General Personnel

Administrative Procedure - Fingerprint-Based Criminal History Record Information Security

The District is required by State law to conduct fingerprint-based criminal history record checks on applicants for employment. See administrative procedure 5:30-AP2, *Investigations*, for the procedures to be followed in carrying out such checks. This procedure outlines the District's responsibility to safeguard applicants' criminal justice information (CJI), including Criminal History Records Information (CHRI), received from the Federal Bureau of Investigation (FBI), whether the information is received directly from the FBI or through the Ill. State Police (ISP) or a live scan vendor pursuant to an existing Outsourcing Management Control Agreement. This procedure is based on the *FBI Criminal Justice Information Services (CJIS) Security Policy* (CJIS Security Policy) available at: https://le.fbi.gov/cjis-division/cjis-security-policy-resource-center (see Appendix J, Noncriminal Justice Agency Supplemental Guidance) and ISP's generic template titled *Criminal History Record Information Proper Access, Use, and Dissemination Procedures*.[1] The FBI's CJIS Security Policy provides a minimum set of security requirements for access to FBI CJIS Division systems and information and to protect and safeguard CJI.

Glossary of Terms

These definitions are based on those provided in the FBI CJIS Security Policy.

Criminal Justice Information (CJI) — All data provided through the FBI CJIS, including, but not limited to, biometric, identity history, person, organization, property (when accompanied by any personally identifiable information), and case/incident history data.

Criminal History Records Information (CHRI) — A subset of CJI that includes identifiable descriptions of arrests, detentions, indictments, information, or other formal criminal charges, and any disposition arising therefrom, including acquittal, sentencing, correctional supervision, and release. For purposes of this procedure, CHRI is interchangeable with CJI.

Authorized Personnel — District employee(s) who have been appropriately vetted through a national fingerprint-based record check and have been granted access to CJI. For purposes of this procedure, Authorized Personnel includes the Superintendent, Human Resources Administrator, Head of Information Technology, and their respective designees.

Electronic Media — Any form of electronic storage media such as a memory device in a laptop or computer (hard drive) or mobile device; and any removable, transportable electronic media, such as magnetic tape or disk, optical disk, flash drive, external hard drive, or digital memory card.

Physical Media — Media in printed form, including, but is not limited to, printed documents, printed imagery, and printed facsimile.

Remote Access — 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).

Actor	Action

Superintendent or Human Resources Administrator	If the District utilizes a live scan vendor, ensures the District has entered in an outsourcing agreement with the vendor that incorporates appropriate FBI security and management control outsourcing standards to protect CHRI. See https://www.fbi.gov/file-repository/compact-council-security-and-management-control-outsourcing-standard-for-non-channelers.pdf/view or www.fbi.gov/file-repository/compact-council-security-and-management-control-outsourcing-standard-for-channelers.pdf/view, depending on the status of the vendor (channelers are contractors selected by the FBI that have a direct connection to the FBI's identification system, see www.fbi.gov/how-we-can-help-you/more-fbi-services-and-information/compact-council/list-of-approved-channelers). For a list of live scan vendors in Illinois, see https://idfprapps.illinois.gov/licenselookup/fingerprintlist.asp. Point of Contact Designates employee(s) to serve as the District's Point of Contact (POC), who serves as the primary point of contact with the ISP regarding the District's handling of CJI. Ensures the District has applicable agreement(s) in place necessary to access CJI, e.g., an interagency user agreement with the ISP. Physical Security Designates a secure location within the District with physical and personnel security controls sufficient to protect CHRI and associated information system(s), including the following: 1. The location shall be prominently posted and physically separate from non-secure locations. 2. Only Authorized Personnel will have access to the physically secure location. 3. The District is able to control all access points and verify individual access authorizations before granting access. 4. The device(s) that displays CHRI is positioned in such a way as to prevent unauthorized individuals from accessing and/or viewing it. 5. CHRI on physical media is always stored in a locked cabinet/drawer/container at the District Office which is only accessible to Authorized Personnel. Physical media is not removed from the secure location area except for purposes of sanitization/disposal. Media Protection and Transport Ensures controls are in place to protect electronic and physical media containing CHRI while at rest, stored, or actively being accessed, as well as during transport outside of secure areas to prevent inadvertent or inappropriate disclosure and use. Only Authorized Personnel may transport electronic media or physical media containing CHRI. If physical and personnel restrictions are not feasible, directs the Head of Information Technology to ensure CHRI is encrypted per the CJIS Security Policy (pg. 160, see SC-13).

