OVERVIEW

This policy addresses the appropriate use and disclosure of information contained within the criminal history record information as obtained from the Law Enforcement Information Network (LEIN). It incorporates the regulations, policies and laws from the Michigan Department of Health and Human Services (MDHHS), Michigan State Police (MSP), Adam Walsh Act, Criminal Justice Information Services (CJIS) Policy Council Act, CJIS Security Policy, and CJIS addendum.

LEGAL BASE

Federal

28 CFR 20 provides provisions for criminal justice information (CJI) systems, dissemination, certification, and penalties for misuse.

34 USC 20961 grants the MDHHS access to National Crime Information Center (NCIC) and NCIC III for investigated cases of child abuse, neglect, or exploitation.

CJIS Security Policy, (CJISSECPOL) provides guidelines and requirements for criminal justice agencies (CJA) to protect CJI, both at rest and in transit. This includes transmission, dissemination, and destruction of CJI.

State

The Criminal Justice Information Services (CJIS) Policy Council Act, 1974 PA 163, as amended, MCL 28.214 provides MDHHS access to LEIN and fingerprint identification systems for the enforcement of child support laws and child and vulnerable adult protection laws.

Social Welfare Act, 1939 PA 280, appointed MDHHS with responsibility to protect the welfare of the people of this state, defining the roles and duties of the agency.

Social Welfare Act, 1939 PA 280, as amended, MCL 400.43b established the Office of Inspector General (OIG) as a criminal justice department under MDHHS.

Michigan State Police Policy

CJIS Michigan Addendum is an adopted revision to the Michigan CJIS Security Policy that requires Michigan users to adhere to

requirements in the FBI CJIS Security Policy, versions 5.1 and future versions.

MSP LEIN Policy Manual provides policy topics and rules on LEIN use.

Admin/Court Rule

CJIS Administrative Rules (State Office of Administrative Hearings and Rules, Administrative Code: R 28.5101 - R 28.5414) provides general provisions, access, eligibility, and data dissemination provisions, NCIC access; authorized agencies, audit information and dissemination, and records.

Inter-Agency Contracts and Agreements

Signed contractual agreements between the MSP and the CJIS-0001, MDHHS, LEIN Memorandum of Agreement and RI-093, User Agreement.

TERMS AND DEFINITIONS

Access

Access is defined as the physical or electronic ability, right, or privilege to view, modify, or make use of CJIS and CJI.

Criminal History Record Information (CHRI)

Criminal history record information (CHRI) is a subset of CJI. This includes 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 from LEIN is nonpublic records.

Criminal Justice Agency (CJA)

An agency is considered a CJA if it is either a court, governmental agency, or any subunit of a governmental agency that performs

administrative activities of criminal justice pursuant to a statute or executive order and allocates a substantial part of its annual budget to the administration of criminal justice.

Criminal Justice Information (CJI)

CJI is the abstract term used to refer to all the FBI CJIS provided data, including but not limited to: biometric, identity history, person, organization, property (when accompanied by any personally identifiable information), and case/incident history data. CJI is data (electronic or hard copy) collected by criminal justice agencies for the purposes as authorized or required by law. (Michigan Administrative Rule, R 28.5101(g)). CJI from LEIN is nonpublic.

Law Enforcement Information Network (LEIN)

LEIN is Michigan's statewide-computerized information system that stores and disseminates criminal justice information (CJI).

Michigan Criminal Justice Information Network (MiCJIN)

MiCJIN is a portal or software bundle providing direct connection to the LEIN.

National Crime Information Center (NCIC)/III

The NCIC is a nationwide, computerized information system that helps the criminal justice community perform its duties by providing accurate and timely documented criminal justice information (for example, wanted person files, article files, missing person files).

The III is a cooperative state-federal system for the electronic exchange of criminal history record information for authorized purposes as specified by local, state, and federal laws.

Noncriminal Justice Agency (NCJA)

A NCJA that has access to CJI is any court, governmental agency, or any subunit of a government agency that performs administrative activities other than the administration of criminal justice.

Originating Agency Identifier (ORI)

The MSP provides an Originating Agency Identifier (ORI), as authorized by contractual agreement, to a governmental agency or subunit defined as either a CJA or NCJA. The ORI separately identifies each unit/agency and each transaction made from that unit/agency must include the assigned ORI.

Person Query

A person query is a way to look up criminal justice information available in LEIN without using the criminal history record form. Queried information requires the same privacy and protections outlined herein this policy and the Criminal Justice Information Systems (CJIS) Security policy.

Rap Back

A Next Generation Identification (NGI) program service that allows unauthorized agencies to receive notification of subsequent criminal activity reported to the FBI committed by persons of interest.

Verified Information

Information obtained from credible public sources that corroborate information obtained from LEIN.

Public sources include:

- Public court reports.
- Michigan *Internet Criminal History Access Tool (ICHAT); see CRM, 402, ICHAT-Internet Criminal History Access Tool for approved uses and allowable dissemination.
- National and state sex offender online registries.
- Offender Tracking Information System (OTIS).

- Police/law enforcement public reports.
- Prosecuting attorney's office public reports.
- Michigan Secretary of State (SOS) public reports.
- Self-disclosure.
- Victim Information Notification Everyday (VINE).

ROLES AND RESPONSIBILITIES

Each agency or sub-unit that has an assigned ORI(s) must appoint one or more selected staff to serve the following role(s): operator, terminal agency coordinator (TAC), and local agency security officer (LASO). An appointed person can serve dual roles as long they uphold all security policy and contract requirements.

Authorized User

An authorized user is an individual/group of individuals authorized to access CJI from LEIN as required by policy and as permitted access by law.

MDHHS authorized users typically include local office staff, such as clerical, case managers, office supervisors; managers; and directors. Authorized users can be an appointed requester, operator, terminal agency coordinator (TAC), or local area security officer (LASO).

Central Office Local Agency Security Officer (LASO)

The central office LASO serves as the compliance expert for local office appointed LASOs. The central office LASO helps to ensure physical security, software compliance, and physical security screening requirements are adhered to and immediately reports breaches to the MSP LEIN field services.

The central office LASO must:

- Identify who is using the approved hardware, software, and firmware and ensure that only authorized individuals have access.
- Ensure the upholding of personnel security-screening procedures, as outlined in this policy.

- Assist local office LASO's to ensure the approved and appropriate security measures are in place and working as expected.
- Support policy compliance and promptly inform the CJIS System Agency information security officer (ISO) of security incidents.

Central Office Terminal Agency Coordinator (TAC)

The central office TAC is responsible for ensuring LEIN use compliance for MDHHS, Children's Services Administration (CSA) assigned ORI(s).

TAC's role/responsibility includes:

- Serve as a liaison to local office users and help with supervision and system integrity across all assigned ORIs within the agency.
- Manage information system accounts.
- Grant access based on least privilege.
- Monitor and track user compliance.
- Annually affirm and/or validate users.
- Report any agency violations to MSP.
- Disseminate delay-hit notifications.
- Serve as the agency liaison between MSP and MDHHS for audit, contractual, training assistance and policy compliance.

For specific roles and responsibilities, see MSP TAC Manual.

Local Office Local Agency Security Officer (LASO)

A local office LASO serves as the local office-appointed security contact for CJIS related issues. The local office LASO ensures physical security, software compliance, and physical security

screening requirements are adhered and immediately reports breaches to the central office LASO.

The local office LASO must:

- Identify who is using the approved hardware, software, and firmware and ensure that only authorized individuals have access.
- Ensure the upholding of personnel security-screening procedures, as outlined in this policy.
- Ensure the approved and appropriate security measures are in place and working as expected.
- Support policy compliance and promptly inform the central office LASO of security incidents.

Local Office Terminal Agency Coordinator (TAC)

The local office TAC serves as the point-of-contact to the central office TAC and the local office authorized users. The local office TAC is responsible for LEIN use compliance for their local office assigned ORI. All TACs are trained by MSP. MSP-trained TACs are responsible for training local office operators. For specific roles and responsibilities, see MSP TAC Manual.

Operator

An operator has direct access into the LEIN application and processes CJI requests under the assigned ORI and records and retains the transactions for audits. The operator is responsible for ensuring safety and security of the generated criminal history information. For specific roles and responsibilities, see MSP Operations Manual.

Requester

A requester, granted permission by policy and law, requests and reviews CJI from LEIN.

Authorized requesters include case managers or supervisors assigned or associated to cases in:

- Adoption.

- Adult protective services (APS).
- Children's protective services (CPS).
- Child welfare licensing.
- Foster care (FC).
- Interstate Compact on the Placement of Children (ICPC).
- Interstate Compact for Juveniles (ICJ).
- Juvenile guardianship.
- Juvenile justice (JJ).

When requesting CJI from LEIN, the requester must be assigned or associated to the open/active case requiring the CJI. The requester should be knowledgeable in the policies that require a criminal history background check; see SRM 700, LEIN. Interpreting and securing the received criminal history report is the responsibility of the requester.

LEIN ACCESS

Local child welfare offices have access to information in the LEIN through a department agreement with the Michigan State Police (MSP). This access includes the following information:

- State of Michigan criminal history information.
- Sex offender registry.
- Missing/wanted persons.
- Prison and parole information.
- Gun registration/permits.
- Personal protection orders.
- Officer cautions.
- Michigan Secretary of State (SOS).
- National Crime Information Center (NCIC).
- Wants/warrants only within the United States (U.S.).

Note: Full access may be restricted according to agency authorization. Criminal history information from outside the U.S. is restricted to criminal justice agencies.

Requirements for requesting LEIN; see SRM 700, Required LEIN Requests.

NATIONAL CRIME INFORMATION CENTER (NCIC)/III

The NCIC contains restricted and non-restricted interface files. The NCIC restricted files are distinguished from NCIC non-restricted

files by the policies governing their access and use; see, CJIS Security Policy v5.9.2 §4.2. Proper access and dissemination of data from the restricted files must be consistent with the access and dissemination policies for the III as described in 28 CFR Part 20 and the NCIC Operating Manual.

34 USC 20961 authorizes state access to NCIC/III files for purposes of obtaining national criminal history information on persons involved in cases of child abuse, neglect, or exploitation.

ACCESS CONTROL

Fingerprint background checks are required before granting direct access to the LEIN system.

The FBI recommends agencies perform follow up name-based background checks at least once every five years to ensure an employee has not had a disqualifying arrest/conviction and not told the employer. However, if Rap Back is available, this follow up recommendation is not necessary after the initial fingerprint clearance; see *Rap Back and Remediation* in this item.

Fingerprint Clearance Requirements

Fingerprints are required for any MDHHS staff appointed to serve as a LEIN TAC, operator, or LASO with direct LEIN access. Only the agency's appointed central office TAC receives fingerprint based CHRI results. Approvals for LEIN access is based on a criminal record clearance and passing required training exams.

State fingerprints must be taken at the time of appointment and prior to training and access. To be fingerprint cleared, the individual must not have any conviction or offense that the agency would, at its discretion and based on nature and severity, deny LEIN access. If necessary, the Chief Security Officer (CSO) at MSP will make a final determination, pursuant to CJIS policy.

Direct Access Determination Pause

A pause in a determination for direct access will be in place until the following are completed satisfactorily, updated with a final disposition, and/or closed:

- Missing final conviction data.
- Open probation for any offense, including violations.

- Open arrest or warrant for arrest.

Upon satisfactory completion, updated with final disposition, and/or closed, a notice of the disposition must be sent by either the employee or court to the central office TAC for final review and consideration.

Direct Access Termination or Denial

Termination or denial of an employee's direct LEIN access may occur under certain circumstances, including but is not limited to:

- Any felony conviction.
- Any probation violation that escalates to a charge of a misdemeanor or felony.
- The individual having fugitive status.
- Any conviction that is punishable by more than one year, including any probation or Holmes Youthful Trainee Act (HYTA).
- Any offense or conviction that, at the agency's discretion, is determined to be severe, lacking good moral character, and/or not in the public's best interest.
- Consistent violations or misuse of LEIN.
- Prohibitions listed in CJIS and/or MSP policies.
- As requested by the local office TAC or director.
- As requested by the MSP.

When necessary to explain the reason for pause, termination or denial of direct access, only public source information can be disseminated.

Rap Back and Remediation

Rap Back services provide continuous monitoring of employees required by law to be fingerprinted and background checked for direct access to LEIN. If an employee is not qualified to gain access, the employee may not be eligible to work in a position requiring direct access to LEIN.

If an employee is denied access due to results from a fingerprint report or a Rap Back and wishes to contest the decision, the employee may contact the central office TAC, human resources and/or MSP for remediation.

Fingerprint Access Validation

Central office TAC must annually review direct access accounts to ensure that continued access to fingerprint reports and Rap Back notifications commensurate with the requirements for direct access. Subscriptions to fingerprint reports and Rap Back must be terminated when the employee is confirmed to no longer require direct access into LEIN.

Direct Access

MDHHS is a direct access agency with access to non-public LEIN information via the MiCJIN Talon system. A person who directly accesses LEIN information is the appointed operator,TAC, or LASO.

To obtain authorization for direct access, a person must pass a state fingerprint criminal history background check and complete the following:

- Attend an operator and/or TAC training and have a passing grade of no less than 70 percent.
- Attend security/privacy awareness and training, see *LEIN: Security/Privacy Awareness and Training*, in this item.
- Sign forms: MDHHS 5518, LEIN Notice of Criminal Penalties, and MDHHS 5528, Access & Operator Request: Security Agreement.

The operator and/or TAC training and forms must be completed within the first six months of appointment and biennially thereafter. The security/privacy awareness and training must be completed before access or review of CJI and annually thereafter.

To maintain system integrity and reduce the threat for potential breach, appointed positions for direct access are limited. The allowable number of operators per local office is a ratio of 15 percent of the number of total requesters at that location.

Example: A local office with 40 requesters can have up to six operators (40 x .15 = 6).

The allowable number of TACs per local office is one primary with two serving as back up. To request additional operators and/or TACs beyond the noted ratio, send a justification request to the central office TAC.

Fingerprint Clearance Application

For an applicant to apply for a fingerprint clearance for direct access to LEIN, complete the following process:

1. Complete RI-030, LiveScan Fingerprint Background Check Request, form. This form is required by MSP to verify staff authorized permission to be fingerprinted allowing MDHHS to receive the individual's criminal history information record.

2. Schedule a fingerprint appointment through Idemia agency or go to a police station.

3. Submit signed RI-030 to the central office TAC to allow for review of results and to retain form for audit purposes.

Upon being fingerprinted, the central office TAC will receive any applicable Rap Back notices, see *Rap Back and Remediation,* in this item.

Indirect Access

Indirect access is having the authority to review CJI; but, without direct access to MiCJIN, as used to conduct transactional activity within the LEIN.

Authorized users with indirect access may include any agency staff required to review and interpret CJI as part of a case review. Staff may include, but are not limited to, case managers, supervisors, managers, and directors.

Authorized users who have indirect access to LEIN reports must complete the following:

- Attend security/privacy awareness and training, see *LEIN: Security/Privacy Awareness and Training*, in this item.

- Sign form: MDHHS 5518, LEIN Notice of Criminal Penalties.

The signing of the form must be completed within the first six months of appointment and again biennially thereafter. The security/privacy awareness and training must be completed before access or review of CJI and annually thereafter.

LEIN: Security/Privacy Awareness and Training

Security/Privacy Awareness and Training (AT) is required before direct access to, or review of CJI, and any unescorted access to the physically secure location or controlled environment. Training assignment is based on an individual's role and access need:

- **Basic Role: "Individuals with Unescorted Access to Secure Locations" (previously known as Level 1)**: Personnel with Unescorted Access to a Physically Secure Location. This role is designed for people who have access to a secure area that contains CJI but are not authorized to access the CJI. Examples include building maintenance and janitorial personnel. Individuals without online access may sign the MDHHS-5502, Security Awareness Acknowledgement for Personnel with only Physical Access to Physically Secure Locations, form.

