Policy Title:	Agency Security Policy
Effective Date:	
Revision Date:	Every 2 years or as needed
Approval(s):	
LASO:	
CSO:	
Agency Head:	

Purpose:
The overriding goal of this policy is to protect Criminal Justice Information (CJI) and CJI systems from unauthorized disclosure, alteration, or misuse. It is meant to ensure that all *[agency name]* personnel authorized to collect, store, maintain, disseminate, or otherwise access CJI data conform to all rules and regulations set forth by CJIS Security Policy and applicable state statutes and policies. This policy adopts the security requirements of the CJIS Security Policy as a minimum set of requirements.

Scope:
This policy applies to all agency personnel with access to CJI providing security requirements associated with the creation, viewing, modification, transmission, dissemination, storage, or destruction of CJI.

Authorized *[agency name]* personnel will take appropriate safeguards for protecting CJI to limit potential mishandling or loss. Any inadvertent or inappropriate CJI disclosure and/or use will be reported to the *[agency name]* Local Agency Security Officer (LASO).

Definitions:

A. **Administration of Criminal Justice** -- as per 28 CFR (Code of Federal Regulations) 20.3(b), the performance of any of the following activities: detection, apprehension, detention, pretrial release, post-trial release, prosecution, adjudication, correctional supervision, or rehabilitation of accused persons or criminal offenders. The administration of criminal justice shall include criminal identification activities and the collection, storage, and dissemination of criminal history record information.
B. **Authorized Personnel** -- A Agency Name employee who has been properly vetted for access to CJI, including a fingerprint-based background check, completion of the required security awareness training, and signature of the Security Addendum Certification Page.
C. **Criminal History Record Information (CHRI)** — A subset of CJI. Any notations or other written or electronic evidence of an arrest, detention, complaint, indictment, information or other formal criminal charge relating to an identifiable person that includes identifying information regarding the individual, as well as the disposition of any charges. CHRI shall only be used for an authorized purpose consistent with the purpose for which III was accessed.

D. **Criminal Justice Information (CJI)** – In general, any information obtained from an FBI or CSA CJIS system including, but not limited to, biometric, identity history, biographic, property, and case/incident history that has not been officially released to the public or otherwise authorized for release by court order.
E. **CJIS Systems Agency (CSA)** – The state agency providing statewide (or equivalent) service to its criminal justice and non-criminal justice users with respect to the CJIS data from various systems managed by the FBI CJIS Division. The CSA for _____ is _____.
F. **Criminal Justice Agency (CJA)** - As per 28 CFR 20.3(g), Criminal justice Agency means:
(1) Courts; and
(2) A governmental agency or any subunit thereof that performs the administration of criminal justice pursuant to a statute or executive order, and that allocates a substantial part of its annual budget (more than 50%) to the administration of criminal justice. State and Federal Inspector General Offices are included as Criminal Justice Agencies.
Dissemination -- The transmission/distribution of CJI/CHRI to Authorized Recipients within an agency.
G. **NCIC –** The National Crime Information Center.
H. **Non-criminal Justice Agency (NCJA)** –- A governmental agency or any subunit thereof that provides services primarily for purposes other than the administration of criminal justice.
I. **Secondary Dissemination** — The transmission/distribution of CJI/CHRI from an agency to another authorized recipient agency, when the recipient agency has not been previously identified in a formal Information Exchange Agreement.
J. **Personally Identifiable Information (PII)** –- Defined as information about a person that contains some unique identifiers, including but not limited to name or Social Security Number, from which the identity of the person can be determined.

Physical Security:
Users shall adhere to all requirements of the *[agency name]* CJI Related Physical Protection Policy.

Technical Security
Users shall adhere to all technical security related requirements of this policy. Any questions should be forwarded to *[agency name]* IT for clarification.

Security and Awareness Training
Access to CJI shall be restricted to the users who have met the Security and Awareness Training requirements specified in the CJIS Security Policy for access to CJI. All training records shall be maintained by the *[agency name]*.

1. Persons with unescorted access to CSP-defined Physically Secure Locations shall complete basic Security and Awareness Training. These personnel do not perform any functions relating to the administration of criminal justice. This training is currently referred to as "Level 1" training.
2. All persons with access to CJI: Security and Awareness Training shall be required within six months of initial assignment, and biennially thereafter, for all employees who have access to CJI. This training is currently referred to as "Level 2" training.
3. Persons with logical access to CJIS applications: Users whose responsibilities include query or entry of CJI via CJIS systems shall successfully complete CJIS certification training. Training must be renewed biennially. This training is currently referred to as "Level 3" training.
4. Information Technology employees: In addition to training specified in 1), 2), and 3) above, IT employees shall complete CJIS Security and Awareness Training. Training must be renewed biennially. This training is currently referred to as "Level 4" training.

