Book	Policy Manual
Section	Board Review 39.1
Title	Vol. 39, No. 1 - September 2024 Revised CRIMINAL JUSTICE INFORMATION SECURITY (NON-CRIMINAL JUSTICE AGENCY)
Code	po8321
Status	
Adopted	May 13, 2013
Last Revised	April 12, 2021
Last Reviewed	February 24, 2021

Revised Policy - Vol. 39, No. 1

8321 - **CRIMINAL JUSTICE INFORMATION SECURITY (NON-CRIMINAL JUSTICE AGENCY)**

The District is required by State law to have the Michigan State Police (MSP) obtain both a State and a Federal Bureau of Investigation ("FBI") criminal history record information ("CHRI") background check report for all employees of the District and contractors, vendors and their employees who work on a regular and continuous basis in the District. This policy provides the appropriate access, maintenance, security, confidentiality, dissemination, integrity, and audit requirements of CHRI in all its forms, whether at rest or in transit. This policy/procedure shall be reviewed and updated at least annually and following any security incidents involving CHRI. To assure the security, confidentiality, and integrity of the CHRI background check information received from the MSP/FBI, the following standards are established:

A. **Sanctions for Non-Compliance**

Employees who fail to comply with this policy, State and Federal law, current CJISSECPOL, rules or regulations, and any guidelines issued to implement this policy will be subject to discipline for such violations. Discipline can ~~will~~ range from counseling and retraining to discharge and prosecution, based on the nature and severity of the violation, at the District's discretion. All violations will be recorded in writing, with the corrective action taken. The Superintendent shall review, approve, sign, and date all such corrective actions.

B. **Local Agency Security Officer (LASO)**

The Human Resources Director ~~Specialist~~ shall be designated as the District's Security Officer ("LASO"). ~~and~~ The LASO is an authorized user/personnel, has completed a fingerprint-based background check where required, and has been found appropriate to access CHRI, and an employee directly involved in evaluating an individual's qualifications for employment or assignment. The LASO shall be responsible for overall implementation of this policy and for data and system security. This shall include:

1. identifying who is using or accessing CHRI and/or systems with access to CHRI;
2. identifying and documenting any equipment connected to the State system;
3. ensuring that personnel security screening procedures are being followed as set forth in this policy;
4. ensuring that approved and appropriate security measures are in place and working as expected;
5. supporting policy compliance and instituting the incident response reporting procedures;
6. ensuring annual awareness and training is being completed by all personnel with authorized access to the CHRI;
7. ensuring that the Michigan State Police are promptly informed of any security incidents involving the abuse or breach of the system and/or access to criminal justice information;

8. reviewing and updating information security policy/procedures annually or after security incidents involving CHRI;

9. ~~to the extent applicable, identifying and documenting how District equipment is connected to the Michigan State Police system;~~

10. employing one (1) or more of the following techniques to increase the security and privacy awareness of system users: displaying posters, offering supplies inscribed with security and privacy reminders; displaying logon screen messages; generating email advisories or notices from organizational officials; conducting awareness events; and

11. to the extent applicable, identifying who is using the Michigan State Police approved hardware, software, and firmware, and ensuring that no unauthorized individuals have access to these items.

The District's LASO shall be the point of contact for the Michigan State Police and should be the person most knowledgeable about this policy. The District's LASO shall be designated on the appropriate form as prescribed and maintained by the Michigan State Police. A new form shall be submitted every time a new LASO is designated and kept on file by the District indefinitely.

C. **Privacy Act Statement Disclosure**

The District shall ensure that the applicant receives the Federal Privacy Act Statement Disclosure by providing the applicant with the most current version of the MSP RI-030 Live Scan consent form. The applicant will receive this information by hard or electronic copy.

D. **Agency User Agreements**

The District shall enter into any required User Agreement for Release of CHRI ("User Agreement"), and future amendments, by the Michigan State Police necessary to access the required CHRI on applicants, volunteers, and all other statutorily required individuals, such as contractors and vendors and their employees assigned to the District. Agreements are in place to provide data ownership, individual roles, responsibilities, etc. The District shall request a new user agreement in the event they have a legal name change, they move to a new physical address, or they wish to add or remove fingerprint reason codes. The most current copy of the Agreement shall be maintained on file at the agency indefinitely. The LASO shall be responsible for the District's compliance with the terms of any such User Agreement.