	<u>Sanitization and Disposal of CHRI</u> Properly sanitizes or disposes of (or designates Authorized Personnel to sanitize or dispose of) physical or electronic media containing CHRI in accordance with the District's record retention schedule. Physical media will be destroyed by one of the following methods: 1. Shredding using District-issue shredders. 2. Placement in locked shredding bins for a private District contractor to come on-site and shred, witnessed by Authorized Personnel. 3. Incineration using District incinerators or witnessed by Authorized Personnel onsite at a District or contractor incineration site, if conducted by non-authorized personnel. Electronic media will be disposed of by one of the following methods: 1. Overwriting at least three times (using a program to write onto the location of the media where the file to be sanitized is located) 2. Degaussing (magnetic erasure of data from magnetic media) 3. Physical destruction. (crushing, disassembling, etc., ensuring that the platters have been physically destroyed so that no data can be pulled). <u>Misuse of CHRI</u> In the event of misuse of CHRI by a District employee, issues discipline to the employee (such as loss of access privileges) or recommends discipline to the Board up to and including termination and/or refers the matter to law enforcement. See Board policies 5:200, *Terms and Conditions of Employment and Dismissal*, 5:240, *Suspensions*, and 5:290, *Employment Termination and Suspensions*.
Head of Information Technology	Assists the Superintendent and Human Resources Administrator as requested to implement appropriate controls for access to CHRI within the District. <u>Account Management</u> Manages information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. Validates information system accounts at least annually and documents the validation process. Monitors electronic system log access to CHRI on a weekly basis for indications of inappropriate or usual activity. <u>Remote Access and Personally Owned Devices</u> Authorizes, monitors, and controls all methods of remote access to the information systems that can access, process, transmit, and/or store CJI. Employs automated mechanisms to facilitate the monitoring and

	control of remote access methods and control all remote accesses through managed access control points. Permits remote access for privileged functions only for compelling operational needs and documents the rationale for such access in the security plan for the information system. If the District permits Authorized Personnel to use personal devices to access, process, store, or transmit CHRI, establishes and documents the specific terms and conditions for personal device use consistent with the requirements in Section 5.13 of the CJIS Security Policy (pg. 173-179). <u>Sanitization and Disposal of CHRI</u> Ensures that Information Technology systems that have been used to process, store, or transmit CHRI may not be released from the District's control until the equipment and has been sanitized and all stored information has been cleared using one of the methods authorized in this procedure. <u>Security Incidents</u> Assists the POC with the reporting of any security incidents to ISP. When feasible, employs automated mechanisms to assist in the reporting of security incidents.
District Point of Contact (POC)	Communicates as needed with the ISP regarding audits, District personnel changes, training, and security. Disseminates information security alerts and other communications from ISP to all Authorized Personnel. If applicable, identifies who is using live scan hardware, software, and firmware and ensures no unauthorized individuals or processes have access to the same. Identifies and documents how the equipment is connected to the ISP system. Ensures appropriate security measures to protect CHRI are in place and working as expected. Maintains a list of Authorized Personnel that is updated annually and when new users are registered or off boarded. Annually reviews all information system accounts to ensure that access and account privileges align with job functions, need-to-know, and employment status on systems that contain CHRI. Maintains a log for access to any physical files containing CHRI and monitors the log on a weekly basis for indications of inappropriate or unusual activity. Maintains Security Awareness Training Certificates for all Authorized Personnel. Informs all Authorized Personnel of the procedures for reporting security events and weaknesses that might have an impact on the security of CHRI. Ensures the ISP's Information Security Officer is promptly informed of any security incidents by contacting ISP.LEADSISO@illinois.gov.

	Upon an Authorized Person's separation form District employment, terminates that individual's access to systems or physical areas where CHRI is accessible.
Authorized Personnel	Completes Basic Security Awareness Training within six months of initial assignment and every two years thereafter as required under Section 5.2 of the CJIS Security Policy, as well as any other role-based training that may be required under the CJIS Security Policy (pgs. 11-16). Security Awareness Training is available at: https://www.cjisonline.com/. Submits Security Awareness Training Certificates to the POC. Complies with the District's established controls for access and handling of CHRI. Positions documents or other physical media containing CHRI and any devices through which CHRI is viewed in such a manner to prevent authorized persons from accessing or viewing the CHRI. Only communicates CHRI in secure, private areas. Takes extreme care to prevent overhearing or interception of communication. Unless authorized by the District under specific terms and conditions, never uses a personal device (computer, smartphone, tablet, flash drive, etc.) to access, view, process, store or transmit CHRI. Never uses a publicly accessible computer to access, process, store, or transmit CHRI. Promptly reports to the POC any security incidents or weaknesses associated with the District's information systems of which he or she becomes aware.