well as both civil and criminal penalties. |
| **Approved by / Date** | Highlight this text, then type name of person approving here | Highlight this text, then enter date of approval here |

|  |  |
| --- | --- |
| **Policy** | LINK/NCIC Policy |
| **Name of Procedure** | **System and Information Integrity**  |
| **Reference Number** | 8.0 |
| **Applicable Parties** | **CJIS Users**: This includes any personnel who access Criminal Justice Information Systems, including full-access users and inquiry-only users.**Terminal Agency Coordinator (TAC)**: The individual responsible for overseeing CJIS System programs within the local agency and ensuring compliance with CJIS system policies.**Assistant Terminal Agency Coordinator (ATAC)**: The person who assists the TAC and assumes the TAC duties if they are unavailable.**Local Agency Security Officer (LASO):** Responsible for ensuring the security of CJIS systems and hardware, including personnel screening and reporting security incidents.**Private Contractors/Vendor Personnel**: Any third-party personnel who provide services that involve access to CJIS systems or secure locations. |
| **Effective Date** | Highlight this text, then type effective date here |
| **Purpose** | To ensure that **Agency** resources and information systems are established with effective security controls and control enhancements that reflect applicable federal and state laws, Executive Orders, directives, regulations, policies, standards, and guidance. |
| **Procedures** | This policy is applicable to all **Agency** and users of IT resources and assets.* 1. **FLAW REMEDIATION**

**Agency** shall:* 1. Identify, report, and correct information system flaws.
	2. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation.
	3. Install security-relevant software and firmware updates within 30 days of the release of the updates.
	4. Incorporate flaw remediation into the configuration management process.
	5. Employ automated mechanisms, in accordance with FBI CJIS Security Policy, to determine the state of information system components with regard to flaw remediation.

* 1. **MALICIOUS CODE PROTECTION**

**Agency** shall:* 1. Employ malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code.
	2. Update malicious code protection mechanisms whenever new releases are available in accordance with configuration management policy and procedures.
	3. Configure malicious code protection mechanisms to:
		1. Perform periodic scans of the information systems, as required in FBI CJIS Security Policy and real-time scans of files from external sources at endpoint; network entry/exit points as the files are downloaded, opened, or executed in accordance with the security policy.
		2. Block malicious code; quarantine malicious code; send alert to administrator immediately in response to malicious code detection.
		3. Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.
	4. **INFORMATION SYSTEM MONITORING**

**Agency** shall:1. Monitor the information system to detect:
2. Attacks and indicators of potential attacks.
3. Unauthorized local, network, and remote connections.
4. Identify unauthorized use of the information system through defined techniques and methods.
5. Deploy monitoring devices strategically within the information system to collect [**Agency** determined essential information] and at ad hoc locations within the system to track specific types of transactions of interest to the **Agency**.
6. Protect information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion.
7. Heighten the level of information system monitoring activity whenever there is an indication of increased risk to operations and assets, individuals, other organizations, or based on law enforcement information, intelligence information, or other credible sources of information.
8. Obtain legal opinion with regard to information system monitoring activities in accordance with applicable state and federal laws, directives, policies, or regulations.
9. Provide information system monitoring information to authorized personnel or business units as needed.
	1. **SYSTEM-GENERATED ALERTS**

**Agency** shall ensure that:1. The information system that may be generated from a variety of sources, including, for example, audit records or inputs from malicious code protection mechanisms, intrusion detection or prevention mechanisms, or boundary protection devices such as firewalls, gateways, and routers will be disseminated to authorized personnel or business units that shall take appropriate action on the alert(s).
2. Alerts be transmitted telephonically, electronic mail messages, or by text messaging as required. Personnel on the notification list can include system administrators, mission/business owners, system owners, or information system security officers.
	1. **SECURITY ALERTS, ADVISORIES, AND DIRECTIVES**

**Agency** shall:* 1. Receive information system security alerts, advisories, and directives from [Agency defined external organizations] on an ongoing basis.
	2. Generate internal security alerts, advisories, and directives as deemed necessary.
	3. Disseminate security alerts, advisories, and directives to: [Agency defined personnel or roles]; [Agency defined elements within the organization]; [Agency defined external organizations].
	4. Implement security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance.
	5. **SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY**

