
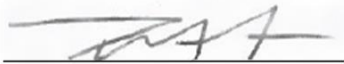


<b>POLICY TITLE: CRIMINAL JUSTICE INFORMATION SYSTEM SECURITY</b>		<b>PAGE 1 OF 8</b>
<b>POLICY NUMBER: 5.6</b>		
<b>CHAPTER 5: MANAGEMENT INFORMATION SYSTEM</b>		
	<b>STATE of MAINE</b> <b>DEPARTMENT of CORRECTIONS</b>  <b>Approved by Commissioner:</b> 	<b>PROFESSIONAL STANDARDS:</b>  <b>See Section VIII</b>
	<b>EFFECTIVE DATE:</b> <b>December 21, 2015</b>	<b>LATEST REVISION:</b> <b>February 20, 2024</b>

## I. AUTHORITY

The Commissioner of Corrections adopts this policy pursuant to the authority contained in 34-A M.R.S.A. Section 1403.

## II. APPLICABILITY

Entire Maine Department of Corrections

## III. POLICY

This policy establishes procedures that govern access to and transmission, storage, and destruction of Criminal Justice Information (CJI) in compliance with the requirements of the FBI CJIS Security Policy, the Maine Department of Administrative and Financial Services, Office of Information Technology policies, and other applicable state and federal regulations and policies. Moreover, it mandates regular audits to ensure compliance.

## IV. DEFINITIONS

1. Agency Agreement - a written agreement between the Maine Department of Corrections and its facilities, community corrections regions, and Central Office, as applicable, and the Maine State Police (MSP), State Bureau of Identification (SBI) specifying the terms and conditions for the Department to access and receive computerized Criminal Justice Information from the SBI.
2. [CJIS Security Policy](#) - the security policy established by the FBI that must be followed in exchange for access to Criminal Justice Information.
3. Criminal Justice Information (CJI) - data necessary for criminal justice agencies to perform their mission and enforce the laws, including, but not limited to, biometric, identity history, person, organization, property (when accompanied by any personally identifiable information), and case/incident history data. In addition, CJI refers to the FBI CJIS-provided data necessary for civil agencies to perform their mission, including, but not limited to data used to make hiring decisions.
4. Criminal Justice Information Services (CJIS) - a division of the United States Federal Bureau of Investigation (FBI) whose mission is to reduce terrorist and criminal activities by maximizing the ability to provide timely and relevant criminal justice information to the

FBI and to qualified law enforcement, criminal justice, civilian, academic, employment, and licensing agencies concerning individuals, stolen property, criminal organizations/activities, and other law enforcement-related data.

5. Local Agency Security Officer (LASO) - Department employee responsible for oversight and compliance with this policy and who serves as a liaison to the MSP information security officer (ISO) for any security related matters, including technical security audits.
6. Multi-factor authentication - requires the use of two or more different factors to verify identity to access CJI.
7. Physical media - printed documents and imagery that contain Criminal Justice Information.
8. Terminal Agency Coordinator (TAC) - a role required by the FBI Criminal Justice Information Services (CJIS) Security Policy filled by a Department employee who serves as a point-of-contact relating to CJIS information access. Also, a TAC is a liaison to the Maine State Police Access Integrity Unity (AIU) for METRO/NCIC audits (for their use of III Criminal History).

## V. CONTENTS

Procedure A:	Criminal Justice Information System Security, General
Procedure B:	Terminal Agency Coordinator (TAC) Responsibilities
Procedure C:	Local Agency Security Officer (LASO) Responsibilities
Procedure D:	Criminal Justice Information Access
Procedure E:	Account Management
Procedure F:	Security Awareness Training
Procedure G:	Incident Response
Procedure H:	Disposal of Criminal Justice Information
Procedure I:	Agency Agreements

## VI. ATTACHMENTS

Attachment A:	<a href="#">Security Addendum (FBI CJIS form)</a>
Attachment B:	<a href="#">CJIS Security Incident Reporting Form</a>

## VII. PROCEDURE

### Procedure A: Criminal Justice Information System Security, General

1. The Maine State Police, State Bureau of Identification is the designated CJIS System Agency (CSA) for the State of Maine that provides oversight to Maine’s criminal justice agencies with respect to Criminal Justice Information (CJI) from various systems managed by the FBI CJIS Division.
2. This policy:
  - a. applies to all staff, volunteers, student interns and other persons with access to the Department’s CJI information or in a location where CJI is accessible; and
  - b. pertains to all equipment that is owned or leased by the Department that processes, stores, and/or transmits CJI to include, but not limited to, any equipment that accesses the Maine Telecommunications and Routing Operations System (METRO) or CORIS (Corrections Information System).