E. **Personnel Security**

Authorized users/personnel shall be individuals who have been appropriately vetted through a national fingerprint-based background check, as required by school safety legislation, and have been granted access to CHRI data, wherein access is only for the purpose of evaluating an individual's qualifications for employment or assignment.

1. **Subsequent Arrest/Conviction** - If an individual granted access to criminal justice information is subsequently arrested and/or convicted, access shall be suspended immediately until the matter is reviewed by the LASO to determine if continued access is appropriate. Such determination shall be recorded in writing, signed, dated, and maintained with the individual's file. In the event that the LASO has the arrest/conviction, the Superintendent (if not the designated LASO) shall make the determination. If the Superintendent is also the designated LASO, the determination shall be made by the Human Resources Specialist; except that, as noted in D(1)(a), individuals with a felony conviction of any kind will have ~~their~~ access indefinitely suspended.

2. **Public Interest Denial** - If the LASO determines that access to criminal justice information by any individual would not be in the public interest, access shall be denied whether that person is seeking access or has previously been granted access. Such decision and reasons shall be in writing, signed, dated, and maintained in the individual's file.

3. **Approval for Access** - All requests for access to criminal justice information shall be as specified and approved by the LASO. Any such designee must be a direct employee of the District. The District must maintain a readily accessible list that includes the names of all LASO approved personnel with access to criminal justice information, as well as the reason for providing each individual access. This list shall be made available to the Michigan State Police upon request.

4. **Notification of Termination of Employment/Access or Transfer/Re-assignment** - When an employee's access or employment is terminated, or if the duties for accessing criminal justice information have been transferred or re-assigned to another individual, the LASO shall be notified promptly in writing. The individual responsible for the termination or transfer/re-assignment shall directly notify the Superintendent.

5. **Termination of Employment/Access** – Within twenty-four (24) hours of the termination of employment, all access to criminal justice information shall be terminated immediately for that individual, such as requiring the individual to return any keys or access cards to buildings, offices, and/or files, or closing the individual's account and/or blocking access to any systems containing such information at the District.

6. **Transfer/Re-assignment** - When an individual who has been granted access to criminal justice information has been transferred or re-assigned to other duties, the LASO shall determine whether continued access is necessary and appropriate. If not, the LASO~~s/he~~ shall take such steps as necessary to block further access to such information within the twenty-four (24) hour period immediately following the transfer or reassignment. If such access is not necessary and appropriate, steps to eliminate the individual's access will be taken immediately, such as requiring the individual to return any keys or access cards to buildings, offices, and/or files, or closing the individual's account and/or blocking access to any systems containing such information at the District.

F. **Media Protection**

Access to digital and physical media in all forms, which contains criminal history background information provided by the Michigan State Police through the statutory record check process, is restricted to authorized individuals only. Only individuals involved in the hiring determination of both District employees and volunteers shall be authorized to access digital and physical media containing CHRI.

1. **Media Storage and Access** – All digital and physical media shall be stored in a physically secure location or controlled area, such as a locked office, locked cabinet, or other similarly secure area(s) which can only be accessed by authorized individuals. If such security cannot be reasonably provided, then all digital CHRI background data shall be encrypted. Access to such media will be secured at all times when not in use or under the supervision of an authorized individual. Digital media shall be stored on a District or School server and unless encrypted, shall be maintained in a lockable filing cabinet, drawer, closet, office, safe, vault, etc. Storage on a third party server, such as cloud service, is not permitted. Storage of digital media must conform to the requirements in AG 8321 and must be encrypted. Physical media will be stored within individual records when feasible, or by itself when necessary, and will be maintained in a lockable filing cabinet, drawer, closet, office, safe, vault, etc.

2. **Media Transport** – Digital and physical media shall only be transported upon sufficient justification approved by the LASO. Digital and physical media shall be protected when being transported outside of a controlled area. Only authorized individuals shall transport the media. Physical media (e.g. printed documents, printed imagery, etc.) shall be transported using a locked container, sealed envelope, or other similarly secure measure. To the extent possible, digital media (e.g., hard drives and removable storage devices such as disks, tapes, flash drives, and memory cards) shall be either encrypted and/or be password protected during the transport process. The media shall be directly delivered to the intended person or destination and shall remain in the physical control and custody of the authorized individual at all times during transport. Access shall only be allowed to an authorized individual.