**Agency** shall:* 1. Employ integrity verification tools to detect unauthorized changes to [Agency defined software, firmware, and information];
	2. Ensure the information system performs an integrity check of [Agency defined software, firmware, and information] at startup, and/or at [Agency defined transitional states or security-relevant events], in accordance with FBI CJIS Security Policy.
	3. Incorporate the detection of unauthorized [Agency defined security-relevant changes to the information system] into the incident response capability.
	4. **SPAM PROTECTION**

**Agency** shall:* 1. Employ spam protection mechanisms at information system entry and exit points to detect and take action on unsolicited messages.
	2. Update spam protection mechanisms when new releases are available in accordance with the configuration management policy and procedures.
	3. Manage spam protection mechanisms centrally.
	4. Ensure information systems automatically update spam protection mechanisms.
	5. **INFORMATION INPUT VALIDATION**

**Agency** shall:1. Ensure the information system:
2. Checks the validity of the following:
	1. License Plate Numbers
	2. Driver’s license numbers
	3. Names and DOBs
	4. ORI numbers
	5. Vehicle identification number (VINs)
	6. Warrant or Protection Order entries
	7. Firearms serial numbers entered for checks
3. Provides a manual override capability for input validation of [Agency defined inputs].
4. Restricts the use of the manual override capability to only [Agency defined authorized individuals].
5. Audits the use of the manual override capability.
6. Reviews and resolve within input validation errors.
7. Behaves in a predictable and documented manner that reflects system objectives when invalid inputs are received.
	1. **ERROR HANDLING**

**Agency** shall:1. Ensure the information system:
	* 1. Generates error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries.
		2. Reveals error messages only to [Agency defined personnel or roles].
		3. **INFORMATION HANDLING AND RETENTION**

**Agency** shall:1. Handle and retain information within the information system and information output from the system in accordance with applicable state and federal laws, directives, policies, regulations, standards, and operational requirements.
	* 1. **MEMORY PROTECTION**

**Agency** shall:1. Implement security safeguards for memory protection, included, but not limited to, enabling Data Execution Prevention (DEP), Address Space Layout Randomization (ASLR), Secure Boot protections, restricting unauthorized script executions, and deploying endpoint protection platforms capable of detecting and blocking memory-based exploits. Exceptions to these protections shall be documented and approved by agency security personnel.
 |
| **Approved by / Date** | Highlight this text, then type name of person approving here | Highlight this text, then enter date of approval here |

|  |  |
| --- | --- |
| **Policy** | LINK/NCIC Policy |
| **Name of Procedure** | **Access Control** |
| **Reference Number** | 9.0 |
| **Applicable Parties** | **CJIS Users**: This includes any personnel who access Criminal Justice Information Systems, including full-access users and inquiry-only users.**Terminal Agency Coordinator (TAC)**: The individual responsible for overseeing CJIS System programs within the local agency and ensuring compliance with CJIS system policies.**Assistant Terminal Agency Coordinator (ATAC)**: The person who assists the TAC and assumes the TAC duties if they are unavailable.**Local Agency Security Officer (LASO):** Responsible for ensuring the security of CJIS systems and hardware, including personnel screening and reporting security incidents.**Private Contractors/Vendor Personnel**: Any third-party personnel who provide services that involve access to CJIS systems or secure locations. |
| **Effective Date** | Highlight this text, then type effective date here |
| **Purpose** | To ensure that **Agency** resources and information systems are established with effective security controls and control enhancements that reflect applicable federal and state laws, Executive Orders, directives, regulations, policies, standards, and guidance. |
| **Procedures** | * 1. **ACCOUNT MANAGEMENT**

