THOMAS MACLAREN SCHOOL

Policy SY22-23.1: Criminal History Record Information (CHRI) Proper Access, Use and Dissemination Procedure

Revised: October 27, 2022

Purpose:

The intent of the following policy is to ensure the protection of the Criminal Justice Information (CJI) and its subset of Criminal History Record Information (CHRI) until such time as the information is purged or destroyed in accordance with applicable record retention rules.

The following policy was developed using the FBI's Criminal Justice Information Services (CJIS) Security Policy.

Scope:

The scope of this policy applies to any electronic or physical media containing FBI CJI while being stored, accessed, or physically moved from a secure location from the **Secure Documents Room**. In addition, this policy applies to any authorized person who accesses, stores, and/or transports electronic or physical media.

Criminal Justice Information (CJI) and Criminal History Record Information (CHRI)

CJI is the term used to refer to all of the FBI CJIS provided data necessary for law enforcement and civil agencies to perform their missions including, but not limited to, biometric, identity history, biographic, property, and case/incident history data.

CHRI, is a subset of CJI and for the purposes of this document is considered interchangeable. Due to its comparatively sensitive nature, additional controls are required for the access, use, and dissemination of CHRI. In addition to the dissemination restrictions outlined below, Title 28, Part 20, Code of Federal Regulations (CFR), defines CHRI and provides the regulatory guidance for dissemination of CHRI.

Proper Access, Use, and Dissemination of CHRI

Information obtained from the Interstate Identification Index (III) is considered CHRI. Rules governing the access, use, and dissemination of CHRI are found in Title 28, Part 20, CFR. The III shall be accessed only for an authorized purpose. Further, CHRI shall only be used for an authorized purpose consistent with the purpose for which III was accessed. Dissemination to another agency is authorized if (a) the other agency is an Authorized Recipient of such information and is being serviced by the accessing agency, or (b) the other agency is performing noncriminal justice administrative functions on behalf of the authorized recipient and the outsourcing of said functions has been approved by appropriate CJIS Systems Agency (CSA) or State Identification Bureau (SIB) officials with applicable agreements in place.

Personnel Security Screening

Access to CJI and/or CHRI is restricted to authorized personnel. Authorized personnel is defined as an individual or group of individuals who have been appropriately vetted and have been granted access to

CJI data. In the case of Thomas MacLaren School, **authorized personnel** is defined as an individuals in the Personnel Department; these staff are the sole persons to have access to CJI data.

Security Awareness Training

Basic security awareness training shall be required within six months of initial assignment, and biennially thereafter, for all personnel who have access to CJI. This training will be completed through CBI who offers a free solution for compliant Security Awareness Training. To take advantage of this training an email should be sent to cdps.cbi.audit@state.co.us.

Physical Security

A physically secure location is a facility or an area, a room, or a group of rooms within a facility with both the physical and personnel security controls sufficient to protect the FBI CJI and associated information systems. The perimeter of the physically secure location shall be prominently posted and separated from non-secure locations by physical controls. Only authorized personnel will have access to physically secure non-public locations. Thomas MacLaren School's **Secure Documents Room** is locked and all physical data is stored in a locked filing cabinet for which on authorized personnel (the school administrator) has access. Electronic data is stored on the computer of only authorized personnel (the school administrator) which is password protected. The school administrator will take necessary steps to prevent and protect the agency from physical, logical and electronic breaches.

Media Protection

Controls shall be in place to protect electronic and physical media containing CJI while at rest, stored, or actively being accessed. "Electronic media" includes memory devices in laptops and computers (hard drives) and any removable, transportable digital memory media, such as magnetic tape or disk, backup medium, optical disk, flash drives, external hard drives, or digital memory card. "Physical media" includes printed documents and imagery that contain CJI. The agency shall securely store electronic and physical media within physically secure locations or controlled areas. The agency shall restrict access to electronic and physical media to authorized individuals. If physical and personnel restrictions are not feasible then the data shall be encrypted per Section 5.10.1.2.