3. **Media Disposal/Sanitization** – When the CHRI background check is no longer needed, the media upon which it is stored shall either be destroyed or sanitized. The LASO and the Superintendent shall approve in writing the media to be affected. This record shall be maintained by the LASO during the individual's active employment plus an additional six (6) years. **[Note: the regulations do not specify a specific period for maintaining this information. This time period is suggested based on the State of Michigan's background information retention schedule and will likely cover most statutes of ~~limitaiton~~ limitation and can be retained in digital format.]**

    a. **Digital Media** - Sanitization of the media and deletion of the data shall be accomplished by either overwriting at least three (3) times or by degaussing, prior to disposal or reuse of the media, but optical media (such as CDs and DVDs) will be physically destroyed. If the media is inoperable or will not be reused, it shall be destroyed by shredding, cutting, or other suitable method to assure that any data will not be retrievable.

    b. **Physical Media** – Disposal of documents, images, or other type of physical record of the criminal history information shall be cross-cut shredded or incinerated. Physical security of the documents and

their information shall be maintained during the process by authorized individuals. Documents may not be placed in a wastebasket or burn bag for unauthorized individuals to later collect and dispose of.

All disposal/sanitization shall be either conducted or witnessed by authorized personnel to assure that there is no misappropriation of, or unauthorized access to, the data to be deleted. Written documentation of the steps taken to sanitize or destroy the media shall be maintained for ten (10) years, and must include the date as well as the signatures of the person(s) performing and/or witnessing the process. (See also, AG 8321.)

4. **Personal Mobile Devices** – A personally owned mobile device (mobile phone, tablet, laptop, etc.) or no identifiable owner digital media device shall not be authorized to access, process, store or transmit criminal justice information unless the District has established and documented the specific terms and conditions for personally owned mobile devices through a Mobile Device Management ("MDM") system. An MDM is not required when receiving CHRI from an indirect access information system (i.e., the system provides no capability to conduct transactional activities on State and national repositories, applications, or services).

5. **CHRI Background Check Consent and Documentation**

   All individuals requested to complete a fingerprint-based CHRI background check must execute Michigan State Police Form RI-088A at the time of application, and be notified fingerprints will be used to check the criminal history records of the FBI, prior to completing a fingerprint-based CHRI background check. The most current and unaltered Livescan form (RI-030) will satisfy this requirement and must be retained. Individuals subject to a fingerprint-based CHRI background check shall be provided the opportunity to complete or challenge the accuracy of the individual's criminal history record.

   Some type of documentation identifying the position for which a fingerprint-based CHRI background check has been obtained must be retained for every CHRI background check conducted, such as the "Agency User Agreement" (RI-087), an offer letter, employment agreement, new hire checklist, employment contract, volunteer background check form, etc.

6. **Controlled Area/Physical Protections**

   All CHRI obtained from the Michigan State Police pursuant to the statutorily required background checks shall be maintained in the Human Resources Office, which is a physically secure and controlled area. The following security precautions will apply to the controlled area:

   a. Limited unauthorized personnel access to the area during times that criminal justice information is being processed or viewed.

   b. The controlled area shall be locked at all times when not in use or attended by an authorized individual.

   c. Information systems devices (e.g., computer screens) and physical documents, when in use, shall be positioned to prevent unauthorized individuals from being able to access or view them.

   d. Encryption shall be used for digital storage of criminal justice information. (See AG 8321)

7. **Passwords (Standard Authentication)**[1]

   All authorized individuals with access to computers or systems where processing is conducted or containing criminal justice information must have a unique password to gain access. This password shall not be used for any other account to which the individual has access and shall comply with the following attributes and standards:

   a. at least eight (8) characters long on all systems

   b. not be a proper name or a word found in the dictionary

   c. not be the same as the user identification

   d. not be displayed when entered into the system (must use feature to hide password as typed)

   e. not be transmitted in the clear outside of the secure location used for criminal justice information storage and retrieval

f. must expire and be changed every ninety (90) days

g. renewed password cannot be the same as any prior ten (10) passwords used (See also, AG 8321)

8. **Security Awareness Training**

All individuals who are authorized by the District to have access to criminal justice information or to systems which store criminal justice information shall have basic security awareness training as part of initial training for new users prior to accessing CJI and annually thereafter, and when required by system changes or within thirty (30) days of any security event for individuals involved in the event.~~within six (6) months of initial assignment/authorization and every two (2) years thereafter.~~ LASOs require enhanced training on the specific duties and responsibilities of those positions and the impact those positions have on the overall security of information systems.