**Agency** shall:1. Identify and select the following types of information system accounts to support organizational missions and business functions: individual, shared, group, system, guest/anonymous, emergency, developer/manufacturer/vendor, temporary, and service.
2. Assign account managers for information system accounts.
3. Establish conditions for group and role membership.
4. Specify authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account.
5. Require approvals by system owners for requests to create information system accounts.
6. Create, enable, modify, disable, and remove information system accounts in accordance with approved procedures.
7. Monitor the use of information system accounts.
8. Notify account managers when accounts are no longer required, when users are terminated or transferred, and when individual information system usage or need-to-know changes.
9. Authorize access to the information system based on a valid access authorization or intended system usage.
10. Review accounts for compliance with account management requirements, at a minimum annually.
11. Establish a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.
12. Employ automated mechanisms to support the management of information system accounts.
13. Ensure that the information system automatically disables temporary and emergency accounts after usage.
14. Ensure that the information system automatically disables inactive accounts, in accordance with FBI CJIS Security Policy.
15. Ensure that the information system automatically audits account creation, modification, enabling, disabling, and removal actions, and notifies appropriate IT personnel.
	1. **ACCESS ENFORCEMENT**

**Agency** shall:1. Ensure that the information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.
	1. **INFORMATION FLOW ENFORCEMENT**

**Agency** shall:1. Ensure that the information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on applicable policy.
	1. **SEPARATION OF DUTIES**

**Agency** shall:* 1. Separate duties of individuals as necessary, to prevent malevolent activity without collusion.
	2. Document the separation of duties of individuals.
	3. Define information system access authorizations to support separation of duties.
	4. **LEAST PRIVILEGE**

**Agency** shall:1. Employ 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.
2. Authorize explicitly access to hardware and software controlling access to systems and filtering rules for routers/firewalls, cryptographic key management information, configuration parameters for security services, and access control lists.
3. Require that users of information system accounts, or roles, with access to [Agency defined security functions or security-relevant information], use non-privileged accounts or roles, when accessing non-security functions.
4. Restrict privileged accounts on the information system to [Agency defined personnel or roles].
5. Ensure that the information system audits the execution of privileged functions.
6. Ensure that the information system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.
	1. **UNSUCCESSFUL LOGON ATTEMPTS**

**Agency** shall ensure that the information system:1. Enforces a limit of five (5) consecutive invalid login attempts by a user during a 15-minute period; and
2. Automatically lock the account or node until released by the administrator when the maximum number of unsuccessful attempts is exceeded.
3. The system shall automatically lock the account/node for a 10-minute time period unless released by an administrator.
	1. **SYSTEM USE NOTIFICATION**

**Agency** shall ensure that the information system:1. Displays to users an approved system use notification message or banner before granting access to the system that provides privacy and security notices consistent with applicable state and federal laws, directives, policies, regulations, standards, and guidance and states informing that:
2. Users are accessing a [**Agency**] information system.
3. Information system usage may be monitored, recorded, and subject to audit.
4. Unauthorized use of the information system is prohibited and subject to criminal and civil penalties.
5. Use of the information system indicates consent to monitoring and recording.
6. There are not rights to privacy.
7. Retains the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the information system.
8. For publicly accessible systems, the **Agency** shall ensure that the information system:
9. Displays system use information before granting access.
10. Displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities.
11. Includes a description of the authorized uses of the system.
	1. **SESSION LOCK**

**Agency** shall ensure that the information system:1. Prevent further access to the system by initiating a session lock after 30 minutes of inactivity or upon receiving a request from a user. NOTE: This does not apply to systems used for dispatch functions or criminal justice conveyance.
2. Retain the session lock until the user reestablishes access using established identification and authentication procedures.
3. Conceal, via the session lock, information previously visible on the display with a publicly viewable image.
	1. **SESSION TERMINATION**

**Agency** shall:1. Ensure that the information system automatically terminates a user session after a user has been logged out.
	* 1. **PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION**

**Agency** shall:1. Identify user actions that can be performed on the information system without identification or authentication consistent with organizational missions and business functions.
2. Document and provide supporting rationale in the security plan for the information system, user actions not requiring identification or authentication.
	* 1. **REMOTE ACCESS**