NCIC Data

In accordance with the NCIC Operations Manual, users and systems must meet the requirements of the CJIS Security Policy prior to cutting or copying and pasting from an NCIC response into a local system. Local systems include email, records management system (RMS), jail management system, or any other computer application or storage medium.

CJI Information E-Mailed

All users wishing to email CJI must use an encrypted email account for sending CJI. No unencrypted CJI may be emailed wherein that email is accessible via a public network.

Personally Identifiable Information (PII)

[agency name] personnel shall protect Personally Identifiable Information (PII) using the security policies mandated for CJI.

Misuse of CJI

1. Misuse of CJI can take many forms. Some examples of misuse, but not limited to, include:
    a. Any unauthorized access, disclosure, modification, destruction, handling, transmission, or deletion of CJI, whether by malice or mistake.
    b. Any attempt to intercept or otherwise obtain CJI by means other than those authorized by governing authority.
    c. Any use of CJI for personal reasons, especially involving personal relationships.
    d. Any use of CJI for political purposes.

e. Any use of CJI for monetary gain.
f. Any use of CJI to satisfy one's curiosity.
g. Performing or assisting in the performance of any act that will interfere with the authorized use of CJI.
h. Any violation of CJI related policies may constitute CJI misuse.

2. Any suspected misuse of CJI data will be immediately investigated to determine the type, degree, intent, and consequence of the misuse. A substantiated violation of the NCIC or CHRI shall result in such sanctions as specified by policy or deemed appropriate by the *[agency name]* agency authority. Additional penalties for violations of this policy may include immediate removal of access to CJIS system and data. Subsequent violations of this policy may result in disciplinary action up to and including termination.
3. Substantiated misuse of the system must be reported to the CSA ISO.
4. Any misuse that constitutes a violation of a CJI-related security policy must be reported in accordance with the procedures in the *[agency name]* CJI Incident Response Plan.

Information Exchange/Secondary Dissemination (CSP Section 5.1.1)

1. Dissemination of CJI/CHRI is restricted to authorized agencies and personnel only.

2. Prior to sharing, disseminating, or forwarding CJI to another entity, authorized *[agency name]* personnel must validate that the other entity and person are authorized to receive CJI/CHRI. Questions regarding whether an entity is authorized should be referred to the CSA _____.

3. If the person or agency is unknown to *[agency name]* personnel,

- Ask to see the requestor's credentials.
- Ask the requestor's supervisor's name and phone number.
- Ask the requestor to identify their agency and their agency's ORI.
- Contact the agency using a phone number found on the Internet for the agency (do not use the number provided by the individual).
- Ask for the supervisor and confirm the requestor works for the agency and that the requestor is authorized to receive CJI.

- Log the dissemination in the secondary dissemination log.

Authentication Strategy & Authenticator Management
(CSP Section 5.6.2 & 5.6.3.2 {2})

1. All users will comply with *[agency name]* Computer Use policies in regard to the access to and use of *[agency name]* computer hardware, software, network, and technology systems. Access to *Application* is controlled through the use of a unique username and password. All passwords must comply with the CJIS Security Policy (CSP).

2. *Application* uses usernames and passwords for identification and authentication. New users are assigned usernames as part of their on-boarding as an *[agency name]* employee for roles requiring *Application* access. *Application* users are notified by email/hard copy of their username and initial password. Users are required to change their initial password the first time they log onto *Application*.

3. In the event a user forgets their password, they will contact XXXXX (person) via email and request a password reset. XXXXX will notify the user of the password reset. Users will immediately login and change their password.

4. When a user no longer requires access to *Application*, XXXXX will be notified by the user's supervisor via email. XXXXX will deactivate or, if needed, change the user's access level if appropriate.

5. Users must not share the passwords with other *[agency name]* personnel. Users will not post their passwords anywhere near their monitors, or hide them in or around their desks. If needed, it is suggested that a user keeps a private log (not stored around their work area) or uses a password "manager" on their smartphone or computer.

6. In the event a user's password is compromised or the user suspects that it might be compromised, the user will take appropriate measures to change their password and notify their supervisor.

CJI Related Media Protection (Section 5.8, 5.8.3 & 5.8.4)

1. Any electronic (e.g. thumb drive, hard drive, CD/DVD, server disk) or physical (e.g. printed) media containing CJI shall be protected against unauthorized disclosure or release while being stored, accessed or physically transported from *[agency name]* to another approved location. Transporting CJI outside *[agency name]'s* assigned Physically Secure area shall be continually monitored and controlled by *[agency name]* personnel.

2. Controls shall be in place to protect electronic and physical media containing CJI while being stored, transmitted/transported, or actively being accessed.

3. To protect CJI, *[agency name]* personnel shall:
    a. Securely store electronic and physical media in an appropriate container. An appropriate container includes a locked drawer, cabinet, or room.
    b. Restrict access to electronic and physical media to CJI authorized personnel only.
    c. Ensure that only authorized personnel have access to printed form or digital media CJI.

d. Physically protect CJI until the media's end of life. CJI at end of life shall be destroyed or sanitized using approved equipment, techniques and procedures.
e. Not use personally owned information systems to access, process, store, or transmit CJI unless *[agency name]*has established and documented the specific terms and conditions for personally owned information system use. (CSP Section 5.5.6.1)
f. Not utilize publicly accessible computers to access, process, store, or transmit CJI. Publicly accessible computers include but are not limited to: hotel business center computers, convention center computers, public library computers, public kiosk computers, etc.
g. Store all hardcopy CJI printouts in a locked secure area or locked cabinet/desk accessible to only CJI authorized personnel.
h. Safeguard all CJI against unauthorized access or possible misuse.
i. Take appropriate action when in possession of CJI while not in a physically secure area:
    i. CJI must not leave the authorized employee's immediate control. CJI printouts shall not be left unsupervised when physical controls are not in place.
    ii. Precautions shall be taken to obscure CJI from public view, such as by means of an opaque file folder or envelope for hard copy printouts. For electronic devices like laptops, use session lock and/or privacy screens. CJI shall not be left in plain view.
    iii. When CJI is electronically transmitted outside the boundary of a Physically Secure Location, the data shall be immediately protected using encryption.
    iv. *[agency name]*personnel shall only use storage devices that are approved by *[agency name]*IT. Storage devices include external hard drives from computers, printers and copiers used with CJI. In addition, storage devices include thumb drives, flash drives, backup tapes, mobile devices, laptops, etc.
    v. *[agency name]* IT will ensure all external storage devices meet CJIS Security Policy (CSP) standards. When encryption is employed, the cryptographic module used shall be certified to meet FIPS 140-2 standards.
    vi. Lock or log-off computer when not in the immediate vicinity of the work area to protect CJI. Not all personnel have the same CJI access permissions, and CJI needs to be kept protected on a need-to-know basis.
    vii. Establish appropriate administrative, technical and physical safeguards to ensure the integrity, security, and confidentiality of CJI. (See Physical Protection Policy.)

4. Dissemination to another agency is authorized if the other agency is an Authorized Recipient of such information and is being supported by *[agency name]*, and has requested CJI to perform a recognized criminal justice function.

5. *[Agency name]* personnel shall dispose of electronic and physical media according to agency Media Disposal policy.

Breach Notification and Incident Reporting:
The agency shall promptly report incident information to appropriate authorities according to agency Incident Reporting policy. Information security events and weaknesses associated with information systems shall be communicated in a manner allowing timely corrective action to be taken. Incident-related information can be obtained from a variety of sources including, but not limited to, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports.

Roles and Responsibilities:
If CJI is improperly disclosed, lost, or reported as not received, the following procedures must be immediately followed:

1. *[agency name]* personnel shall notify his/her supervisor or LASO, and an incident-report form must be completed and submitted within 24 hours of discovery of the incident. The submitted report is to contain a detailed account of the incident, events leading to the incident, and steps taken/to be taken in response to the incident. (Agency Discretion)
2. The supervisor will communicate the situation to the LASO to notify of the loss or disclosure of CJI records.
3. The LASO will ensure the CSA ISO (CJIS System Agency Information Security Officer) is promptly informed of security incidents.
4. The CSA ISO will:
    a. Establish a security incident response and reporting procedure to discover, investigate, document, and report to the CSA, the affected criminal justice agency, and the FBI CJIS Division ISO major incidents that significantly endanger the security or integrity of CJI.
    b. Collect and disseminate all incident-related information received from the Department of Justice (DOJ), FBI CJIS Division, and other entities to the appropriate local law enforcement POCs within their area.
    c. Act as a single POC for their jurisdictional area for requesting incident response assistance.

Penalties:
Violation of any of the requirements in this policy by any authorized personnel will result in suitable disciplinary action, up to and including loss of access privileges, civil and criminal prosecution and / or termination.

Acknowledgement:
I have read the policy and rules above and I will:

- Abide by the *[agency name]*'s Security Policy. I understand any violation of this policy may result in discipline up to and including termination.
- Report any *[agency name]* CJI security incident to Supervisor and / or LASO as identified in this policy.

Signature: _____ Date: _____/2012____

Questions
Any questions related to this policy may be directed to the *[agency name]*'s LASO:

LASO Name:	LASO Phone:	LASO email:
State C/ISO Name:	C/ISO Phone:	C/ISO email:

Other Related Policy Reference:

- Media Protection Policy
- Media Disposal Policy
- Physical Protection Policy
- Incident Reporting Policy