Training is a role-based security and privacy training for personnel with the following roles:

a. **Basic Role:** All individuals with unescorted access to a physically secure location. (Not typical for NCJAs)

b. **General Role:** All personnel with access to CJI. This level is designed for people who have physical and logical access to CJI.

c. **Privileged Role:** This level is designed for all information technology personnel including system administrators, security administrators, network administrators, etc. More access is needed than a general user, but not an assigned LASO. (i.e., CHRISS Administrator)

d. **Security Role:** This level is designed for personnel with the responsibility to ensure the confidentiality, integrity, and availability of CJI and the implementation of technology in a manner compliant with the CJISSECPOL. (i.e., LASO)

The training shall, to the extent possible, be received through a program approved by the Michigan State Police. A template of the training is provided on the Michigan State Police's website. At a minimum, the training shall comply with the standards established by the U.S. Department of Justice and Federal Bureau of Investigation for Criminal Justice Information Services. (See AG 8321.) A record shall be kept current of all individuals who have completed the security awareness training.

9. **Secondary Dissemination of Information**

If criminal history background information received from the Michigan State Police is released to another authorized agency under the sharing provision designated by the revised school code, a log of such releases shall be maintained and kept current for all dissemination outside of the CHRISS system indicating:

a. the date of release;

b. record disseminated;

c. method of sharing;

d. agency personnel that shared the CHRI;

e. the agency to which the information was released;

f. the name of the individual recipient at the agency; and

g. whether authorization was obtained.

A log entry need not be kept if the receiving agency/entity is part of the primary information exchange agreements between the District and the Michigan State Police. A release form consenting to the sharing of CHRI shall be maintained at all relevant times.

If CHRI is received from another District or outside agency, an Internet Criminal History Access Tool ("ICHAT") background check shall be performed to ensure the CHRI is based on personal identifying information, including the individual's name, sex, and date of birth, at a minimum.

Incident Handling and Responses

The District shall establish operational incident handling procedures for instances of an information security breach. Information security incidents are major incidents that significantly endanger the security or integrity of CHRI. The District will identify responsibilities for information security incidents and include how and who to report such incidents to. The District will ensure appropriate security incident capabilities exist and should incorporate the lessons learned from ongoing incident handling activities. The District will ensure procedures exist and are implemented for a follow-up action of a security breach and for the collection of evidence in cases of legal action. All individuals with direct or indirect access to CHRI shall be trained on how to handle an information security incident, and such training will be included within the provided awareness and training. Information system security incidents shall be tracked using Form CJIS-016 and documented on an ongoing basis. Incident-related information may be obtained from audit monitoring, network monitoring, physical access monitoring, and user/administrator reports. The LASO shall maintain completed security incident reporting forms for three (3) years or until legal action (if warranted) is complete, whichever timeframe is greater. The District shall implement steps for incident handling capabilities, for both digital and physical CHRI media. Incident response testing will be conducted annually using the following tests: tabletop or walk-through exercises, simulations, or other agency appropriate tests. At a minimum, the following will be implemented:

	Physical - Hard Copy CHRI	**Digital - Digitally Saved CHRI**
1. Preparation	The CHRI container will be locked at all times in the business office where it is stored. The office must be locked when the office staff is not present.	Firewalls, virus protection, and/or malware/spyware protection shall be implemented and maintained to prevent unauthorized access or intrusion of the information systems.
2. Detection	Unauthorized activities or physical intrusions to the building shall be monitored by building alarm or video surveillance. Doors must be locked and checked at night.	Electronic intrusions shall be monitored and detected by the firewalls, virus protection, and/or malware/spyware protection software.
3. Analysis	The LASO will work with police authorities to determine how the incident occurred and what data was affected.	The LASO shall work with the IT department to determine what systems or data were compromised and affected.
4. Containment	The LASO shall lock uncompromised CHRI information in a secure container, or transport CHRI to a secure area.	The IT department shall stop the spread of any intrusion of the information systems and prevent further damage.
5. Eradication	The LASO shall work with law enforcement to remove any threats and compromised CHRI data.	The IT department shall remove the intrusion of the information systems before restoring the system. All steps necessary to prevent recurrence shall be taken before restoring the system.
6. Recovery	The Police shall handle and/or oversee the recovery of stolen CHRI media. The LASO may contact MSP for assistance in re-fingerprinting if necessary.	The IT department shall restore the agency information system and media to a safe environment.

