AR 3580.1 Criminal Justice Information Security

Note: The District does not currently receive, transmit, store, or access criminal justice information (CJI) electronically. Before any personnel working with District CJI can receive, transmit, store, or access CJI electronically, the District would be required to adopt additional policies that meet the Federal Bureau of Investigations Criminal Justice Information Services Security Policy requirements for: Acceptable Use, Antivirus Guidelines, Passwords, and Unique Identifiers~~, and User Account Access Validation~~.

A. User Account/Access Validation Policy

1. Purpose:

This User Account / Access Validation policy was developed using the FBI's Criminal Justice Information Services (CJIS) Security Policy. The intended target audience is District personnel with access to CJI whether logically or physically. The FBI Criminal Justice Information Services Security Policy shall always be the minimum standard concerning CJI received from the FBI and/or DPS. District may complement, augment, or increase the standards, but shall not detract from the FBI Criminal Justice Information Services Security Policy standards. This policy is in place to protect the employee and District. Unacceptable use of resources exposes District to risks including theft, misuse, virus attacks, compromises of the network systems and services, and legal issues.

2. Scope:

This policy applies to all employees, contractors, consultants, temporary staff, and other workers at District who are authorized any physical, logical, and/or electronic premise of the District to access, process, store, and/or transmit CJI. This also includes any private contractors/vendors who will conduct maintenance on any network device that processes, stores, and/or transmits FBI CJI. **Authorized User/Personnel** is an individual, or group of individuals, who have been appropriately granted access to CJI.

3. User Account access validation:

Primary responsibility for account management belongs to the Local Agency Security Officer (LASO) or his/her designee. All accounts shall be reviewed at least every six months by the LASO 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 LASO or his/her designee may also conduct periodic reviews.

The LASO or his/her designee must disable all new accounts that have not been accessed within 30 days of creation. Accounts of individuals on extended leave

(more than 30 days) should be disabled. (Note: Exceptions can be made in cases where uninterrupted access to IT resources is required.)

LASO or his/her designee shall:

1. Modify user accounts in response to events like name changes, accounting changes, permission changes, office transfers, etc.,
2. Periodically review existing accounts for validity (at least once every 6 months), and
3. Cooperate fully with a DPS or FBI authorized security team during an investigation of a security incident or performing an audit review.

The LASO or his/her designee must be notified if a user's information system usage or need-to-know changes (i.e., the employee is terminated, transferred, etc.). If an individual is assigned to another office for an extended period (more than 90 days), the LASO or his/her designee will transfer the individual's account(s) to the new office.

The LASO or his/her designee will remove or disable all access accounts for separated or terminated employees immediately following separation from the agency.

4. Guest Accounts:

All guest accounts (for those who are not official employees of the agency) with access to the criminal justice information on the network, shall contain an expiration date of one year or the work completion date, whichever occurs first. All guest accounts (for private contractor personnel) must be sponsored by the appropriate authorized member of the administrative entity managing the resource.

5. Enforcement:

Any violation of this policy may result in CJI access suspension, access removal, access revocation, corrective, or disciplinary action, civil or criminal prosecution, and termination of employment.

(cf. 1340 - Access to District Records)

(cf. 4119.23/4219.23/4319.23 - Unauthorized Release of Confidential Information)

(cf. 4118 - Suspension/Disciplinary Action)

(cf. 4218 - Dismissal/Suspension/Disciplinary Action)

B. Physical Security Policy

The District will store all criminal justice information (CJI) in a controlled area, such as a fireproof, locked filing cabinet. Access to the controlled area will be limited to personnel who are authorized to access or view CJI:

- The controlled area will be located in the District Office or other area with limited access.
- The controlled area will be locked when unattended.
- The key to the controlled area will be accessible only by those personnel who are authorized to access CJI.

(cf. 1340 - Access to District Records)

(cf. 4119.23/4219.23/4319.23 - Unauthorized Release of Confidential Information)

~~B~~C. Media Protection Policy

1. Purpose

The intent of the Media Protection Policy is to ensure the protection of the Criminal Justice Information (CJI) until such time as the information is either released to the public via authorized dissemination (e.g. within a court system or when presented in crime reports data), or is purged or destroyed in accordance with applicable record retention rules. The local policy may augment, or increase the standards, but shall not detract from the ~~Cjis~~Criminal Justice Information Services Security Policy standards.

2. Scope

The scope of this policy applies to any electronic or physical media containing State/FBI Criminal Justice Information (CJI) while being stored, accessed or physically moved from a secure location from the District. This policy applies to any authorized person who accesses, stores, and / or transports digital or physical media. Transporting CJI outside the agency's assigned physically secure area must be monitored and controlled only by authorized personnel.

Authorized District personnel shall protect and control digital and physical CJI while at rest and in transit. The District will take appropriate safeguards for protecting CJI to prevent potential mishandling or loss while being stored, accessed, or transported. Any inadvertent or inappropriate CJI disclosure and/or use will be reported to the District Local Agency Security Officer (LASO).

3. Media Storage and Access

Controls shall be in place to protect electronic and physical media containing CJI while at rest, stored, or actively being accessed. "Digital 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.

To protect CJI, the District personnel shall:

- Securely store electronic and physical media within a physically secure or controlled area. A secured area includes a locked drawer, cabinet, or room, to which only authorized personnel are able to access.
- Restrict access to electronic and physical media to authorized individuals.
- Ensure that only authorized users remove printed or digital media from the CJI.
- Physically protect CJI until media end of life. End of life CJI is destroyed or sanitized using approved equipment, techniques and procedures. (See Media Sanitization Destruction Policy)
- Not use personally owned information system 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. (See Personally Owned Device Policy, if allowed)
- Not utilize publicly accessible computers to access, process, store, or transmit CJI. Publicly accessible computers include but are not limited to: hotel business center computers, convention center computers, public library computers, public kiosk computers, etc.
- Store all hardcopy CJI printouts maintained by the District in a secure area accessible to only those employees whose job function requires them to handle such documents.
- Safeguard all CJI by the District against possible misuse by complying with the Physical Protection Policy, Personally Owned Device Policy, and Disciplinary Policy.
- Take appropriate action when in possession of CJI while not in a secure area:
    - CJI must not leave the employee's immediate control. CJI printouts cannot be left unsupervised while physical controls are not in place.

Precautions must be taken to obscure CJI from public view, such as by means of an opaque file folder or envelope for hard copy printouts. For electronic devices like laptops, use session lock use and /or privacy screens. CJI shall not be left in plain public view. When CJI is electronically transmitted outside the boundary of the physically secure location, the data shall be immediately protected using

encryption and advanced authentication, in accordance to the FBI ~~CJIS~~Criminal Justice Information Services Security Policy.

When CJI is at rest (i.e. stored electronically) outside the boundary of the physically secure location, the data shall be protected using encryption. Storage devices include external hard drives from computers, printers and copiers used with CJI. In addition, storage devices include thumb drives, flash drives, back-up tapes, mobile devices, laptops, etc.

When encryption is employed, the cryptographic module used shall be certified to meet FIPS 140-2 standards.

Lock or log off computer when not in immediate vicinity of work area to protect CJI. Not all personnel have same CJI access permissions and need to keep CJI protected on a need-to- know basis.

Establish appropriate administrative, technical and physical safeguards to ensure the security and confidentiality of CJI.

4. 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. "Electronic media" means electronic storage media including 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.

The District personnel shall:

- Protect and control digital and physical media during transport outside of the physically secure location or controlled area.
- Restrict the pickup, receipt, transfer and delivery of such media to authorized personnel.

The District personnel will control, protect, and secure electronic and physical media during transport from public disclosure by:

- ~~Use of~~Using privacy statements in electronic and paper documents.
- Limiting the collection, disclosure, sharing and use of CJI.
- Following the least privilege and role based rules for allowing access. Limit access to CJI to only those people or roles that require access.
- Securing hand carried confidential electronic and paper documents by:

    - Storing CJI in a locked briefcase or lockbox.
    - Only viewing or accessing the CJI electronically or document printouts in a physically secure location by authorized personnel.
    - Package hard copy printouts in such a way as to not have any CJI information viewable.