**Agency** shall:1. Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed.
2. Authorize remote access to the information system prior to allowing such connections.
3. Ensure that the information system monitors and controls remote access methods.
4. Ensure that the information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.
5. Ensure that the information system routes all remote accesses through [Agency defined number] managed network access control points to reduce the risk for external attacks.
6. Authorize the execution of privileged commands and access to security-relevant information via remote access only for [Agency defined needs].
7. Document the rationale for such access in the security plan for the information system.
	* 1. **WIRELESS ACCESS**

**Agency** shall:1. Establish usage restrictions, configuration/connection requirements, and implementation guidance for wireless access.
2. Authorize wireless access to the information system prior to allowing such connections.
3. Ensure that the information system protects wireless access to the system using authentication of users and devices and encryption.
	* 1. **ACCESS CONTROL FOR MOBILE DEVICES**

**Agency** shall:1. Establish usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices.
2. Authorize the connection of mobile devices to organizational information systems.
3. Employ full-device encryption or container encryption to protect the confidentiality and integrity of information on approved devices.
	* 1. **USE OF EXTERNAL INFORMATION SYSTEMS**

**Agency** shall:1. Establish terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to:
2. Access the information system from external information systems.
3. Process, store, or transmit organization-controlled information using external information systems.
4. Permit authorized individuals to use an external information system to access the information system or to process, store, or transmit organization-controlled information only when the organization:
5. Verifies the implementation of required security controls on the external system as specified in the organization’s information security policy and security plan.
6. Retains approved information system connection or processing agreements with the organizational **Agency** hosting the external information system.
	* 1. **INFORMATION SHARING**

**Agency** shall:* 1. Facilitate information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for [Agency defined information sharing circumstances where user discretion is required].
	2. Employ processes to assist users in making information sharing/collaboration decisions.
		1. **PUBLICLY ACCESSIBLE CONTENT**

**Agency** shall:1. Designate individuals authorized to post information onto a publicly accessible information system.
2. Train authorized individuals to ensure that publicly accessible information does not contain nonpublic information.
3. Review the proposed content of information prior to posting onto the publicly accessible information system to ensure that nonpublic information is not included.
4. Review the content on the publicly accessible information system for nonpublic information monthly.
 |
| **Approved by / Date** | Highlight this text, then type name of person approving here | Highlight this text, then enter date of approval here |

|  |  |
| --- | --- |
| **Policy** | LINK/NCIC Policy |
| **Name of Procedure** | **Awareness and Training** |
| **Reference Number** | 10 |
| **Applicable Parties** | **CJIS Users**: This includes any personnel who access Criminal Justice Information Systems, including full-access users and inquiry-only users.**Terminal Agency Coordinator (TAC)**: The individual responsible for overseeing CJIS System programs within the local agency and ensuring compliance with CJIS system policies.**Assistant Terminal Agency Coordinator (ATAC)**: The person who assists the TAC and assumes the TAC duties if they are unavailable.**Local Agency Security Officer (LASO):** Responsible for ensuring the security of CJIS systems and hardware, including personnel screening and reporting security incidents.**Private Contractors/Vendor Personnel**: Any third-party personnel who provide services that involve access to CJIS systems or secure locations. |
| **Effective Date** | Highlight this text, then type effective date here |
| **Purpose** | To ensure that **Agency** resources and information systems are established with effective security controls and control enhancements that reflect applicable federal and state laws, Executive Orders, directives, regulations, policies, standards, and guidance. |
| **Procedures** | This policy is applicable to all **Agency** and users of IT resources and assets.* 1. **SECURITY AWARENESS TRAINING**

The [Agency] shall: 1. Schedule security awareness training as part of initial training for new users.
2. Schedule security awareness training when required by information system changes and then annually thereafter.
3. IT shall determine the appropriate content of security awareness training and security awareness techniques based on the specific organizational requirements and the information systems to which personnel have authorized access. The content shall:
4. Include a basic understanding of the need for information security and user actions to maintain security and to respond to suspected security incidents.
5. Address awareness of the need for operations security. Security awareness techniques can include, for example, displaying posters, offering supplies inscribed with security reminders, generating email advisories/notices from senior organizational officials, displaying logon screen messages, and conducting information security awareness events.
	1. **SECURITY AWARENESS | INSIDER THREAT**

