## Series 4000: District Employment

### 4200 Employee Conduct and Ethics

### *4205-AG-1 Criminal Justice Information Security (Non-Criminal Justice Agency)*

The District will conduct background checks, consistent with Policy 4205(C) and Administrative Guidance 4205-AG, and will have the Michigan State Police ("MSP") obtain criminal history record information ("CHRI") from both the state and Federal Bureau of Investigation ("FBI") for all District employees, contractors, volunteers, and vendors and their employees who regularly and continuously work under contract as provided in Policy 4205(C)(2). Employees who fail to follow these procedures will be subject to discipline subject to the Superintendent's review and written approval of any corrective action.

A. Local Agency Security Officer ("LASO")

   The District will appoint the Director of Human Resources as its LASO who is responsible for the adoption of this guidance along with data/system security.

   1. The LASO is responsible for ensuring:

      a. compliance with these regulations and laws;

      b. personnel security screening procedures are followed under this administrative guideline;

      c. approved and appropriate security measures are in place and functioning properly to protect CHRI;

      d. only approved District employees have access to and are using the information in compliance with the law;

      e. compliance with this administrative guideline; and

      f. that the MSP is promptly informed of any security breach(es).

   2. The LASO is also responsible for identifying and documenting, to the extent applicable:

      a. how District equipment is connected to the MSP; and

      b. who is using the MSP-approved equipment.

   3. When a new LASO is established, the District will complete and deliver a LASO appointment form to the MSP and will keep a copy of the appointment form on file indefinitely. The LASO will make all MSP fingerprint account changes.

B. Personnel (Authorized User) Security

Only authorized users will have access to CHRI. An authorized user must be vetted through the national fingerprint background check and be given CHRI access by the LASO to evaluate potential employees, contractors, or volunteers for employment or assignment. If the District maintains digital CHRI, the LASO will assign authorized users unique passwords compliant to 4205-AG-1 (C)(3) to access it. Those who are not authorized users but who, by the function of their job, will be close to CHRI or computer systems with access to CHRI will be supervised by an authorized user. Employees who do not comply with state or federal laws or District policies or administrative guidelines will be subject to discipline, up to discharge.

1. Security with Separated Authorized Users

   After an authorized user is separated from the District, that individual's access to CHRI will be terminated within twenty-four (24) hours. This includes, but is not limited to, returning keys, access cards, and ceasing access to digital CHRI.

2. Security with Transferred Authorized Users

   When an authorized user is transferred or reassigned, the LASO will take steps necessary to block that individual's access to CHRI within twenty-four (24) hours, unless the LASO determines that the individual must retain access.

C. Media Protection

Authorized users may only access CHRI on authorized devices, which does not include a personally owned mobile device, cell phone, computer, or other technology, unless the personally owned devices are approved, consistent with specific terms and conditions, for access. All CHRI (including digital media) will be maintained in a physically secure location or controlled area. A physically secure location or controlled area will be (1) locked whenever an authorized user is not present or supervising and (2) limit access to unauthorized users. An authorized user accessing CHRI must position the media to prevent unauthorized users from accessing or viewing CHRI. Physical CHRI will be stored in a locked filing cabinet, safe, or vault. Digital CHRI will be encrypted consistent with FBI CJIS Security Policy. If digital CHRI is stored on a storage device without encryption, it must be stored like physical CHRI.

1. Media Transport

   The LASO must approve all CHRI media transportation and will not grant approval unless transportation is reasonably justified. CHRI must be secured during transport. Physical CHRI must be transported in a sealed, locked, or secured medium and digital CHRI must be encrypted, and if not, secured in the same fashion as physical CHRI.

2. Media Disposal/Sanitization

CHRI media will be stored and retained for the duration required by law. Disposal must be made with the written approval of the LASO and the Superintendent. Only authorized users may dispose of CHRI media. Physical media will be cross-cut shredded or incinerated. Digital media must either be overwritten at least three (3) times or degaussed, passing a strong magnet over the media, before disposal or reuse. The LASO will keep written records (date and authorized user's signature) of CHRI media destroyed and the process for destroying or sanitizing CHRI media for ten (10) years.

3. Passwords

When the LASO assigns a unique password to an authorized user, it must have the following attributes:

a. at least eight (8) characters;

b. not consisting of only a proper noun or word found in a dictionary;

c. not similar or identical to the username;

d. not be displayed while entered or transmitted outside of the physically secure location or controlled area;

e. expires every ninety (90) days; and

f. cannot be the same as the previous ten (10) passwords.

4. Security Awareness Training

The District will provide all authorized users with security awareness training, following the template provided on the MSP website, within six (6) months of authorization and every two (2) years thereafter. The LASO will keep a current record of all users who have completed the training.

5. CHRI Dissemination

The District must maintain a record of any CHRI dissemination to another authorized agency, consistent with the Revised School Code, which must include (1) date of release, (2) records released, (3) means of sharing, (4) District personnel who disseminated the CHRI, (5) whether authorization to disseminate was obtained, and (6) the agency to whom the CHRI was disseminated and the recipient's name.

D. Incident Handling

1. In General

The District has established operational incident handling procedures for instances of an information security breach. CHRI security breach incidents will be tracked using the report the MSP provides on its website https://www.michigan.gov/msp/0,4643,7-123-72297_24055-332662--,00.html.

The District has provided specific handling capabilities for CHRI, consistent with the following table:

| **Capabilities shall be handled according to the following description:** | **Physical – Hard Copy CHRI** | **Digital – Digitally Accessed/Saved CHRI** |
|---|---|---|
| Preparation | The CHRI container will be locked at all times in the office in which it is stored. When office staff is not present, the office must be locked | Firewalls, anti-virus protection, and anti-malware/spyware protection will be maintained. |
| Detection | Physical intrusions to the building will be monitored. A building alarm or video surveillance will monitor for physical or unauthorized intrusions. The building must be locked at night. | Electronic intrusions will be monitored by the virus and malware/spyware detection. |
| Analysis | The LASO will work with police authorities to determine how the incident occurred and what data was affected. | The IT department will determine what systems or data were affected and compromised. |
| Containment | The LASO will lock uncompromised CHRI in a secure container or transport CHRI to a secure area. | The IT department will stop the spread of any intrusion and prevent further damage. |
| Eradication | The LASO will work with local law enforcement to remove any threats that compromise CHRI data. | The IT department will remove the intrusion before restoring the system. All steps necessary to prevent recurrence will be taken before restoring the system |
| Recovery | Local law enforcement will handle and oversee the recovery of stolen CHRI media. The LASO may contact MSP for assistance in re-fingerprinting, if necessary. | The IT department will restore the agency information system and media to a safe environment. |

When a CHRI security breach incident occurs, the following will apply:

a. the LASO will be notified immediately;

b. the LASO or appointed authorized user will stop any unauthorized access, secure the media, and shut down the systems necessary to avoid further unauthorized exposure;

c. the LASO or appointed authorized used will record all necessary information regarding the breach, the District's response to the breach, and who was involved in taking response measures;

d. the LASO will file the incident report with the MSP; and

e. when such incident results in legal action (either civil or criminal) against a person or the District, evidence shall be collected, retained, and presented according to the evidentiary rules of the appropriate jurisdiction(s).

2. Mobile Device Incident Handling

The District will, in addition to the handling procedure in the table above, establish and implement additional procedures for mobile devices to reduce the risk of unauthorized access to CHRI.

When a device is lost, the District will document and indicate how long the device has been lost. For a lost device, the District will report if the owner believed the device was locked, unlocked, or could not verify the device's locked state. For a total loss of a device (unrecoverable), the District will report if CHRI was stored on the device, whether it was locked or unlocked, and whether the District can track or wipe the device remotely. The District will report any compromise of a device while still in the owner's possession and any compromise outside of the United States.

Adoption date: September 13, 2021

Revised date: February 14, 2022