POLICY NUMBER/TITLE	CHAPTER NUMBER/TITLE	PAGE NUMBER
5.6 Criminal Justice Information System Security	5. Management Information Systems	Page 2 of 8 2/20/24R

3. Private contractors that process Criminal Justice Information (CJI) must meet security requirements and controls laid out in the CJIS Security policy and sign the Security Addendum, Attachment A
4. Information obtained from the CJI systems must only be used for criminal justice purposes. Staff and other persons with access to the Department's CJI information shall follow this policy, the FBI CJIS Security Policy, and other state and federal policies and regulations regarding CJI information.
5. Improper access, use, or dissemination of CJI is in violation of this policy and may result in the termination of system access, disciplinary action up to and including termination of employment, and/or state or federal criminal penalties.

**Procedure B: Terminal Agency Coordinator (TAC) Responsibilities**

1. Each facility Chief Administrative Officer shall designate a staff person as the facility's Terminal Agency Coordinator (TAC) to oversee access to Criminal Justice Information (CJI) at the facility. Further, the Chief Administrative Officer, or designee, shall notify the Maine State Police within thirty (30) days of a change of TAC assignment.
2. Each Regional Correctional Administrator shall designate a staff person as the community corrections region's TAC to oversee access to CJI in the region. Further, the Regional Correctional Administrator, or designee, shall notify the Maine State Police within thirty (30) days of a change of TAC assignment.
3. The Commissioner shall designate a Central Office staff person as the Department TAC to oversee access to CJI at Central Office. Further, the Commissioner, or designee, shall notify the Maine State Police within thirty (30) days of a change of TAC assignment. In addition, the Department TAC shall oversee the facility and regional TACs for the facilities and regions and shall ensure:
  - a. security practices related to CJI access are maintained;
  - b. appropriate safeguards are in place for protecting CJI to limit potential mishandling or loss while being stored, accessed, or transported;
  - c. standards for the selection of staff permitted to have access to CJI are met; and
  - d. in coordination with the Department's Director of Training, that staff are trained in accordance with CJIS Security Awareness training requirements.
4. Each TAC, with respect to their location, shall:
  - a. be at least a limited access certified terminal operator;
  - b. institute reasonable quality assurance standards;
  - c. institute a program of systematic self-audit; and
  - d. ensure staff in their location receive CJIS Security Awareness training; and
  - e. serve as the liaison to the MSP Access Integrity Unit (AIU) for METRO/NCIC audits pertaining to the use of Interstate Identification Index (III) criminal history records.

POLICY NUMBER/TITLE	CHAPTER NUMBER/TITLE	PAGE NUMBER
5.6 Criminal Justice Information System Security	5. Management Information Systems	Page 3 of 8 2/20/24R

## Procedure C: Local Agency Security Officer (LASO) Responsibilities

1. Each facility Chief Administrative Officer shall designate a staff person as the facility's Local Agency Security Officer (LASO) to oversee CJI access at the facility. Further, the Chief Administrative Officer, or designee, shall notify the Maine State Police (MSP) within thirty (30) days of a change of LASO assignment.
2. Each Regional Correctional Administrator shall designate a staff person as the community corrections region's LASO to oversee CJI access in the region. Further, the Regional Correctional Administrator, or designee, shall notify the MSP within thirty (30) days of a change of LASO assignment.
3. The Commissioner shall designate a Central Office staff person as the Department LASO to oversee the facilities and regions LASOs. Further, the Commissioner, or designee, shall notify the MSP within thirty (30) days of a change of LASO assignment. The Department LASO shall:
  - a. serve as a liaison with the Maine State Police's Information Security Officer (ISO) and provide technical guidance as to the intent and implementation of operational and technical policy issues;
  - b. assist with developing audit compliance guidelines as well as identifying and reconciling security-related issues; and
  - c. prepare and maintain a network topological drawing showing the physical location within the facility or office of every computer and server used to access CJI, other than remote access laptop computers.
4. A TAC may also be designated as a LASO.
5. Each LASO, with respect to their location, shall:
  - a. ensure staff who are accessing CJI are authorized and ensure that no unauthorized persons have access to CJI;
  - b. identify and document how the equipment is connected to the state system;
  - c. ensure that personnel security screening procedures are being followed;
  - d. ensure that appropriate hardware security measures are in place and working as expected;
  - e. ensure that this policy is complied with and that any security incident that might compromise CJI is reported to the Maine State Police Access Integrity Unit using the Computer Security Incident Form (Attachment B).
  - f. serve as a point-of-contact (POC) for computer incident notification and distribution of security alerts to the MSP ISO;
  - g. prepare and maintain a list of staff allowed to access METRO;
  - h. ensure security of computers, servers, and other associated equipment used to access CJI;
  - i. coordinate with the Department's Human Resources Director to ensure compliance with fingerprint-based record check requirements for staff with access to CJI;
  - j. ensure compliance with log-in requirements; and