**Agency** shall:1. Include security awareness training on recognizing and reporting potential indicators of insider threat.
	1. **ROLE-BASED SECURITY TRAINING**

**Agency** shall:1. Provide role-based security training to personnel with assigned security roles and responsibilities:
2. Before authorizing access to the information system or performing assigned duties.
3. When required by information system changes and annually thereafter.
4. Designate personnel to receive initial and ongoing training in the employment and operation of environmental controls to include, for example, fire suppression and detection devices/systems, sprinkler systems, handheld fire extinguishers, fixed fire hoses, smoke detectors, temperature/humidity, HVAC, and power within the facility.
	1. **PHYSICAL SECURITY CONTROLS**

**Agency** shall:1. Provide initial and ongoing training in the employment and operation of physical security controls; physical security controls include, for example, physical access control devices, physical intrusion alarms, monitoring/surveillance equipment, and security guards (deployment and operating procedures).
2. Identify personnel with specific roles and responsibilities associated with physical security controls requiring specialized training.
	1. **PRACTICAL EXERCISES**

**Agency** shall:1. Provide practical exercises in security training that reinforce training objectives; practical exercises may include, for example, security training for software developers that includes simulated cyber-attacks exploiting common software vulnerabilities (e.g., buffer overflows), or spear/whale phishing attacks targeted at senior leaders/executives. These types of practical exercises help developers better understand the effects of such vulnerabilities and appreciate the need for security coding standards and processes.
	1. **SUSPICIOUS COMMUNICATIONS AND ANOMALOUS SYSTEM BEHAVIOR**

**Agency** shall:1. Provide training to its specified staff on how to recognize suspicious communications and anomalous behavior in organizational information systems.
	1. **SECURITY TRAINING RECORDS**

The [**Agency**] shall:1. Designate personnel to document and monitor individual information system security training activities including basic security awareness training and specific information system security training.
2. Retain individual training records for an audit cycle.
 |
| **Approved by / Date** | Highlight this text, then type name of person approving here | Highlight this text, then enter date of approval here |

|  |
| --- |
| **Review/Revision History for CJIS Security Policy:**Each time the above information pertinent to these Policies and Procedures is:* Reviewed for accuracy and no changes made, enter the date of the review, the person doing the review and a brief description such as “Reviewed by \_\_\_\_\_\_\_\_\_\_\_\_. No revisions needed.”
* Reviewed for accuracy and revision(s) made, enter the date of the revision(s), the name of the person making the revision(s), and a detailed description of the change(s) such as “Reviewed by Sally Doe. Employment status of Dispatcher Elizabeth Watson updated to Inactive.”
 |
| Date of Review/Revision | Person Reviewing/Revising | Description |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**ADDENDUM: THIRD PARTY SERVICE PROVIDERS**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name of Service Provider&Address | Service Provided(Attach contract to electronic file, especially Non-disclosure agreement) | Employee Responsible for Regular Review of Service Provider | Last Renewal Date | Next Renewal Date |
|  | (Website) |  |  |  |
|  | (IT consultant) |  |  |  |
|  | (Shredding company) |  |  |  |
|  | (Cleaning staff) |  |  |  |
|  | (Storage warehouse) |  |  |  |
|  | (Supply services / deliveries) |  |  |  |
|  | (Vendors) |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
| **Review/Revision History of Relationship with Third Party Service Providers:**Each time the above information pertinent to Third Party Service Providers is:* Reviewed for accuracy and no changes made, enter the date of the review, the person doing the review and a brief description such as “Reviewed by \_\_\_\_\_\_\_\_\_\_\_\_. No revisions needed.”
* Reviewed for accuracy and revision(s) made, enter the date of the revision(s), the name of the person making the revision(s), and a detailed description of the change(s) such as “Reviewed by Sally Doe. John Wilson removed as Wire Initiator and added as Wire Approver.”
 |
| Date of Review/Revision | Person Reviewing/Revising | Description |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |