
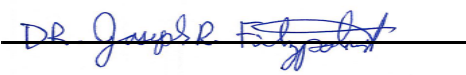


POLICY TITLE: CRIMINAL JUSTICE INFORMATION SYSTEM SECURITY		PAGE 1 of 7
POLICY NUMBER: 5.6		
CHAPTER: MANAGEMENT INFORMATION SYSTEM		
	STATE of MAINE DEPARTMENT OF CORRECTIONS Approved by Commissioner: 	PROFESSIONAL STANDARDS: See Section VII
EFFECTIVE DATE: December 21, 2015	LATEST REVISION:	CHECK ONLY IF APA []

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

The purpose of this policy is to provide for the security, integrity, and confidentiality of Criminal Justice Information (CJI) that is available electronically to authorized staff in obtaining criminal background information through the Maine Telecommunications and Routing Operations System (METRO). This policy describes the security requirements associated with the creation, viewing, modification, transmission, dissemination, storage, and destruction of criminal justice information and adheres to the requirements of the Maine Criminal Justice Information Network (CJIN) and is based on the Maine State Police Metro Security Policy.

IV. 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: [CJIS Security](#)
- Procedure E: [Terminal/Computer Users](#)
- Procedure F: [CJIS Incident Response Requirements](#)
- Procedure G: [Training](#)
- Procedure H: [Agreements](#)

V. ATTACHMENTS

Attachment A: CJIS Security Incident Reporting Form

VI. PROCEDURES

Procedure A: Criminal Justice Information System Security, General

1. Criminal Justice Information (CJI) is arrest-based data and any derivative information from the arrest record and it includes, but is not limited to, descriptive data, conviction status, sentencing data, FBI Number, incarceration status, and probation and parole information.
2. The Maine State Police is the CJIS System Agency (CSA) for the State of Maine.
3. The CSA provides oversight to Maine's criminal justice agencies with respect to Criminal Justice Information (CJI) from various systems managed by the FBI CJIS Division.
4. CJI acquired through CJI systems is for use by law enforcement and criminal justice agencies for official criminal justice purposes only, consistent with the purpose for which the information was requested.
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/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 METRO by facility staff designated by the Chief Administrative Officer as authorized to have access to METRO. Further, the Chief Administrative Officer, or designee, agrees to 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 Terminal Agency Coordinator (TAC) for each office that has criminal justice information access devices to oversee access to METRO by community corrections staff designated by the Regional Correctional Administrator as authorized to have access to METRO. Further, the Regional Correctional Administrator, or designee, agrees to 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 METRO by authorized by Central Office staff. In addition, the Department TAC shall oversee the TACs for the facilities and regions and shall:

POLICY NUMBER/TITLE	CHAPTER NUMBER/TITLE	PAGE NUMBER
5.6 Criminal Justice Information System Security	5. Management Information Systems	2 of 7 12/21/15

- a. establish standards for the selection of staff permitted to have access to METRO;
 - b. work with the Department's Director of Training to establish standards for the training of selected staff;
 - c. establish security practices related to access to METRO and printed CJIS information; and
 - d. disseminate related publications to departmental staff with access to METRO.
4. Each TAC, with respect to his or her 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. work with the Department's Training Director to ensure METRO users receive CJIS Security Awareness training.

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 access to METRO by facility staff designated by the Chief Administrative Officer as authorized to have access to METRO. Further, the Chief Administrative Officer, or designee, agrees to notify the Maine State Police with thirty (30) days of a change of LASO assignment.
2. Each Regional Correctional Administrator shall designate a staff person as the Local Agency Security Officer (LASO) for each office that has criminal justice information access devices to oversee access to METRO by community corrections staff designated by the Regional Correctional Administrator as authorized to have access to METRO. Further, the Regional Correctional Administrator, or designee, agrees to notify the Maine State Police with 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 LASOs for the facilities and regions and shall:
 - a. serve as a liaison with the CSA'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;
 - 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 METRO, other than remote access laptop computers; and

POLICY NUMBER/TITLE	CHAPTER NUMBER/TITLE	PAGE NUMBER
5.6 Criminal Justice Information System Security	5. Management Information Systems	3 of 7 12/21/15

- d. prepare and maintain an inventory of every remote access laptop computer used to access METRO.
- 4. A TAC may also be designated as a LASO.
- 5. Each LASO, with respect to his or her location, shall:
 - a. identify those persons who are accessing METRO to ensure that they are authorized to access METRO and to ensure that no unauthorized persons have access to METRO;
 - 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;
 - e. ensure that this policy is complied with and that any security incident that might compromise METRO is reported to the Maine State Police Access Integrity Unit using the Computer Security Incident Form (Attachment A).
 - f. serve as a point-of-contact (POC) for computer incident notification and distribution of security alerts to the 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 METRO;
 - i. work with the Department's Human Resources Director to ensure compliance with fingerprint-based record check requirements for staff with access to METRO and others as set out below;
 - j. ensure compliance with logging requirements; and
 - k. ensure security of printed CJIS information.