- **General Role: "General Users" (previously known as Level 2 and Level 3a/b):** All personnel with access to CJI. This role is designed for people who have physical (paper copies) and logical (computer systems) access to CJI. This training was previously split between those who have access to physical only and those who have access to both physical and logical CJI. The Federal Bureau of Investigation (FBI) has combined the two modules into "General Users." Examples include all assigned LEIN operators, local and central office terminal agency coordinators, requesters, and reviewers of CJI.

- **Privileged Role: "Privileged Users" (previously known as Level 4):** Personnel with information technology roles. This role is designed for all information technology personnel including system administrators, security administrators, network administrators, those that require more access than a general user, and those who can create user accounts for systems that access CJI (network accounts, multibridge accounts, etc.), but are not an assigned Local Area Security Officer (LASO), for example TACs who create accounts into MiCJIN.

- **Security Role: "Organizational Personnel with Security Responsibilities" (previously known as Enhanced Security Training for LASOs):** This role is designed for personnel with

the responsibility of ensuring the confidentiality, integrity, and availability of CJI and the implementation of technology in a manner compliant with the CJISSECPOL. Examples include those serving as a LASO for LEIN use and access.

Appointed TACs and/or LASOs must assign staff to the appropriate AT and monitor individual information system training activities.

LEIN Security/Privacy Awareness and Training (AT) is required to be completed:

- Before authorizing access to the LEIN information or performing assigned duties,
- Before authorizing unescorted access to the physically secure location or controlled environment,
- When required by information system changes, and
- Annually.

Non-completion of AT will result in removal of access to, or review of, CJI or denial to unescorted access to the physically secure location. For Retention of the training record, see SRM 700, LEIN for LEIN Document Disposal and Retention.

Access Validation

Access to accounts is based on least privilege, which permits only authorized access for users which are necessary to accomplish assigned tasks in accordance with roles and responsibilities of job functions. Local office TAC or LASO must annually review all direct access accounts and report the validation to the central office TAC.

Local office TAC or LASO must annually review authorized user access to ensure that access and account privileges commensurate with the following statuses/need: job functions, policy requirements, and employment status on systems that contain CJI.

Immediately, but no longer than one business day, report to the central office TAC any of the following situations or status of any appointed operator, LASO, or TAC, including:

- Any extended leave of more than 30 days.
- Termination or departure.
- Any name changes.

- Any transfer to another local office.
- Not accessing their account in 6 months.
- Any violations of use of CJI.
- Any other need for direct access removal.
- Any violations or misuse of LEIN.

The central office TAC will disable account access for any of the above situations. If any account needs to be reinstated, the central office TAC will review current training certifications, fingerprint subscription, and position authorizations to determine approval.

Penalties for violating this policy section may result in network removal, access revocation, or corrective or disciplinary action, and termination of employment. For DTMB access control policies, see DTMB technical Standard for Access Control,1340.00.020.01.

PHYSICAL PROTECTION REQUIREMENTS

To access and view CJI from LEIN, secure the physical location according to the below MSP-approved layout as described in this policy, and in accordance with the CJIS security policy.

Physically Secure Location

A physically secure location is a facility, an area, a room, or a group of rooms within a facility with both the physical and personnel security controls sufficient to protect the LEIN-based CJI and associated information systems. The perimeter of the physically secure location should be:

- Noticeably identifiable and separated from non-secure locations by physical controls.
- Controlled and secured.
- Identified as restricted non-public areas with a sign at the entrance.

To meet the physical protection requirements, units and counties with access to CJI must create a secured area with either a preferred set up or a controlled area.