Media Transport

Controls shall be in place to protect electronic and physical media containing CJI while in transport (physically moved from one location to another) to prevent inadvertent or inappropriate disclosure and use. The agency shall protect and control electronic and physical media during transport outside of controlled areas and restrict the activities associated with transport of such media to authorized personnel.

Media Sanitization and Disposal

When no longer usable, hard drives, diskettes, tape cartridges, CDs, ribbons, hard copies, print-outs, and other similar items used to process, store and/or transmit FBI CJI shall be destroyed within 60 days of the record being reviewed in accordance with measures established by the **Administrative Office**.

Physical media (print-outs and other physical media) shall be disposed of by one of the following methods:

1) shredding using shredder in the **Administrative Office**

2) placed in locked shredding bins for a private contractor to come on-site and shred, witnessed by the school administrator throughout the entire process.

3) incineration witnessed by the Authorized Personnel onsite at agency or at contractor incineration site, if conducted by nonauthorized personnel.

Electronic media (hard-drives, tape cartridge, CDs, printer ribbons, flash drives, printer and copier Hard-drives, etc.) shall be disposed of by one of the methods:

1) **Overwriting (at least 3 times)** - an effective method of clearing data from magnetic media. As the name implies, overwriting uses a program to write (1s, 0s, or a combination of both) onto the location of the media where the file to be sanitized is located.

2) **Degaussing** - a method to magnetically erase data from magnetic media. Two types of degaussing exist: strong magnets and electric degausses. Note that common magnets (e.g., those used to hang a picture on a wall) are fairly weak and cannot effectively degauss magnetic media.

3) **Destruction** – a method of destroying magnetic media. As the name implies, destruction of magnetic media is to physically dismantle by methods of crushing, disassembling, etc., ensuring that the platters have been physically destroyed so that no data can be pulled.

IT systems that have been used to process, store, or transmit FBI CJI and/or sensitive and classified information shall not be released from the control of the **Administrative Office** until the equipment has been sanitized and all stored information has been cleared using one of the above methods.

Account Management

The agency shall manage information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The agency shall validate information system accounts at least annually and shall document the validation process. All accounts shall be reviewed at least annually by the designated CJIS point of contact (POC) or his/her designee to ensure that access and account privileges commensurate with job functions, need-to-know, and employment status on systems that contain Criminal Justice Information. The POC may also conduct periodic reviews.

Remote Access

The **Administrative Office** does not allow for remote access.

Personally Owned Information Systems

A personally owned information system shall not be authorized to access, process, store or transmit CJI unless the agency has established and documented the specific terms and conditions for personally owned information system usage. A personal device includes any portable technology like camera, USB flash drives, USB thumb drives, DVDs, CDs, air cards and mobile wireless devices such as Androids, Blackberry OS, Apple iOS, Windows Mobile, Symbian, tablets, laptops or any personal desktop computer. When bring your own devices (BYOD) are authorized, they shall be controlled using the requirements in Section 5.13 of the CJIS Security Policy.

Reporting Information Security Events

The agency shall promptly report incident information to appropriate authorities to include the state CSA or SIB's Information Security Officer (ISO). Information security events and weaknesses associated with information systems shall be communicated in a manner allowing timely corrective action to be taken.

Formal event reporting and escalation procedures shall be in place. Wherever feasible, the agency shall employ automated mechanisms to assist in the reporting of security incidents. All employees, contractors, and third-party users shall be made aware of the procedures for reporting the different types of event and weakness that might have an impact on the security of agency assets and are required to report any information security events and weaknesses as quickly as possible to the designated point of contact.

Policy Violation/Misuse Notification

Violation of any of the requirements contained in the CJIS Security Policy or Title 28, Part 20, CFR, by any authorized personnel will result in suitable disciplinary action, up to and including loss of access privileges, civil and criminal prosecution and/or termination.

Likewise, violation of any of the requirements contained in the CJIS Security Policy or Title 28, Part 20, CFR, by any visitor can result in similar disciplinary action against the sponsoring employee, and can also result in termination of services with any associated consulting organization or prosecution in the case of criminal activity.