CRIMINAL HISTORY RECORDS CHECK – MSP REQUIREMENTS

A. Criminal Justice Information Security (Non-Criminal Justice Agency)

The District is required by State law to have the Michigan State Policy (MSP) obtain both a State and a Federal Bureau of Investigation (FBI) criminal history record information (CHRI) background check report for all employees (full-time and part-time) and contractors (under assignment to work regularly and continuous). To assure the security, confidentiality, and integrity of the CHRI background check information received from the MSP and FBI the following standards are established:

B. Local Agency Security Officer (LASO)

The Director of Human Resources shall be designated as the District’s LASO and shall be responsible for overall implementation of this policy and for data and system security. This shall include:

1. Ensuring that personnel security screening procedures are being followed as set forth in this policy

2. Ensuring that approval and appropriate security measures are in place and working as expected

3. Supporting policy compliance and ensuring the Criminal Justice Information Security Systems Agencies (CSA) Information Security Officer (ISO) is promptly informed of security incidents

4. To the extent applicable, identifying and documenting how District equipment is connected to the MSP system

5. To the extent applicable, identifying who is using the MSP approved hardware, software and firmware, and ensuring that no unauthorized individuals have access to those items

C. Agency User Agreements

The District shall enter into any required User Agreement for Release of CHRI (“User Agreement”), and future amendments, by the MSP necessary to access the statutorily required CHRI on applicants, volunteers and contractors. The LASO shall be responsible for assuring the District’s compliance with the terms of any such Agreement.
D. Security Awareness Training

All individuals who are authorized by the District to have access to criminal justice information (CJI) or to systems which store CJI shall have basic security awareness training within six (6) months of initial assignment/authorization and every two (2) years thereafter. The training shall, to the extent possible, be received through the MSP or a program approved by the MSP. At a minimum, the training shall comply with the standards established by the U.S. Department of Justice and FBI for Criminal Justice Information Services. A record shall be kept current of all individuals who have completed the security awareness training.

E. Personnel Security

All individuals that require access to any criminal justice information shall be subject to the following standards prior to granting of access:

1. Background Checks – A state of residency and a national fingerprint-based record check shall be conducted within thirty (30) days of assignment to a position with direct access to CJI or with direct responsibility to configure and maintain computer systems and networks with direct access to CJI. Background re-checks should be conducted every five (5) years.

   a. A felony conviction of any kind will disqualify an individual for access to CJI. However, the District may ask for review by the SCO in extenuating circumstances where the severity of the offense and the time that has passed would support a possible variance

   b. If any other results/records are returned, the individual shall not be granted access until the LASO reviews and determines access is appropriate. This includes, but is not limited to, any record which indicates the individual may be a fugitive or shows arrests without convictions. Such approval shall be recorded in writing, signed, dated and maintained with the individual’s file.

   c. If support personnel, contractors or custodial workers need to be in an area where CHRI is maintained or processed, they shall be escorted by or under the supervision of authorized personnel at all times while in those area. Information Technology contractors or vendors will be physically or virtually escorted by authorized personnel anytime said individual have access to facilities, areas, rooms, or an agency’s CHRI information system.

2. Subsequent Arrest/Conviction – If an individual granted access to CJI 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. Except that,
as noted in E(1)(a), individuals with a felony conviction of any kind will have their access indefinitely suspended.

3. **Public Interest Denial** – If the LASO determines that access to CJI 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.

4. **Approval for Access** – All requests for access to CJI shall be as specified and approved by the LASO. Any such designee must be an 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 Michigan State Police upon request.

5. **Termination of Employment/Access** – The LASO or authorized designee shall terminate access to CHRI immediately, which is within 24 hours of a notification that an individual’s termination of employment has occurred.

The specific steps of how personnel termination will be addressed:
- a. Once a resignation, retirement or termination is submitted to Human Resources, the LASO will be notified immediately.
- b. Upon termination individuals with access to physical CHRI media will return all file keys and name badges that provide building access.
- c. Upon termination, all accounts including email and network accounts are disabled. The CHRISS account will be inactivated for the individual. If needed, a new LASO administrator or CHIRSS administrator will be assigned.

6. **Transfer/Re-assignment** – Individuals with access to CHRI, and where the individual has been reassigned or transferred, shall have his or her access reviewed by the LASO or authorized designee to ensure access is still appropriate. If access is determined to be suspended, the individual shall be restricted from access to CHRI within the immediate 24 hours of transfer or reassignment and the following steps shall be taken by Ingham ISD immediately:

The specific steps of how personnel transfer will be addressed:
- a. The LASO will review access to CHRI.
- b. All personnel changes are processed through Human Resources. Once Human Resources is notified of a change, the review will be initiated.
- c. If it is determined the employee no longer requires access to physical CHRI media to perform his or her daily job responsibilities will return all file keys. If the individual changes buildings, their building access shall be changed by the Facilities department.
d. If it is determined the employee no longer requires access to digital CHRI media to perform their daily job responsibilities, the access to the files will be disabled. The CHRISS account will be inactivated for the individual. If needed, a new LASO administrator or CHIRSS administrator will be assigned.

7. Sanctions - Persons found noncompliant with state or federal laws, current FBI CJIS Security Policy, rules or regulations, including Ingham ISD’s Information Security Policy, will be formally disciplined. Discipline can be, but not limited to, counseling, the reassignment of CHRI responsibilities, dismissal, or prosecution. Discipline will be based on the severity of the infraction and at the discretion of Ingham ISD.

F. Controlled Area

All CHRI obtained from the MSP pursuant to the statutorily required background checks shall be maintained in a controlled area, which shall be designated office, room, area or lockable storage container. The following security precautions will apply to the controlled area.

1. Limited unauthorized personnel access to the area during times that CJI is being processed or viewed.

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

3. 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.

4. Encryption shall be used for electronic storage of CJI.

G. Secondary Dissemination of Information

If CHRI received from the MSP is released to another authorized agency under the sharing provision designated by state statute, a log of such releases shall be maintained and kept current.

H. Incident Response

Ingham ISD 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 agency will identify responsibilities for information security incidents and include how and who to report such incidents to. The agency will ensure appropriate security incident capabilities exist, and should incorporate the lessons learned from ongoing incident handling activities. The agency 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 is to be included within the agency’s Security Awareness Training. (See section on Security Awareness Training at the end of this document.) Procedures shall be in place to track and document information security incidents, whether physical or digital, on an ongoing basis. When an incident has been determined a breach involving CHRI, the agency will report the security breach to the MSP ISO by use of the “Information Security Officer (ISO) Computer Security Incident Response Capability Reporting” form (CJIS-016).

The specific steps of how incident response will occur:

a. The Assistant Superintendent for Human Resources and Organizational Development who also services as the LASO shall be notified of any incident.

b. Handling Capabilities implemented by the agency:

<table>
<thead>
<tr>
<th>Capabilities shall be handled according to the following description:</th>
<th>Physical – Hard Copy CHRI</th>
<th>Digital – Digitally Accessed/Saved CHRI</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Preparation</td>
<td>The CHRI container will be locked at all times in the human resources office which will be locked when office staff is not present.</td>
<td>Firewalls, virus protection, and malware/spyware protection will be maintained.</td>
</tr>
<tr>
<td>2. Detection</td>
<td>Physical intrusions to the building will be monitored by means of a building alarm system in conjunction with Safety Systems. All doors must be locked at night before the building alarm is set.</td>
<td>Electronic intrusions will be monitored by the virus and malware/spyware detection.</td>
</tr>
<tr>
<td>3. Analysis</td>
<td>The LASO will work with police authorities to determine how the incident occurred and what data were affected.</td>
<td>IT department will determine what systems or data were compromised and affected.</td>
</tr>
<tr>
<td>4. Containment</td>
<td>The LASO will lock uncompromised CHRI in a secure container or transport CHRI to secure area.</td>
<td>The IT department will stop the spread of any intrusion and prevent further damage.</td>
</tr>
<tr>
<td>5. Eradication</td>
<td>The LASO will work with law enforcement of the Mason Police Department or Ingham County Sherriff’s Office to remove any threats that compromise CHRI data.</td>
<td>The IT department will remove the intrusion before restoring the system. All steps necessary to prevent recurrence will be taken before restoring the system.</td>
</tr>
<tr>
<td>6. Recovery</td>
<td>The law enforcement agency of the Mason Police Department or Ingham County Sherriff’s Office in charge will handle and oversee recovery of stolen CHRI media. The LASO may contact MSP for assistant in re-fingerprinting if necessary.</td>
<td>The IT department will restore the agency information system and media to a safe environment.</td>
</tr>
</tbody>
</table>
c. We will collect evidence and share with the Mason Police Department or Ingham County Sheriff’s Office. If needed, we would work with the Clark-Hill Law Firm for legal counsel.

d. The Information Security Officer (ISO) Computer Security Incident Response Capability Reporting,” form (CJIS-016) will used for reporting security incidents to the MSP

e. We will retain the CJIS-016 is to track and document information security incidents.

LEGAL CITATION: MCLA 380.1535, 380.1230, 38.101, 38.103

ADMINISTRATIVE REGULATION

Amended: March 10, 2014
January 26, 2017
August 15, 2017
February 20, 2018
January 25, 2019