POLICY NUMBER/TITLE	CHAPTER NUMBER/TITLE	PAGE NUMBER
5.6 Criminal Justice Information System Security	5. Management Information Systems	Page 4 of 8 2/20/24R

- k. ensure security of printed CJI.

**Procedure D: Criminal Justice Information Access**

1. The Chief Administrative Officer, Regional Correctional Administrator, or Central Office supervisor, or their designees, shall:
  - a. only authorize staff who have been screened and clear a background check to access CJI;
  - b. grant access to CJI in accordance with the least privilege principle after staff is screened and clears a background check;
  - c. ensure that any computer in a Departmental facility or office used to access Criminal Justice Information (CJI) and all associated equipment, including any server, shall be located in a physically secure area so as not to allow access by any unauthorized person; and
  - d. ensure that any remote access laptop computer with CJI access shall be secured in such a way that displayed CJI is not visible to any unauthorized person.
2. Authorized staff are allowed to access criminal justice information only through a multi-factor authentication for access to CJI.
3. Staff shall be prohibited from having access to the CJI if the staff:
  - a. has been convicted of a felony (a Class A, B, or C crime);
  - b. has been convicted of a misdemeanor offense (Class D or E crime) that was directly related to the use of the METRO system;
  - c. has been convicted of a misdemeanor offense for which they were sentenced to a period of incarceration;
  - d. has been convicted of a misdemeanor offense for which the underlying conduct is directly related to reliability and trustworthiness; or
  - e. appears to be a fugitive, or appears to have an arrest history without conviction, for a felony or one of the above-described misdemeanors.

**Procedure E: Account Management**

1. The Department’s Human Resources Director, or designee, shall ensure staff allowed access to CJI has a state and national fingerprint-based criminal background record check within thirty (30) days of being allowed access and has a criminal background record check every five (5) years thereafter.
2. New staff may have access to all CJI systems upon start date but shall lose access to CJI systems if training courses are not completed/ or passed within thirty (30) days.
3. The access level granted to the user for all information systems shall be granted based on the satisfactory screening and valid need-to know/need-to-share as required by assignment of official duties.
4. If a staff person permitted access to CJI is separated from employment, the appropriate TAC shall take immediate steps to ensure that the person is not permitted access to any computer used to access CJI. The TAC shall also notify the Access Integrity Unit of the

POLICY NUMBER/TITLE	CHAPTER NUMBER/TITLE	PAGE NUMBER
5.6 Criminal Justice Information System Security	5. Management Information Systems	Page 5 of 8 2/20/24R

Maine State Police to suspend the person's Open Fox Messenger (MSP's application) or other software account and notify the appropriate service provider to disable any applicable computer access.

**Procedure F: Security Awareness Training**

1. The Department's TAC in coordination with the Department's Director of Training, or designee, shall:
  - a. manage the development, documentation, and dissemination of the security awareness training that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance;
  - b. review and update the current security awareness training when changes to the CJIS Security Policy are made; and
  - c. incorporate lessons learned from internal or external security incidents or breaches into role-based training.
  
2. All staff with authorized access to CJI shall receive training on their responsibilities and expected behavior when accessing CJI and the systems which process CJI. Security Awareness Training shall be required within six (6) months of initial assignment, and annually thereafter, for all staff, student interns, and volunteers who have access to CJI in a physically secure location or in a location where CJI is accessible.
  
3. LASOs shall receive enhanced training on the specific duties and responsibilities of those positions and the impact those positions have on the overall security of information systems.
  
4. Persons who have not been trained shall not be allowed unescorted access to areas where CJI information is accessible.
  
5. The Security Awareness Training as stipulated in the FBI CJIS Security Policy shall provide:
  - a. literacy training on recognizing and reporting potential indicators of insider threat;
  - b. literacy training on recognizing and reporting potential and actual instances of social engineering and social mining; and
  - c. appropriate role-based security and privacy training to staff, student interns, volunteers, and other persons with the following roles and responsibilities:
    - 1) All staff, student interns, volunteers, and other persons with unescorted access to a physically secure location where CJI is accessible;
    - 2) General User: A user who is authorized to use an information system;
    - 3) Privileged User: A user who is authorized to perform security-relevant functions that general users are not authorized to perform; and
    - 4) Staff with Security Responsibilities: Staff with the responsibility to ensure the confidentiality, integrity, and availability of CJI and the implementation of technology in a manner compliant with the FBI CJIS Security Policy.

POLICY NUMBER/TITLE	CHAPTER NUMBER/TITLE	PAGE NUMBER
5.6 Criminal Justice Information System Security	5. Management Information Systems	Page 6 of 8 2/20/24R

## **Procedure G: Incident Response**

1. A security incident may be a physical or electronic breach and includes, but is not limited to, unauthorized access to CJI, an unauthorized person in an area that has CJIS equipment or information, malicious code attacks, compromise of user logon account credentials, and loss of CJI printout, remote access laptop, or a smart phone, thumb drive, or any other equipment to which CJI has been transmitted, or any other incident that constitutes a risk to the confidentiality and integrity of CJIS.
2. All authorized users are responsible for the protection of information subject to confidentiality concerns. This includes CJI in current systems, archived, on backup media, etc. until the CJI is destroyed.
3. All authorized users are also responsible for ensuring threats, vulnerabilities, and risks associated with accessing CJIS systems and services are eliminated prior to accessing the CJIS system.
4. Any security incidents that may arise shall be reported immediately by staff to their supervisor for action deemed necessary.
5. In addition to informing their supervisor, the reporting person is responsible for completing and forwarding the CJIS Security Incident Reporting Form (Attachment B) to the Maine State Police CJIS Information Security Officer via email at [METRO.AIU@maine.gov](mailto:METRO.AIU@maine.gov). and shall also forward a copy to their supervisor, the appropriate Terminal Agency Coordinator (TAC), and the Local Agency Security Officer (LASO) for their location.
6. The Terminal Agency Coordinator (TAC) and the Local Agency Security Officer (LASO) shall forward a copy of the form to the Department TAC and LASO.

## **Procedure H: Disposal of Criminal Justice Information**

1. When CJI is no longer needed, it shall be destroyed by burning, shredding, or other method rendering the information unreadable. Record destruction shall be observed or carried out by an authorized user.
2. Prior to release for reuse for any other purpose, any computer, server, or other associated equipment used to access CJI shall be sanitized. The sanitization shall be observed or carried out by authorized Department staff or Office of Information Technology (OIT) staff, and the time, place and manner of sanitizing shall be documented.
3. If the computer, server, or other associated equipment used to access CJI is to be retired from such use and not reused for another purpose, it shall be destroyed. The destruction shall be observed or carried out by authorized Department staff or OIT staff and the time, place and manner of destruction shall be documented.,
4. Physical CJI such as hard copy printouts shall be disposed of by burning, shredding, or other method rendering the information unreadable. Record destruction shall be observed or carried out by an authorized user.

<b>POLICY NUMBER/TITLE</b>	<b>CHAPTER NUMBER/TITLE</b>	<b>PAGE NUMBER</b>
<b>5.6 Criminal Justice Information System Security</b>	<b>5. Management Information Systems</b>	Page 7 of 8 2/20/24R

**Procedure I: Agency Agreements**

1. Each facility, community corrections region, and Central Office that has METRO access shall maintain a CJIS Terminal Agency agreement with the Maine State Police, which shall be reviewed annually and revised as necessary.
2. The Department shall maintain an inter-agency and management control agreement with applicable service providers such as the Office of Information and Technology (OIT). The agreement shall stipulate that any OIT staff providing technical assistance on a Department computer (either in person or team viewer) is required to complete the CJIS Security Awareness Training.

**VIII. PROFESSIONAL STANDARDS**

None

<b>POLICY NUMBER/TITLE</b>	<b>CHAPTER NUMBER/TITLE</b>	<b>PAGE NUMBER</b>
5.6 Criminal Justice Information System Security	5. Management Information Systems	Page 8 of 8 2/20/24R