Procedure D: CJIS Security

- 1. The Chief Administrative Officer, or designee, or Regional Correctional Administrator, or designee, shall ensure that any computer in a departmental facility or office used to access the Maine Telecommunications and Routing Operations System (METRO) system 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.
- 2. The Regional Correctional Administrator, or designee, shall ensure that any remote access laptop computer with METRO access shall be secured in such a way that displayed criminal justice information is not visible to any unauthorized person.
- 3. Prior to release for reuse for any other purpose, any computer, server, or other associated equipment used to access METRO shall be sanitized. The sanitization shall be observed or carried out by authorized departmental staff or OIT staff and the time, place and manner of sanitizing shall be documented.

POLICY NUMBER/TITLE	CHAPTER NUMBER/TITLE	PAGE NUMBER
5.6 Criminal Justice Information System Security	5. Management Information Systems	4 of 7 12/21/15

4. If the computer, server, or other associated equipment used to access METRO 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 departmental staff or OIT staff and the time, place and manner of destruction shall be documented.
5. When Criminal Justice Information (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.

Procedure E: Terminal/Computer Users

1. Staff permitted access to METRO shall be limited access users (query capable only) and shall access METRO for criminal justice purposes only.
2. If a staff person permitted access to METRO 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 METRO. The TAC shall also immediately notify the Access Integrity Unit of the Maine State Police to suspend the person's Messenger or other software account and notify the appropriate service provider to disable any applicable computer access.
3. The Department's Human Resources Director, or designee, shall ensure staff allowed access to METRO has a state and national fingerprint-based criminal background record check within thirty (30) days of being allowed access and shall have a criminal background record check every five (5) years thereafter.
4. Each LASO, for his or her location, shall ensure that any other person with access to physically secure areas in which equipment used to access METRO is located has a state and national fingerprint-based criminal background record check within thirty (30) days of being allowed access and shall have a criminal background record check every five (5) years thereafter, unless staff authorized to have access to METRO escort the person at all times while he or she is in the physically secure area.
5. Staff shall be prohibited from having access to the METRO system and/or Criminal Justice Information (CJI) if the staff:
 - a. is a convicted felon;
 - b. has been convicted of a misdemeanor offense that was directly related to the use of the METRO system;
 - c. has been convicted of a misdemeanor offense for which he or she was 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

POLICY NUMBER/TITLE	CHAPTER NUMBER/TITLE	PAGE NUMBER
5.6 Criminal Justice Information System Security	5. Management Information Systems	5 of 7 12/21/15

- e. appears to be a fugitive, or appears to have an arrest history without conviction, for a felony or serious misdemeanor.
- 6. If a record of any other kind exists, systems access shall not be granted until the Maine State Police CJIS Information Security Officer (ISO) reviews the matter to determine if systems access is appropriate.
- 7. If the ISO determines that CJIS systems access by the individual would not be in the public interest, access shall be denied and the Department's Director of Human Resources shall be notified, in writing, of the access denial.
- 8. Disqualifications or appeals, upon written request, will be reviewed and decided by the Maine State Police CJIS Information Security Officer.

Procedure F: CJIS Incident Response Requirements

- 1. A security incident is a violation or possible violation that threatens the confidentiality, integrity or availability of state/FBI CJIS data.
- 2. 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.
- 3. A user of a CJI system or other person who knows or suspects that a security incident has occurred is responsible for informing his or her supervisor immediately.
- 4. In addition to informing his or her supervisor, the reporting person is responsible for completing and forwarding the CJIS Security Incident Reporting Form (Attachment A) to the Maine State Police CJIS Information Security Officer via email at METRO.AIU@maine.gov. and shall also forward a copy to his or her supervisor, the Terminal Agency Coordinator (TAC), and the Local Agency Security Officer (LASO) for their location.
- 5. 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 G: Training

- 1. Basic security awareness training shall be required within six (6) months of initial assignment, and biennially thereafter, for all staff that have access to CJI.
- 2. Each person need only complete the tier which applies for the type of access he or she may have. Determining which tier is most appropriate is as follows:
 - a. Tier 1: All persons

POLICY NUMBER/TITLE	CHAPTER NUMBER/TITLE	PAGE NUMBER
5.6 Criminal Justice Information System Security	5. Management Information Systems	6 of 7 12/21/15

Training is required for all staff and anyone else having unescorted access to areas where METRO/CJIS systems data is accessed, processed, or stored. This would include anyone having indirect access to criminal justice information (CJI) via printouts or access to computerized systems used to store CJI (i.e., records management system). This would also include anyone having unescorted access to areas where there are computers (used to access and/or store CJI), printers (used to print CJI), or cabinets and/or paper files (used to store CJI). In other words, all maintenance, cleaning, or other persons with keys (or other means to provide unescorted access) need to complete Tier 1 of the security awareness training.

b. Tier 2: All persons with physical and logical access

Training is required for all staff with direct (logon) access to METRO/CJIS systems data. If an individual has direct access and therefore can query METRO/CJIS systems, he or she needs to complete Tier 2 of security awareness training in lieu of Tier 1.

c. Tier 3: All persons with information technology roles

This would include all persons involved in information technology (IT) (system administrators, security administrators, network administrators, etc.) tasked with supporting systems utilized to access, process, or store CJI. All such persons need to complete Tier 3 of security awareness training in lieu of Tier 1 or 2.

Procedure H: Agreements

1. Each facility and 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 Tier 3 training.

VII. PROFESSIONAL STANDARDS

None

POLICY NUMBER/TITLE	CHAPTER NUMBER/TITLE	PAGE NUMBER
5.6 Criminal Justice Information System Security	5. Management Information Systems	7 of 7 12/21/15