A new policy to consider. This policy is based upon one originally developed by the Federal Bureau of Investigation (FBI) pertaining to this topic. This topic is also covered in policy 4112.5/4212.5 and its accompanying administrative regulation.

Personnel -- Certified/Non-Certified

Security Check/Fingerprinting

Criminal History Record Information (CHRI)

(Proper Access, Use and Dissemination Procedures)

Purpose

The Board of Education's (Board) intent of this policy is to ensure the protection of the Criminal Justice Information (CJI) and its subset of Criminal History Record Information (CHRI) until the information is purged or destroyed in accordance with applicable record retention rules.

This policy is based upon the FBI's Criminal Justice Information Services (CJIS) Security Policy. The Board considers the FBI CJIS Security Policy as the minimum standard. This Board policy may augment, or increase the standards, but shall not detract from the CJIS Security Policy standards.

Scope

This policy applies to any electronic or physical media containing FBI CJI while being stored, accessed or physically moved from a secure location within the District. 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 refers 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 policy 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.

Personnel -- Certified/Non-Certified

Security Check/Fingerprinting

Criminal History Record Information (CHRI)

Proper Access, Use, and Dissemination of CHRI (continued)

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, appropriately vetted through a national fingerprint-based record check and granted access to CJI data. Agencies, including school districts, located within states with legislation authorizing or requiring civil fingerprint-based background checks for personnel with access to CHRI for the purposes of licensing or employment shall submit a fingerprint-based record check within 30 days of employment or assignment on all personnel with those who have direct access to CJI, those who have direct responsibility to configure and maintain computer systems and networks with direct access to CJI, and any persons with access to physically secure locations or controlled areas containing CJI.

Security Awareness Training

Basic security awareness training is required, within six months of initial assignment, and biennially thereafter, for all personnel with access to CJI.

Physical Security

A "physically secure location" is a facility or an area, room, or group of rooms within a facility with sufficient physical and personnel security controls 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 shall access physically secure non-public locations. The District will maintain a current list of authorized personnel. All physical access points into the District's secure areas will be authorized before granting access. The District will implement access controls and monitor physically secure areas to protect all transmission and display mediums of CJI. Authorized personnel will take necessary steps to prevent and protect the District from physical, logical and electronic breaches.

Personnel -- Certified/Non-Certified

Security Check/Fingerprinting

Criminal History Record Information (CHRI) (continued)

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 District shall securely store electronic and physical media within physically secure locations or controlled areas. The District restricts 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 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 District 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 properly disposed of in accordance with measures established by the District.

One of the following methods shall dispose of physical media (printouts and other physical media):

1. Shredding using District issued shredders;
2. Placed in locked shredding bins for private contractor to come on-site and shred, witnessed by District personnel throughout the entire process;
3. Incineration using District incinerators or witnessed by District personnel onsite at District or at contractor incineration site, if conducted by non-authorized personnel.

Personnel -- Certified/Non-Certified

Security Check/Fingerprinting

Criminal History Record Information (CHRI)

Media Sanitization and Disposal (continued)

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 following District methods:

1. *Overwriting* (at least 3 times) – an effective method of clearing data from magnetic media. Overwriting uses a program to write (1's, 0's, 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. Common magnets are weak and shall not be used to degauss magnetic media.
3. *Destruction* – a method of destroying magnetic media. 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 District's control until the equipment has been sanitized and all stored information has been cleared using one of the above methods.

Account Management

The District shall manage information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The District 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 are 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 District shall authorize, monitor, and control all methods of remote access to the information systems that can access, process, transmit, and/or store FBI CJI. Remote access is any temporary access to the District's information system by a user (or an information system) communicating temporarily through an external, non-District controlled network (e.g., the Internet).

Personnel -- Certified/Non-Certified

Security Check/Fingerprinting

Criminal History Record Information (CHRI)

Remote Access (continued)

The District shall employ automated mechanisms to facilitate the monitoring and control of remote access methods. The District shall control all remote accesses through managed access control points. The District may permit remote access for privileged functions only for compelling operational needs, but shall document the rationale for such access in the security plan for the information system.

Utilizing publicly accessible computers to access, process, store or transmit CJI is prohibited. Publicly accessible computers include but are not limited to hotel business center computers, convention center computers, public library computers, public kiosk computers, etc.

Personally Owned Information Systems

A personally owned information system is not authorized to access, process, store or transmit CJI unless the District 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.

Reporting Information Security Events

The District 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 to allow for timely corrective action to be taken. Formal event reporting and escalation procedures shall be in place. Wherever feasible, the District 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 this 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.

Personnel -- Certified/Non-Certified

Security Check/Fingerprinting

Criminal History Record Information (CHRI)

Policy Violation/Misuse Notification (continued)

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 result in termination of services with any associated consulting organization or prosecution in the case of criminal activity.

(cf. 4112.5/4212.5 - Security Check/Fingerprinting)
(cf. 4112.51/4212.51 - Employment/Reference Checks)

Legal Reference: Connecticut General Statutes

10-221d Criminal history records checks of school personnel. Fingerprinting. Termination or dismissed. (as amended by PA 01-173, PA 04-181 and June 19 Special Session, PA 09-1, PA 11-93 and PA 16-67)

29-17a Criminal history checks. Procedure. Fees.

PA 16-67 An Act Concerning the Disclosure of Certain Education Personnel Records

Criminal Justice Information Services (CJIS) Security Policy, Version 5.4, U.S. Department of Justice, Federal Bureau of Investigation, Criminal Justice Information Services Division, October 6, 2015.

CJIS Security Policy

Title 28 C.F.R. Part 20

Policy adopted:
cps 4/17