When an incident involving the security of CHRI or systems with access to CHRI is discovered, the following procedures shall be followed:

A. ~~The LASO shall be notified immediately.~~All personnel are required to report suspected incidents to the LASO immediately, but not to exceed one (1) hour after discovery. As such, personnel who become aware of an incident or believe an incident has occurred should report to the following individuals, in order:

1. LASO
2. Superintendent

B. The breach shall be assessed (including determination of whether notification to individuals is needed, assessment of the extent of the harm, and identification of applicable privacy requirements) and steps taken to correct the situation:

   1. access shall be stopped for any unauthorized user;
   2. media shall be secured;
   3. systems shall be shut down as necessary to avoid further exposure to unauthorized access or dissemination of CHRI;
   4. such other steps are deemed necessary by the LASO or authorized personnel involved in assessing the incident.

C. All necessary information regarding the security breach and District responses shall be recorded, analyzed, and preserved, including who was involved in taking incident response measures.

D. The LASO shall be responsible for filing the incident report with the MSP using the CJIS-016. Completed CJIS-016 forms shall be retained on an ongoing basis to meet policy requirements for tracking.

   The LASO shall monitor MSP information/guidance on incident reports and train authorized users with access to CHRI on detection and response to security incidents.

E. **Mobile Device - Incident Handling and Response**

   1. The LASO shall be notified immediately.
   2. The breach shall be assessed and steps taken to correct the situation~~situations~~:

      a. access shall be stopped immediately, and remotely if necessary, for any authorized user;
      b. media shall be secured and steps taken to identify how the incident occurred and what systems or data were compromised or affected;
      c. systems shall be shut down as necessary to avoid further exposure to unauthorized access or dissemination of CJI;
      d. such other steps as are deemed necessary by the LASO or authorized personnel involved in assessing the incident.

   3. All necessary information regarding the security breach and District responses shall be recorded, analyzed, and preserved, including who was involved in taking incident response measures.
   4. Steps shall be taken to restore the device and media to a safe environment.
   5. The LASO shall be responsible for filing the incident report with the MSP using form CJIS-016. A copy of the completed form shall be retained and produced to MSP upon request.

      When a device is lost the District shall document and indicate how long the device has been lost. Special reporting procedures for mobile devices shall apply in any of the following situations:

      a. for a lost device, report if the owner:

         1. believed the device was locked;
         2. believed the device was unlocked;
         3. could not validate the device's locked state;~~.~~

b. for a total loss of a device, report if:

1. CHRI was stored on the device;

2. the device was locked or unlocked;

3. capable of remote tracking or wiping of device;~~.~~

c. report any compromise of a device when the intrusion occurs while still in the owner's possession;

d. report any compromise outside of the United States.

F. **Collection of Evidence**

Where an information security incident involves legal action against the District or an individual (either civil or criminal), evidence shall be collected, retained, and presented in accordance with the rules of evidence of the relevant jurisdiction(s). For criminal matters, local or county law enforcement shall be contacted for evidence collection. For civil matters, district legal counsel will be contacted for evidence collection.

---

[1]Applicable to districts that maintain CHRI within a digital system of records, such as a digital database, filing system, record-keeping software, spreadsheets, etc. Not applicable if CHRI kept solely via e-mail and/or paper copies.

Legal

Ref: Criminal Justice Information Services - Security Policy (Version 5.6, 2017),

U.S. Dept. of Justice and Federal Bureau of Investigation

Noncriminal Justice Agency Compliance Audit Review, Michigan State Police, Criminal Justice Information Center, Audit and Training Section

Conducting Criminal Background Checks, Michigan State Police, Criminal Justice Information Center

Last Modified by Tamara Young on October 24, 2024