NEW POLICY - VOL. 27, NO. 1

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 those contractors who work on a regular and continuous basis in the District. To assure the security, confidentiality, and integrity of the CHRI background check information received from the MSP/FBI the following standards are established.

Sanctions for Non-Compliance

Employees who fail to comply with this policy and any guidelines issued to implement this policy will be subject to discipline for such violations. Discipline will range from counseling and retraining to discharge, based on the nature and severity of the violation. All violations will be recorded in writing, with the corrective action taken. The Superintendent shall review, approve, sign and date all such corrective actions.

Local Agency Security Officer (LAS0)

~~The~~ **[Christine Veld** ~~_____~~ **insert designated administrator]** shall be designated as the District's Security Officer and shall be responsible for overall implementation of this policy and for data and system security. This shall include:

A. ensuring that personnel security screening procedures are being followed as set forth in this policy;

B. ensuring that approved and appropriate security measures are in place and working as expected;

C. supporting policy compliance and institute the CSA incident response reporting procedures;

D. ensure the CSA ISO is promptly informed of any security incidents involving the abuse or breach of the system and/or access to criminal justice information;

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

F. to the extent applicable, identify 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 designated on the appropriate form as prescribed and maintained by the Michigan State Police.

Agency User Agreements

The District shall enter into any User Agreement required, and future amendments, by the Michigan State Police 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 User Agreement.

Personnel Security

All individuals that have access to any criminal justice information shall be subject to the following standards.

A. Background Checks - A Michigan (or state of residency if other than Michigan) and a national fingerprint-based criminal history record check shall be conducted within thirty (30) days of assignment to a position with direct access to criminal justice information or with direct responsibility to configure and maintain computer systems and networks with direct access to criminal justice information.

1. A felony conviction of any kind will disqualify an individual for access to criminal justice information.

2. 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.

3. Support personnel, contractors and custodial workers with access to physically secure locations or controlled areas (during criminal justice information processing) are subject to the same clearance standards as other individuals with access, unless they are escorted by authorized personnel at all times when in these locations or areas.

B. 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.

C. 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.

D. 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 an employee of the District.

E. Termination of Employment/Access - Upon termination of employment, all access to criminal justice information shall be terminated for that individual, and steps taken to assure security of such information and any systems at the District to access such information.

F. 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 determine whether continued access is necessary and appropriate. If not, s/he shall take such steps as necessary to block further access to such information.

Media Protection

Access to electronic 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.

A. Media Storage and Access – All electronic and physical media shall be stored in a physically secure location or controlled area, such as 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 electronic CHRI background data shall be encrypted.

B. Media Transport –Electronic and physical media shall be protected when being transported outside of a controlled area. Only authorized individuals shall transport the media. It 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. To the extent possible, electronic 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.

C. 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 for a period of at least five (5) years. **[Note: the regulations do not specify a specific period for maintaining this information. This time period is suggested as it will likely cover most all statutes of limitation and can be retained in electronic format.]**

1. Electronic 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. 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.

2. 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 waste basket 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.)

Controlled Area

All CHRI obtained from the Michigan State Police pursuant to the statutorily required background checks shall be maintained in a controlled area, which shall be a designated office, room, area or lockable storage container. 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 electronic storage of criminal justice information. (See AG 8321.)

Passwords (Standard Authentication)

All authorized individuals with access to computer 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.)

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 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 Michigan State Police or a program approved by the Michigan State Police. At a minimum, the training shall comply with the standards established by U.S. Department of Justice and Federal Bureau of Investigation for Criminal Justice Information Services. (See AG 8321.)

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 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. whether an 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.

Audit Retention

The District shall retain audit records (Position description, consent, and CHRI for both applicants that are hired and those that are not) for at least 365 days. Audit records must continue to be maintained until it is determined they are no longer needed for administrative, legal, audit, or other operational purposes. This includes, for example, retention and availability of audit records subject to Freedom of Information Act (FOIA) requests, subpoena, litigation hold and law enforcement actions.

Ref: Criminal Justice Information Services - Security Policy (Version 5.0, 2011), 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

3/11/13

© **NEOLA 2012**