- For hardcopies that are mailed or shipped, agency must document procedures and only release to authorized individuals. DO NOT MARK THE PACKAGE TO BE MAILED CONFIDENTIAL. Packages containing CJI material are to be sent by method(s) that provide for complete shipment tracking and history, and signature confirmation of delivery.
- Not taking CJI home or when traveling unless authorized by District.

5. Electronic Media Sanitization and Disposal

The agency shall sanitize, that is, overwrite at least three times or degauss electronic media prior to disposal or release for reuse by unauthorized individuals. Inoperable electronic media shall be destroyed (cut up, shredded, etc.). The agency shall maintain written documentation of the steps taken to sanitize or destroy electronic media. Agencies shall ensure the sanitization or destruction is witnessed or carried out by authorized personnel. Physical media shall be securely disposed of when no longer required, using formal procedures. For end of life media policy, refer to "Media Sanitization Destruction Policy".

6. Breach Notification and Incident Reporting

The agency shall promptly report incident information to the District technology department, and if the incident involves CJI, to the LASO. Information security events and weaknesses associated with information systems shall be communicated in a manner allowing timely corrective action to be taken. Incident-related information can be obtained from a variety of sources including, but not limited to, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports.

If CJI is improperly disclosed, lost, or reported as not received, consult District's security incident response policy.

7. Enforcement

Violation of any of the requirements in this policy 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.

(cf. 1340 - Access to District Records)

(cf. 4119.23/4219.23/4319.23 - Unauthorized Release of Confidential Information)

(cf. 4118 - Suspension/Disciplinary Action)

(cf. 4218 - Dismissal/Suspension/Disciplinary Action)

(cf. 3515.4 - Recovery for Property Loss or Damage)

(cf. 5131.5 - Vandalism, Theft, Graffiti)

(cf. 5144 - Discipline)

(cf. 5144.1 - Suspension and Expulsion)

(cf. 5144.2 - Discipline for Students with Disabilities)

(cf. 5145.11 - Questioning and Apprehension)

(cf. 5145.12 - Search and Seizure)

(cf. 6161.4 - Internet)

~~C~~D. Disposal of Media Policy and Procedures

1. Purpose

The purpose of this policy is to outline the proper disposal of media at District. These rules are in place to protect sensitive and confidential information, employees, and District. Inappropriate disposal of District and State and/or FBI criminal justice information (CJI) and media may put employees, District, and the integrity of CJI at risk.

2. Scope

This policy applies to employees, contractors, temporary staff, and other workers at District, including all personnel with access to CJI media and systems that process CJI. This policy applies to all equipment that processes CJI that is owned or leased by District.

3. Policy

When no longer usable or have reached end-of-life/retention, all diskettes, tape cartridges, USB storage devices, hard copies, print-outs, IT systems (e.g., workstations, printers, copiers, fax machines, mobile devices, etc.), and other similar items used to process or store CJI data shall be properly disposed of in accordance with media sanitization and destruction requirements in the FBI

~~CJIS~~Criminal Justice Information Services Security Policy, Policy Area 8: Media Protection. These processes shall be carried out or witnessed by authorized personnel.

- Authorized personnel shall destroy printed CJI by cross-cut shredding or incineration; authorized personnel shall witness this process if it is conducted by non-authorized personnel.

- Digital media containing CJI shall be sanitized by at least three times overwrite or degauss prior to disposal or release for reuse by unauthorized individuals. If digital media are destroyed, they must be sanitized then cut up, shredded, or otherwise rendered completely inoperable so that no data can be recovered.

4. Outsourcing

Unless approved in writing by the Criminal Justice Information Services Systems Agency, which is the State of Alaska Department of Public Safety, outsourcing media storage and disposal to unauthorized personnel who would have unescorted access to unencrypted CJI is not permitted. Before District outsources functions to non-agency personnel or contractors (i.e., delegation of in-house operations to a third-party, such as IT functions, administrative operations, etc.), District must first have prior, written approval from the Criminal Justice Information Services Systems Agency, which for the State of Alaska is the Department of Public Safety, before permitting unescorted access to unencrypted CJI.

5. Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including civil and/or criminal penalties and/or termination of employment. For further information, consult District's CJI misuse policy.

(cf. 1340 - Access to District Records)

(cf. 4119.23/4219.23/4319.23 - Unauthorized Release of Confidential Information)

(cf. 4118 - Suspension/Disciplinary Action)

(cf. 4218 - Dismissal/Suspension/Disciplinary Action)

(cf. 3515.4 - Recovery for Property Loss or Damage)

(cf. 5131.5 - Vandalism, Theft, Graffiti)

(cf. 5144 - Discipline)

(cf. 5144.1 - Suspension and Expulsion)

(cf. 5144.2 - Discipline for Students with Disabilities)

(cf. 5145.11 - Questioning and Apprehension)

(cf. 5145.12 - Search and Seizure)

(cf. 6161.4 - Internet)

~~D~~E. Security Incident Response

1. Overview

A security incident response addresses how District will handle a confirmed security incident that resulted in a compromise of criminal justice information (CJI), whether the breach, theft, intrusion, or other such violation was physical (e.g., paper files, copies of fingerprint cards, etc.) or logical (i.e., digital). Notification to the State of Alaska Department of Public Safety (DPS) Criminal Justice Information Services (CJIS) Information Security Officer (ISO) is required if the incident involved CJI.

2. Purpose

The purpose of this policy is to outline the steps District will take for a confirmed security incident that involves CJI.

3. Scope

This policy applies to employees, contractors, consultants, temporary staff, and other workers at District, who work with or have access to State and/or FBI criminal justice information (CJI). This policy applies to all equipment that is owned or leased by District.

4. Policy

Whoever discovers the incident shall immediately contact their immediate supervisor. ~~S/he~~The person who discovers the incident shall include in a written report, in as much detail as possible, what was occurring that lead up to the discovery of the incident.

1. The superintendent or designee shall conduct an investigation to determine what caused the purported incident.
2. If a security incident is declared, District will take the following steps:

a. For an incident involving physical breaches (building break-ins, stolen items, etc.), District shall do the following:
    i. Report the incident to the appropriate authorities.
    ii. Follow appropriate procedures to secure the area and prevent additional breaches from occurring.
    iii. Review policies and procedures currently in place; recommend updates and/or revisions if warranted.
    iv. If breach is by employee(s) or student(s), ensure the appropriate disciplinary procedures are followed.
b. For an incident involving logical breaches (hacking, social engineering, ransomware, etc.), District shall do the following:
    i. Report the incident to the appropriate authorities.
    ii. Follow appropriate procedures to secure network and prevent additional breaches from occurring.
    iii. Review policies and procedures currently in place; recommend updates and/or revisions if warranted.
    iv. If breach is by employee(s) or student(s), ensure the appropriate disciplinary procedures are followed.
c. Within forty-eight (48) hours of a declared security incident, the ~~DPS~~ Alaska Department of Public Safety ~~CJIS~~Criminal Justice Information Services ~~ISO~~ Information Security Officer shall be notified at DPS.AUDIT@ALASKA.GOV and/or by calling 907-334-0857.
d. After the incident is resolved, District will confer with all parties involved in the security incident response and develop a "Lessons Learned" report which will detail the incident and response actions, as well as how District will reassess existing policies and procedures to reduce the likelihood of a repeat security incident.

(cf. 4118 - Suspension/Disciplinary Action)

(cf. 4218 - Dismissal/Suspension/Disciplinary Action)

(cf. 3515 - School Safety and Security)

(cf. 3515.4 - Recovery for Property Loss or Damage)

(cf. 5131.5 - Vandalism, Theft, Graffiti)

(cf. 5144 - Discipline)

(cf. 5144.1 - Suspension and Expulsion)

(cf. 5144.2 - Discipline for Students with Disabilities)

(cf. 5145.11 - Questioning and Apprehension)

(cf. 5145.12 - Search and Seizure)

Added 02/2019

Adoption Date: 04/09/98