MICHIGAN DEPARTMENT OF CORRECTIONS **POLICY DIRECTIVE**	EFFECTIVE DATE 03/01/2019	NUMBER 01.04.135
SUBJECT LAW ENFORCEMENT INFORMATION NETWORK (LEIN)	SUPERSEDES 01.04.135 (01/01/2002)	
	AUTHORITY MCL 28.211 et seq., MCL 28.214. Administrative Rule 28.5101, et seq. CJIS Security Policy; Executive Order 2011-7, State Administrative Guide, C.J.I.S. Policy Council Act, 1974 PA 163, MCL 28.211 - 28.216	
	PAGE 1 OF 5	

POLICY STATEMENT:

Law Enforcement Information Network (LEIN) operators and LEIN requesters shall have access to LEIN as set forth in this policy. Criminal Justice Information (CJI) shall be properly protected, distributed, stored, and destroyed pursuant to this policy.

RELATED POLICY:

06.01.140 Pre-Sentence Investigation and Report

POLICY:

DEFINITION

A. Criminal Justice Information (CJI) - Information obtained from LEIN or any of its integrated system of databases in any form including, but not limited to: actual printouts or copies of printouts, data in electronic form (e.g., OMNI) and data copied and pasted to other programs or applications. Verbal and written information obtained from an offender or independently verified by a Michigan Department of Corrections (MDOC) employee is not CJI.

B. CJI AREA - An area containing printed CJI, computers capable of accessing CJI, or networks carrying CJI.

C. Electronic storage and communication devices - Memory devices in laptops and computers (hard drives) and any removable/transportable digital memory media (e.g., disk, backup medium, optical disk, flash drives, external hard drives, digital memory card, phones, etc.).

D. LEIN - An online system that provides authorized agencies with an integrated network for sharing information by interfacing with other CJI sources, including the National Crime Information Center (NCIC).

E. LEIN Operator - A Michigan Department of Corrections (MDOC) employee authorized to have direct access to the LEIN or Michigan Criminal Justice Information Network (MICJIN) application.

F. LEIN Requester - An MDOC employee authorized to request CJI from a LEIN Operator(s) or view CJI in any form.

G. Local Agency Security Officer (LASO) - The Manager of the MDOC Data Security and Privacy Unit who provides agency services to the MDOC as outlined in the FBI CJIS Security Policy. This person also serves as the Department CJIS Systems Agency Information Security Officer (CSA ISO).

H. Michigan Criminal Justice Information Network (MICJIN) - A portal that provides a secure infrastructure with data encryption and single user sign-on to access a wide range of software applications designed to promote information sharing among criminal justice agencies in the State of Michigan.

I. Secondary Dissemination - Movement of CJI beyond the control of the original LEIN Operator or LEIN Requester to another authorized recipient of CJI outside of the MDOC.

J. Secure Location - An area, a room, or a group of rooms within a work location with both the physical

and personnel security controls sufficient to protect the LEIN-based CJI and associated information systems.

K. Terminal Agency Coordinator (TAC) - An MDOC agency representative versed and knowledgeable in rules, regulations, and applications relating to LEIN, NCIC and its interfaced systems who serves as the local agency point-of-contact for matters relating to CJIS information access and operations.

L. Visitor - A person who enters an MDOC worksite with proper authorization and who is not employed by the Department.

GENERAL INFORMATION

M. The MDOC shall abide by all requirements pertaining to CJI as contained in the Federal Bureau of Investigation (FBI) Criminal Justice Information Systems (CJIS) Security policy.

N. This policy sets forth the requirements for employees accessing LEIN and requesting and/or receiving CJI. Employees violating this policy, including accessing LEIN or requesting and/or receiving CJI without authorization, may be subject to discipline as set forth in PD 02.03.100 "Employee Discipline" and/or denied use of LEIN. An employee who is no longer able to perform his/her job responsibilities as a result of being denied LEIN access may be terminated from employment or reassigned in accordance with Civil Service Commission rules and applicable collective bargaining unit agreements.

AUTHORIZED ACCESS

O. A person who can access CJI must:

1. Be LEIN cleared prior to accessing CJI.

2. Complete LEIN security awareness training. All authorized Department or Noncriminal Justice Agencies (NCJA) will receive security awareness training prior to being granted duties that require CJI access and every two years thereafter.

LEIN OPERATORS AND REQUESTERS

P. LEIN operators shall access LEIN only as necessary to comply with Department policy. Under no circumstances shall employees access LEIN or request and/or receive CJI for personal reasons. Only employees who are LEIN operators are authorized to directly access LEIN.

Q. In accordance with PD 01.04.105 "Use of Department Computer Equipment, Software and Services," LEIN operators are required to sign a Security Agreement-Data Processing form (CAJ-532) or, if designated as a LEIN operator prior to the effective date of this policy, an approved LEIN use agreement form prior to accessing LEIN.

R. LEIN operators must complete LEIN training and pass certification tests. Once certified, LEIN operators must successfully pass re-certification tests and receive required update training once every two years. LEIN requesters authorized to receive CJI in conjunction with their job responsibilities must successfully complete LEIN Requester training every two years. Contracted staff requiring access to CJI as Requesters must meet all Requester-level training and clearance requirements in addition to signing the FBI CJIS Security Addendum for contracted staff.

S. LEIN operators shall ensure the accuracy, timeliness, and quality of information they enter in LEIN. All entries shall be made in accordance with regulations set forth in the LEIN Operations Manual and NCIC Operations Manual.

T. The LEIN Operator’s supervisor shall keep the agency TAC informed when CJI access is no longer needed.

TERMINAL AGENCY COORDINATORS/TRAINERS

U. There shall be a TAC assigned to the Electronic Monitoring Center, Field Operations Administration

(FOA). This person shall act as the Departmental Specialist for LEIN. Each Deputy Director shall ensure employees are designated as TACs for all other Originating Agency Identifiers (ORIs) in his/her area of responsibility. An employee may be designated as the TAC for more than one ORI.

V. Local Agency TACs shall:

1. Ensure compliance with MDOC policies pertaining to CJI and the TAC manual.

2. Assist with all required audits of LEIN operations in their respective area.

3. Provide LEIN operator and requester and security awareness training and testing required by the FBI CJIS Security Policy ł in conjunction with the Training Division, Budget and Operations Administration (BOA).

4. Distribute, collect, and maintain LEIN-related training and processing records.

5. Report immediately any alleged violation of this policy through the appropriate chain of command and the Michigan State Police (MSP).

6. Provide technical support regarding LEIN use.

7. Maintain a current list of designated LEIN operators for each ORI in his/her respective area.

W. The Departmental Specialist for LEIN shall coordinate formal annual audits on all CJI system accounts to ensure that access and account privileges are commensurate with job functions, need-to-know, and employment status on systems that contain CJI. The local TAC may also conduct periodic informal reviews. All user access approval shall be communicated through, and approved by, the Departmental LEIN Specialist or designee(s).

X. The Departmental Specialist for LEIN shall serve as the TAC trainer for Central Office. The Correctional Facilities Administration (CFA) and FOA Deputy Directors shall ensure trainers are designated for their respective facilities/field offices. The Departmental Specialist for LEIN will provide the training to those trainers designated by the Deputy Directors. In conjunction with the Training Division, TAC trainers shall be responsible for training TACs in their respective areas regarding LEIN regulations and operations.

DISCLOSURE OF CJI

Y. CJI shall be disclosed in accordance with FBI CJIS security policy guidelines and state law. Questions regarding the disclosure of CJI shall be directed to the Department's LEIN Specialist.

Z. CJI shall not be transmitted to anyone via electronic mail (e-mail) unless properly encrypted as set forth in the MDOC TAC Training Manual. CJI may be transmitted via facsimile machine only after the intended recipient has been verified as being authorized and present to receive the information.

AA. Dissemination of CJI to another agency is authorized if the other agency is an authorized recipient. An employee who discloses CJI in violation of state or federal law may be subject to criminal prosecution pursuant to MCL 28.214.

LOGGING

BB. Criminal history queries shall be properly documented according to FBI CJIS Security Policy Guidelines. Information logged must help establish the legitimacy of the query and may point to other locations or files containing information to help support the legitimacy such as case files, employment files, visitor files, or other locations containing supporting information. All criminal history queries must be run for approved purposes only as established in FBI CJIS Security Policy, Michigan Compiled Law, and LEIN Administrative Rules.

CC. Secondary dissemination of Criminal History Information or documents containing Criminal History Information shall be logged. The log must contain a minimum of the date of dissemination and the

name of the individual and agency that received the information.

RETENTION OF CJI

DD. Copies of LEIN printouts shall not be retained beyond the scope for which they were originally obtained. Retained CJI must be stored securely and destroyed according to FBI CJIS security policy specifications when no longer needed.

PROTECTION OF CJI

EE. Controls shall be in place to protect CJI. To protect CJI, Departmental staff shall:

1. Store all forms of CJI within a secure location accessible to employees whose job functions require them to handle such documents.

2. Ensure that only authorized users remove printed or digital media containing CJI.

3. Use only government-owned computers.

4. Take appropriate action when accessing CJI, when in possession of CJI, or when transporting or electronically transmitting CJI. To achieve this, employees must:

   a. Be aware of who is in the area before accessing CJI.

   b. Obscure CJI from public view while actively using or processing CJI.

   c. Immediately protect CJI that is electronically transmitted outside the secure location using encryption meeting FIPS 140-2 standards.

      NOTE: Federal Information Processing Standard Publication (FIPS) 140-2 is a government computer security standard used to approve cryptographic modules.

   d. Protect CJI that is at rest (i.e., stored electronically) outside the secure location using encryption. Storage devices include external hard drives, printers, copiers used with CJI, thumb drives, flash drives, back-up tapes, mobile devices, laptops, etc.

   e. Lock or log off computer when not in immediate vicinity of work area to protect CJI.

5. Protect and not share any individually-issued keys, access cards, computer account passwords, personal identification numbers (PIN), security tokens (i.e., Smartcard), and all other facility and computer systems security access procedures. If loss of any of these items occurs, staff shall follow local worksite operating procedures.

6. Follow the State of Michigan (MDOC, DTMB) established security protocols to protect the State computer from viruses, worms, trojan horses, and other malicious code.

7. Report any security incidents through the chain of command to the LASO.

FF. Visitors in CJI areas must:

1. Be checked in before entering a physically secure location by providing a form of identification used to authenticate visitor's identity.

2. Be accompanied by a Department escort at all times to include delivery or service personnel. An escort is defined as authorized personnel who accompany a visitor at all times while within a secure location to ensure the protection and integrity of the secure location and any CJI therein. The use of cameras or other electronic means used to monitor a secure location does not constitute an escort.

3. Not be allowed to view screen information.

DATA SANITIZATION AND DISPOSAL

GG. Sources of inoperable electronic data shall be destroyed in accordance with the DTMB depot process. Information Technology (IT) systems that have been used to process, store, or transmit FBI CJI and/or sensitive and classified information shall not be released from DTMB control until the equipment has been sanitized (reimaged) and all stored information has been cleared.

HH. Hard Copies of CJI shall be destroyed by use of a cross-cut shredder. A sensitive document disposal company may also be used as long as the shredding is completed on-site and is witnessed by an authorized agency employee. If the shredding is completed off site, all disposal company employees who may have contact with the unshreded materials must receive a name-based background check, submit to a state and national fingerprint search, sign the CJIS Security Addendum, and fully complete Security Awareness Training.

LEIN AUDITS

II. All LEIN-capable MDOC worksites with assigned ORIs are subject to the MSP audit once every three-year audit cycle. On-Site LEIN audits will be coordinated between the agency TAC and the MSP auditor assigned to the on-site audit.

JJ. Details of scheduled audits shall be shared by the agency TAC with the Departmental Specialist for LEIN. The Departmental Specialist for LEIN will assist the TAC in preparing for the audit by providing responses to technical questions in conjunction with the current MDOC LASO and DTMB staff, and by providing guidance and additional documentation as needed.

KK. Following the audit, the MSP audit results will be shared with the Departmental Specialist for LEIN and the Procurement Monitoring and Compliance Division (PMCD) Administrator.

1. Agencies with passing audit results will require no further follow up.

2. The Departmental Specialist for LEIN shall prepare the Corrective Action Correspondence (CAC) or CJIS Systems Officer (CSO) referral for the agency with non-compliant results within 45 days. The CAC or CSO referral will be forwarded to the Supervisor and TAC of the audited MDOC office.

    a. The agency shall be responsible for reviewing and modifying the document as needed and sending the final report to MSP within 45 days of receiving the CSO Referral notice, or in compliance with a due date specified on the CAC. the agency shall be responsible for achieving any proposed corrective actions as stated on the Department's corrective action response.

LL. Within 90 calendar days of the CSO referral the Departmental Specialist for LEIN will contact the MDOC agency for follow-up to assess progress on the submitted corrective actions. The Departmental Specialist for LEIN shall prepare and forward a 90-calendar day response to the Supervisor and TAC of the MDOC Agency. The MDOC agency will review and modify the report and send the final report to MSP prior to the 90-day deadline.

OPERATING PROCEDURES

MM. If necessary, to implement the requirements set forth in this policy directive, Wardens and the FOA Deputy Director shall ensure operating procedures are developed or updated.

AUDIT ELEMENTS

NN. A Primary Audit Elements List has been developed and is available on the Department's Document Access System to assist with self-audit of this policy, pursuant to PD 01.05.100 "Self-Audits and Performance Audits."

APPROVED: HEW 01/07/2019