Preferred Set Up

The preferred secure room set up is to have one vacant room with the following: a lock-capable door, a posted sign on the door that reads “Processing CJI…Do Not Enter," and shared printers must have lock/password capability. This room can have multiple computers that are only accessible by the local office LEIN operator(s) and terminal agency coordinator(s) (TACs).

Controlled Area

Controlled areas are configured working stations assigned to operators for purposes of processing CHRI requests from LEIN. Configured LEIN operator stations shall include the following:

- Have up to five workstation configurations in the local office, depending on the number of operators per office.
- Monitors used to query/view CJI positioned away from door or entry of workstation.
- Privacy screen filters placed on monitors even when monitors are not facing the workstation door opening to restrict viewing by unauthorized personnel who may enter the workstation.
- Workstation walls high enough to restrict viewing by the average height person.
- Locking functionality for any physical media such as LEIN printouts, TAC Manual, LEIN Manual, etc. when not in use.
- Power off computers after working hours.
- Use of the Windows system lock during working hours when employees are away from their desk.
- Use of the LEIN application only when performing LEIN queries.
- A sign on the outside of the workstation that announces when CJI is being processed. Example: “Processing CJI…Do Not Enter.”
- Use of the lock job function if printing CJI on a shared print until the authorized person is at the printer.

Security measures need to be in place for local offices with multiple floors/areas with open workstations that access CJI from LEIN. To secure the area ensure the doors that access the multiple rooms where CJI is accessed is locked and any unescorted access of individuals to those rooms complete the Basic Role Security/Privacy Awareness Training or sign the MDHHS-5502, Security Awareness Acknowledgement for Personnel with Only Physical Access to Physically Secure Locations, form.

Note: Controlled areas may include home offices, agency assigned workstation or other vacant office spaces based on local office capacity. An agency assigned workstation configuration design for LEIN operators is on file and available with the Bureau of Organizational Services. Directors are to contact the central office TAC to discuss variations of office arrangement that will meet compliance.

Note: Configured workstations will become the permanent operator station. When the appointed operator is no longer serving their role and another staff is appointed, the former operator must vacate the station for the new operator to assume.

PHYSICAL ACCESS AUTHORIZATIONS

Authorized users must take the necessary steps to prevent and protect the agency from physical, logical, and electronic breaches. They are responsible for maintaining a current list of authorized users and informing the central office TAC of any changes.

All users with physical access must meet the following requirements:

- Meet the minimum personnel screening requirements prior to CJI access.
    - Conduct a state fingerprint-based record check within 30 days of assignment for all LEIN users who have **direct** access to LEIN.
    - Complete the LEIN Security/Privacy Awareness and Training certificate before access to or review of CJI and recertify annually thereafter.
- Be aware of who is in their secure area before accessing confidential data.

- Take appropriate action to protect all confidential data.
- Protect all terminal monitors with viewable CJI displayed on monitor and not allow viewing by the public or escorted visitors.
- Private contractors/vendors and custodial staff with access to physically secure locations or controlled areas (during CJI processing) shall be escorted or required to take the LEIN Security/Privacy Awareness Training or sign the MDHHS-5502, Security Awareness Acknowledgment for Personnel with Only Physical Access to Physically Secure Locations, form.

- Protect and not share any individually issued keys, proximity cards, computer account passwords, etc.
  - Report loss of issued keys, proximity cards, etc.
  - Safeguard and not share passwords, personal identification numbers (PIN), security tokens (such as VPN), and all other facility and computer systems security access procedures.
- Protect computer/tablet from viruses, worms, Trojan horses, and other malicious code; see APL 68E-110, Protection from Malicious Software Policy and Procedure.
- Protect web usage; see *Information Technology Support: DTMB/IT,* in this item.
- Do not use personally owned devices on computers with CJI access or to access and/or review CJI.
- Secure dissemination and review of CJI when sending or receiving via phone, fax, or email. Follow physical access authorization requirements detailed within this policy.
- Report any physical security incidents to the central office TAC to include facility access violations, loss of CJI, and loss of laptops, cellular phones, thumb drives, CDs/DVDs, and printouts containing CJI.
- Properly release CJI only to authorized personnel and crosscut shredded printouts when no longer needed.
- Ensure data centers with CJI are physically and logically secure.

- Keep the local office and central office TACs informed of when CJI access is no longer required. In the event of terminated employment, the individual must surrender all property and access managed by MDHHS and DTMB.
- Ensure the perimeter security door securely locks after entry or departure. Do not leave any perimeter unprotected, such as a propped door.

Authorized Unescorted Access

Personnel with access to physically secure locations or controlled areas, but who do not directly or indirectly access CJI, must take Basic Role Security Awareness and Training or sign the MDHHS-5502, Security Awareness Acknowledgment for Personnel with Only Physical Access to Physically Secure Locations, form. These personnel include, but are not limited to: support personnel, other MDHHS unit staff, private contractors/vendors, visitors, and custodial staff.

Authorized Escorted Access

An escort is an authorized user who always accompanies a visitor while within a physically secure location to ensure the protection and integrity of the physically secure location and any CJI. The use of cameras or other electronic means used to monitor a physically secure location does not constitute an escort.

A visitor is a person who visits the MDHHS facility on a temporary basis, who is not a MDHHS employee, and who requires escorted access to the physically secure locations within the MDHHS where LEIN-based CJI and associated information systems.

Visitors must:

- Check in before entering a physically secure location.
- Be accompanied by a MDHHS authorized user as an escort at all times.
- Follow the MDHHS policy for authorized unescorted access:
  - For personnel who require frequent unescorted access to restricted area(s).

- For private contractors/vendors who require frequent unescorted access to restricted area(s).

- Not be allowed to view screen information, mitigating shoulder surfing.

- Not be allowed to sponsor another visitor.

- Not enter a secure area with electronic devices unless approved by the MDHHS LASO, to include cameras and mobile devices. No photographs allowed without permission of the MDHHS assigned personnel.

Courteously escort individuals not having any legitimate business in the restricted area to a public area of the facility. Staff should question any unescorted stranger in a physically secure area. If resistance or behavior of a threatening or suspicious nature is encountered, security personnel shall be notified or call 911.

Authorized Offsite Access

MDHHS' authority for use of the LEIN application is based on Michigan laws, and as such, staff must be within the state of Michigan to generate information from the LEIN application. Authorized locations for direct access include a Michigan-based residence and/or any MDHHS office that meets the physically secure, controlled environment requirements noted within this policy.

Authorized offsite access is when a MDHHS authorized user, generating and/or reviewing CJI from LEIN, has been given authorization to access the CJI from outside of the staff's assigned agency office building.

Requirements for access to CJI must:

- Adhere to the CJIS security policy on physical security, controlled area, requirements.

- Be within a state of Michigan residence or agency office to generate information from the LEIN application.

- Not access the CJI using a public connection. For example, a coffee shop, at a client’s residence, using public hotspot, etc.

- Allow for in-home or office audits.

- Only connect directly to state of Michigan VPN via an ethernet cord or Wi-Fi.
- Only use state-issued devices and applications.
- Not print LEIN results from a home or public printer.
- Follow mobile device policy when receiving or reviewing CJI from a mobile device. See SRM 700, LEIN.
- Not store CJI on a network drive unless it meets CJIS policy restrictions and is monitored and tracked by a local office TAC for appropriate authorized access.

Penalties

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

Violation of any of the requirements in this policy by any visitor can result in similar disciplinary action against the sponsoring employee and can result in termination of services with any associated consulting organization or prosecution in the case of criminal activity.

INFORMATION TECHNOLOGY SUPPORT: DTMB/IT

In coordination with above roles, all MSP-vetted DTMB IT support staff will protect CJI from compromise at MDHHS by adhering to the MDHHS/DTMB Management Control Agreement (MCA), the National Institute of Standards and Technology (NIST) requirements, and the agency policies, see Technology/IT Policies, Standards & Procedures (PSP) and APS 1370, System and Information Integrity.

Media Protections

Protect and control digital and non-digital media containing CJI within physically secure locations or controlled areas and encrypt CJI on digital media when physical and personnel restrictions are not feasible. Digital media includes flash drives, diskettes, magnetic tapes, external or removable hard disk drives (e.g., solid state, magnetic), compact discs, and digital versatile discs. Non-

digital media includes paper and microfilm and must be protected at the same level as information would be in electronic form. See, DTMB 1340.00.110.01, Media Protection Standard.

PROCESS FOR REQUESTING A LEIN RECORD

CJI can only be requested by MDHHS authorized users who are assigned or associated to the open, active case and requested for purposes outlined in policy. The person's name as reflected in the electronic case record should be the name written on the DHS-268 and DHS-269 forms. See SRM 700, LEIN for requesting a LEIN Record.

PROCESS FOR REQUESTING DIRECT ACCESS

Appointed TACs, operators, and LASOs can have direct access to the MiCJIN application. To request direct access, first schedule an appointment to be state fingerprinted using the RI-030, LiveScan Fingerprint Background Check Request, form.

Upon notification of fingerprint clearance, the following steps can then occur:

1. Attend an operator and/or TAC training. Have a passing grade of no less than 70 percent.

2. Attend LEIN Security/Privacy Awareness Training, see *LEIN Security/Privacy Awareness Training*, in this item.

3. Sign forms: MDHHS 5518, LEIN Notice of Criminal Penalties, and MDHHS 5528, Access & Operator Request: Security Agreement.

4. Turn all tests and documents into the local office TAC.

The local office TAC will bundle the information and forward copies to the central office TAC. The originals will remain on file at the local office. See Record Retention and Disposal Schedule, 49/BCW, Child Welfare Policy and Programs for record retention policy. If the web link does not work, please call 517-335-9132 for a copy of an agency-specific schedule.

Renew the LEIN Security/Privacy Awareness Training annually and tests and forms biennially to continue to serve in the appointed role.

DISSEMINATION AUTHORITY

Information solely from LEIN must not be included in department reports or case files (including hard copy or electronic- such as the child welfare electronic case management system, BITS, Bridges, ASCAP, etc.). Do not disclose any unverified criminal history information to the individual on which the LEIN clearance was completed. Case files and documents or court reports may include corroborated verified information when the information is required, or the information is the basis for case decision-making. See SRM 700, LEIN for requirements for documenting in reports, files or narratives and dissemination authority.

VIOLATIONS AND BREACHES

CJIS Policy Council Act, MCL 28.214(6)(a) explains penalties to a person who intentionally uses or discloses nonpublic information for personal gain or in a manner that is not authorized by law or rule.

The first offense is a misdemeanor punishable by 93 days imprisonment or $500 fine, or both. The second offense is a felony punishable by not more than four years imprisonment or $2,000 fine, or both.

Staff found to have misused LEIN information will be subject to disciplinary action up to and including dismissal.

Incident Response

DTMB is required to annually review and update the incident response policy and procedure. Any security incidents involving systems used to process, store, or transmit CJI, report to DTMB. See, DTMB, Incident Response policy, 1340.00.090.01. When investigating an incident that significantly endangers the security or integrity of CJI or CJIS, the Local Agency Security Officer (LASO) shall complete a CJIS-016, Information Security Officer (ISO) Computer Security Incident Report form and submit to the MSP, ISO.

Immediately, but not to exceed 24 business hours after discovery, report suspected violations of LEIN policy pertaining to

unauthorized access, use or disclosure of CJI to the local office TAC and the central office TAC.

The central office TAC must report egregious incidents to MSP LEIN field services within 48 business hours from receiving the written violation report. MSP may investigate or send a letter for an agency investigation. They may also request a corrective action plan or provide penalty recommendations.

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.

FORMAL AUDITS

Local office TACs are responsible for periodically validating LEIN use to ensure proper use and procedures of accessing LEIN information. The MSP will triennially audit local office use.

POLICY CONTACT

For questions about this policy, contact Joy Thelen, central office TAC, at the CPS & Redesign via email at ThelenJ12@michigan.gov