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 Guideline 4205-AG-1, 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, 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.

The District will provide employees, contractors, volunteers, and vendors and their employees for whom the District conducts background checks the most current version of the MSP RI-030 Live Scan consent form.

The District will complete and maintain a Noncriminal Justice Agency User Agreement (RI-087) provided by the Michigan State Police.

A. Local Agency Security Officer ("LASO")

The District Superintendent will appoint the Director of Business & Support Services a District employee, who: (1) is an authorized user, (2) has completed a fingerprint-based background check as required, (3) has been found appropriate to have access to CHRI, and (4) is directly involved in evaluating an individual's qualifications for employment or assignment as its LASO, who is responsible for the adoption of this guidance along with data/system security. When changes in the appointed LASO/CHRISS Administrator occur, the District will complete and return a new appointment notification form (CJIS-015) to MSP-CJIC-ATS@michigan.gov.

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. annual Awareness Training is being completed by all personnel authorized to access CHRI;

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

    f. compliance with this administrative guideline;

g. that the MSP Information Security Officer (ISO) is promptly informed of any security incidents by submitted the MSP CJIS-016 Information Security Officer (ISO) Security Incident Report;

h. information security policy/procedures are reviewed and updated at least annually and after any security events involving CHRI; and

i. the District [Note: Select one or more. Delete this note and retain at least one listed item: (1) displays posters, (2) offers supplies inscribed with security and privacy reminders, (3) displays logon screen messages, (4) generates email advisories or notices from District officials, or (5) conducts awareness events]to increase security and privacy awareness of system users.

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

a. District equipment connected to the MSP system; and

b. who is using or accessing CHRI and/or systems with access to CHRI.

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 24 hours. This includes, but is not limited to, returning keys, access cards, and ceasing access to digital CHRI.

a. The Human Resources director or designee must notify the LASO of the effective termination date of a user's employment by written email communication no later than 24 hours after the termination date.

b. The Human Resources director or designee will require the return of any keys, access cards, files, and other related items.

c. The LASO must ensure that access to the District's digital CHRI records system is disabled and the user's CHRISS account is deactivated.

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 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, 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 (1) be 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.

CJI and information system hardware, software and media are located and processed in [add: location and description].

1. Media Transport

The LASO must approve all CHRI media transportation and will not grant approval unless transportation is reasonably justified. The LASO or LASO's designee will transport CHRI, which must be secured during transport. Physical CHRI must remain in the physical presence of authorized personnel until it is delivered. 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 and Incident Response Training and Testing

a. The District will provide all authorized users role-based security and privacy and incident response training consistent with the following roles, as applicable:

Basic Role: users with unescorted access to a physically secure location;

General Role: users with physical and logical access to CJI;

Privileged Role: information technology personnel including system administrators, security administrators, network administrators and other similar roles;

Security Role: users responsible for ensuring confidentiality, integrity, and availability of CJI and compliant implementation of technology with the Criminal Justice Information Services (CJIS) Security Policy (CJISSECPOL).

b. The District will provide users with security awareness training about the user's responsibilities and expected behavior when accessing CJI and the systems which process CJI, and on handling information security incidents as follows:

i. for new users, prior to accessing CJI; and

ii. for all users annually about the user's responsibilities and expected behavior when accessing CJI and the systems which process CJI, and on handling information security incidents;

iii. when required due to system changes; and

iv. within 30 days of any security event for individuals involved in the event.

c. The LASO will keep a current record of all users who have completed training.

5. CHRI Dissemination

The District must maintain a record of any CHRI dissemination to another authorized agency for all dissemination outside the CHRISS system, 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 (7) the recipient's name.

D. Incident Handling, Monitoring, and Reporting

1. In General

The District has established operational incident handling procedures for instances of an information security breach. The LASO will track CHRI security breach incidents and will report such incidents to the superintendent and MSP ISO using the MSP CJIS-016 reporting from. The District has provided specific incident 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 [add company name of building alarm] 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 [name police department] 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 [name police department] 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.

2. CHRI Security Breach Incident

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

a. Notice: Personnel will notify the LASO immediately or no later than one hour after the incident was discovered.

b. Secure Systems: 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. Assessment: The LASO will determine whether notification to individuals is needed, assess the extent of harm, and identify any applicable privacy requirements.

d. Automated Reporting. Using automated mechanisms, such as email, website postings with automatic updates, and automated incident response tools, the LASO will report confirmed incidents to the CJIS Systems Officer (CSO), State Identification Bureaus Chief (SIB Chief), or Interface Agency Official.

e. Supply Chain Coordination. The LASO will provide incident information to product or service providers or organizations involved in the supply chain or supply chain governance for systems or system components related to the incident.

f. Records: The LASO or appointed authorized user will record all necessary information regarding the breach, the District's response to the breach, and who was involved in taking response measures.

g. Coordination of Incident Handling and Contingency Planning: The LASO will coordinate incident handling activities with contingency planning activities and incorporate lessons learned from ongoing incident handing activities into incident response procedures, training, and testing implementing the resulting changes.

h. Predictability: The LASO will ensure the rigor, intensity, scope, and results of incident handling activities are comparable and predictable across the organization.

i. Review of Policy/Procedures: The LASO will review and update information security policy/procedures at least annually and after security incidents involving CHRI.

j. Legal Action: When such incident results in legal action (either civil or criminal) against a person or the District, the local law enforcement agency shall be contacted to collect, retain, and present evidence, according to the evidentiary rules of the appropriate jurisdiction(s).

E. Incident Response Support and Plan

1. Response Support Resource: The District will provide a response support resource that offers advice and assistance to system users for handling and reporting incidents.

2. Automation Support: The District will use automated mechanisms, such as access to a website or to an incident response vendor, to increase availability of incident response information and support.

3. Incident Response Plan: The District will develop an incident response plan that:

   a. provides a roadmap for implementing incident response capability;

   b. describes the structure and organization of incident response capability;

   c. provides high-level approach for how incident response capability fits into overall organization;

   d. meets unique requirements of the District related to mission, size, structure and functions;

   e. defines reportable incidents;

   f. provides metrics for measuring District incident response capability;

   g. defines resources and management support needed to effectively maintain and mature an incident response capability;

   h. addresses sharing of incident information;

i. is reviewed and approved by the superintendent annually; and

j. explicitly designates responsibility for incident response to District personnel with incident reporting responsibilities and CSO or CJIS WAN Official.

4. Incident Response Plan Management: The District will:

a. distribute the incident response plan to personnel with incident handling responsibilities;

b. update the incident response plan to address system and organizational changes or problems during plan implementation, execution or testing;

c. communicate incident response plan changes to District personnel with incident handing responsibilities; and

d. protect the incident response plan from unauthorized disclosure and modification.

5. Incident Response Plan Breaches: The District will include in the incident response plan for breaches involving personally identifiable information:

a. process to determine if notice to individuals or organization is needed;

b. assessment process to determine extent of harm, embarrassment, inconvenience, or unfairness to affected individuals and any mechanism to mitigate such harms; and

c. identification of applicable privacy requirements.

F. Audit and Accountability

1. The District develops, documents, and disseminates to organizational personnel with audit and accountability responsibilities:

b. agency and system-level audit and accountability policy

1. addresses purpose, scope, roles, responsibilities, management commitment, coordination among organization entities, and compliance; and

2. is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines

c. procedures to facilitate the implementation of the audit and accountability policy and the associated audit and accountability controls.

2. The District reviews and updates the current audit and accountability policy and procedures annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI.

3. The District identifies the types of events that the system is capable logging in support of the audit function and coordinates the event logging function with other organizational entities requiring audit-related information to guide and inform the selection criteria for events to be logged.

4. The District specifies certain event types for logging within the system, provides rationale for the adequacy of the event types selected for logging, and annually reviews and updates the selected event types.

5. The District ensures that audit records contain information that establishes the following:

    a. What type of event occurred;

    b. When the event occurred;

    c. Where the event occurred;

    d. Source of the event;

    e. Outcome of the event; and

    f. Identity of any individuals, subjects, or objects/entities associated with the event.

6. The District generates audit records containing the following information:

    a. Session, connection, transaction, and activity duration;

    b. Source and destination addresses;

    c. Object or filename involved; and

    d. Number of bytes received and bytes sent (for client-server transactions) in the audit records for audit events identified by type, location, or subject.

7. The District limits personally identifiable information contained in audit records to the minimum PII necessary to achieve the purpose for which it is collected.

8. The District allocates audit log storage capacity to accommodate the collection of audit logs to meet retention requirements.

9. The District alerts organizational personnel with audit and accountability responsibilities and system/network administrators within one (1) hour in the event of an audit logging process failure and restarts all audit logging processes and verifies that systems are logging properly.

10. The District reviews and analyzes system audit records weekly and reports findings of potential or actual inappropriate or unusual activity to those with the relevant responsibilities.

11. The District adjusts the level of audit record review, analysis, and reporting within the system based on changes in input from law enforcement or intelligence agencies.

12. The District integrates audit record review, analysis, and reporting processes using automated mechanisms.

13. The District analyzes and correlates audit records across different repositories to gain organization-wide situational awareness.

14. The District provides and implements an audit record reduction and report generation capability that both supports on-demand audit record review, analysis, and reporting requirements and after-the-fact investigations or incidents; and does not alter the original content or time ordering of audit records.

G. Access Control Policy

1. The District will develop, document, and disseminate to personnel with access control responsibilities:

   a. Agency-level access control policy that:

      1. addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance;

      2. is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

   b. Procedures to facilitate implementation of the policy and the associated access controls.

2. The LASO will:

   a. manage the development, documentation, and dissemination of the access control policy and procedures; and

   b. review and update the access control policy annually and following any security breaches;

H. Account Management

1. The District will:

   a. define and document the types of accounts allowed and specifically prohibited for use within the system;

   b. prohibit use of personally-owned information systems, including mobile devices (i.e., bring your own device [BYOD]), and publicly accessible systems for accessing, processing, storing, or transmitting CJI;

c. assign account managers;

d. require conditions for group and role membership;

e. specify authorized users of the system, group and role membership, and access authorizations (i.e., privileges) and attributes listed for each account;

f. at least annually, review accounts for compliance with account management requirements;

g. establish and implement process for changing shared or group account authenticators (if deployed) when individuals are removed from the group; and

h. align account management processes with personnel termination and transfer processes.

I. Access Enforcement

1. The District will:

a. enforce approved authorization for logical access to information and system resources will be enforced in accordance with applicable access control policies; and

b. provide automated or manual processes to enable individuals to access elements of their personally identifiable information.

J. Information Flow Enforcement

1. The District will enforce approved authorizations for controlling the flow of information within the system and between connected systems by preventing CJI from being transmitted unencrypted across the public network, blocking outside traffic that claims to be from within the District, and not passing any web requests to the public network that are not from the District-controlled or internal boundary protection devices.

K. Separation of Duties

1. The District will:

a. identify and document separation of duties based on specific duties, operations, or information systems, as necessary to mitigate risk to CJI; and

b. define system access authorizations to support separation of duties.

L. Least Privilege

1. The District will allow only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks.

2. The District will:

    a. authorize access for personnel including security administrators, system and network administrators, and other privileged users with access to system control, monitoring, or administration functions (e.g., system administrators, information security personnel, maintainers, system programmers, etc.) to:

        1. established system accounts, configured access authorizations, set events to be audited, set intrusion detection parameters, and other security functions; and

        2. security-relevant information in hardware, software, and firmware.

    b. require users of system accounts (or roles) with access to privileged security functions or security-relevant information (e.g., audit logs), use non-privileged accounts or roles, when accessing non-security functions;

    c. restrict privileged accounts on the system to privileged users;

    d. review annually the privileges assigned to non-privileged and privileged users to validate the need for such privileges;

    e. reassign or remove privileges, if necessary, to correctly reflect organizational mission and business needs; and

    f. log the execution of privileged functions.

M. Unsuccessful Logon Attempts

1. The District will enforce a limit of five (5) consecutive invalid logon attempts by a user during a 15-minutes time period, and automatically lock the account or node until released by an administrator when the maximum number of unsuccessful attempts is exceeded.

N. System Use Notification (required when access via logon interfaces with human users)

1. A system use notification message will be displayed to users before granting access to the system that provides privacy and security notices consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines stating that:

    a. users are accessing a restricted information system;

    b. system usage may be monitored, recorded, and subject to audit;

    c. unauthorized use of the system is prohibited and subject to criminal and civil penalties; and

    d. use of the system indicates consent to monitoring and recording.

2. The notification message or banner will be retained on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access to the system; and

3. For publicly accessible systems, before the District grants further access to publicly accessible systems:

    a. system use information consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines will be displayed;

    b. references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities will be displayed; and.

    c. a description of the authorized users of the system will be included.

O. Device Lock and Session Termination:

1. The device lock will conceal information previously visible on the display with a publicly viewable image.

2. Further access to the system will be prevented by initiating a device lock after a maximum of 30 minutes of inactivity.

3. Users must log out when a work period has been completed.

4. Users must initiate a device lock before leaving the system unattended.

5. The device lock will be retained until the user reestablishes access using established identification and authentication procedures.

P. Remote Access.

1. The District establishes and documents usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed.

2. The District authorizes each type of remote access to the system prior to allowing such connections.

3. The District employs automated mechanisms to monitor and control remote access methods.

4. The District implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.

5. The District routes remote access through authorized and managed network access control points.

6. The District authorizes the execution of privileged commands and access to security-relevant information via remote access only in a format that provides assessable evidence and for compelling operational needs.

7. The District documents the rational for remote access in the security plan for the system.

Q. Wireless Access. The District:

1. establishes configuration requirements, connection requirements, and implementation guidance for each type of wireless access;

2. authorizes each type of wireless access to the system prior to allowing such connections;

3. protects wireless access to the system using authentication of authorized users and agency-controlled devices, and encryption; and

4. disables wireless networking capabilities embedded within system components prior to issuance and deployment when not intended for use.

R. Access Control for Mobile Devices. The District:

1. establishes configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices, to include when such devices are outside of controlled areas;

2. authorizes the connection of mobile devices to organizational systems; and

3. employs full-device encryption to protect the confidentiality and integrity of information on full-and limited-feature operating system mobile devices authorized to process, store, or transmit CJI.

S. Use of External Systems.

1. The District permits authorized individuals to use an external system to access the system or to process, store, or transmit organization-controlled information only after:

   a. verification of implementation of controls on external system as specified in the District's security and privacy policies and security and privacy plans; or

   b. retention of approved system connection or processing agreements with the organizational entity hosting the external system.

2. The District restricts the use of District-controlled portable storage devices in external systems including how the devices may be used and under what conditions the devices may be used.

T. Information Sharing. The District:

1. enables authorized users to determine whether access authorizations assigned to a sharing partner match the information's access and use restrictions as defined in an executed information exchange agreement; and

2. employs attribute-based access control or manual processes as defined in information exchange agreements to assist users in making information sharing and collaboration decisions.

U. Identification and Authentication (IA) (CJISSECPOL 5.6)

V. Physical and Environmental Protection (CJISSECPOL 5.9)

W. Systems and Communications Protection (CJISSECPOL 5.10)

X. System and Services Acquisition (CJISSECPOL 5.14)

Y. System and Information Integrity (CJISSECPOL 5.15)

Z. Maintenance (CJISSECPOL 5.16)

AA. Planning (CJISSECPOL 5.17)

BB. Contingency Planning (CJISSECPOL 5.18)

CC. Risk Assessment (CJISSECPOL 5.19)

Date adopted:

Date revised: