New policy developed with guidance of AK Department of Public Safety to address corrective action items identified in CJIS Audit.

Business and Noninstructional Operations AR 3580.1(a)

CRIMINAL JUSTICE INFORMATION SECURITY

Acceptable Use Policy

1. Overview

The District's Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, web browsing, and File Transfer Protocol, access are the property of the District. These systems are to be used for business purposes in serving the interests of the agency in the course of normal operations. Effective security is a team effort involving the participation and support of every District employee and affiliate who deals with criminal justice information and/or criminal justice information systems. It is the responsibility of every computer user to know these guidelines and to conduct their activities accordingly.

2. Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at District. These rules are in place to protect the employee and District. Inappropriate use exposes District to risk including virus attacks, compromises of the network systems and services, and legal issues.

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

General Use and Ownership

a. While the District's network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the corporate system remains the property of the District.
b. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should consult their supervisor or management.
c. For security and network maintenance purposes, authorized individuals within District may monitor equipment, systems and network traffic at any time, per District <*Audit Policy*>.
d. District reserves the right to audit the network and systems on a periodic basis to ensure compliance with this policy.

New policy developed with guidance of AK Department of Public Safety to address corrective action items identified in CJIS Audit.

CRIMINAL JUSTICE INFORMATION SECURITY (continued)

Security and Proprietary Information

a. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. Please review District's Password Policy for guidance.
b. All computers, laptops, and workstations must be secured with password-protected screen savers with an automatic activation feature, set at ten minutes or less, or by logging off when the computer is unattended.
c. Because information contained on mobile devices is especially vulnerable, special care should be exercised. Protect these devices in accordance with *<Name of agency's Mobile Device Management policy>*.
d. All devices used by employees that are connected to the District Internet/Intranet/Extranet shall be continually executing approved and up-to-date malicious code, spyware, and spam protection software.
e. Employees must use extreme caution upon receiving e-mail attachments received from unknown senders, which may contain viruses or other malicious code. Employees should contact District IT help desk before opening suspicious emails.

Unacceptable Use

The following activities are, in general, prohibited. Under no circumstances is an employee of the District authorized to engage in any activity that is illegal under local, state, federal, or international law utilizing District owned resources. The list below are by no means exhaustive, but attempts to provide a frame work for activities which fall into the category of unacceptable use.

System and Network Activities

The following activities are strictly prohibited, with no exceptions:

a. Unauthorized access, coping, or dissemination of confidential or sensitive information (e.g., state and/or FBI CJI, state criminal information, etc.).
b. Installation of any copyrighted software for which District or end user does not have an active license is strictly prohibited.
c. Installation of any software without preapproval and virus scan is strictly prohibited.
d. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, logic bombs, etc.).
e. Revealing your account password to others or allowing use of your account by others.
f. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server that the employee is not expressly authorized to access,. For the purpose of this policy, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

New policy developed with guidance of AK Department of Public Safety to address corrective action items identified in CJIS Audit.

CRIMINAL JUSTICE INFORMATION SECURITY (continued)

h. Port scanning or security scanning is expressly prohibited unless prior notification has been given to District Security administration.
i. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's assigned job/duty.
j. Circumventing user authentication or security of any host, network, or account.
k. Interfering with or denying service to any user other than the employee's host.
l. Using any program/script/command or sending messages of any kind, with the intent to interfere with or disable a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

5. Enforcement

Violations of this policy include, but are not limited to: accessing data to which the individual has no authorization enabling unauthorized individuals to access data; disclosing data in a way that violates applicable policy, procedures, or relevant regulations or law; inappropriately modifying or destroying data; inadequately protecting restricted data. Any violation of this policy may result in network removal, access revocation, corrective or disciplinary action, civil or criminal prosecution, and termination of employment.

Anti-Virus Guidelines

1. Purpose

To establish requirements which must be met by all computers connected to District networks that process, store, or transmit criminal justice information to ensure effective virus detection and prevention.

2. Scope

This policy applies to all District computers that are PC-based or use PC-file directory sharing. This includes, but is not limited to, desktop computers, file/ftp/tftp/proxy servers, and any PC-based equipment.

3. Policy

All District PC-based computers must have District's standard, supported anti-virus software installed and scheduled to run at regular intervals. In addition, the anti-virus software and the virus pattern files must be kept up-to-date. District's information security team has provided the following processes to ensure that anti-virus software is run at regular intervals, and to keep computers virus-free.

Processes to prevent virus problems:

a. Only run current, supported operating systems and software.
b. Run the current version of and install malicious code protection software updates as they become available.

New policy developed with guidance of AK Department of Public Safety to address corrective action items identified in CJIS Audit.

CRIMINAL JUSTICE INFORMATION SECURITY (continued)

c. Anti-virus software is to be enabled on all workstations and servers at start-up and employ resident scanning.
d. Detect and eliminate viruses on computer workstations, laptops, servers, and simple mail transfer protocol gateways.
e. On servers, update virus signatures files immediately, or as soon as possible, with each new release.
f. NEVER open any files or macros attached to an email from an unknown, suspicious, or untrustworthy source. Delete these attachments immediately, then "double delete" them by emptying your Trash.
g. Delete spam, chain, and other junk email without opening the messages and report them to technical support staff.
h. Never download files from unknown or suspicious sources.
i. Always have IT scan any media that is brought into the agency before introducing it to the network.
j. Any activities with the intention to create and/or distribute malicious programs into District's networks (e.g., viruses, worms, Trojan horses, logic bombs, etc.) are prohibited. Virus- infected computers must be removed from the network until they are verified as virus-free. If a virus is detected on your workstation and the anti-virus software can not eliminate the virus, please contact <*Agency Representative*>.

4. 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.

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

New policy developed with guidance of AK Department of Public Safety to address corrective action items identified in CJIS Audit.

CRIMINAL JUSTICE INFORMATION SECURITY (continued)

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 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.

Password Policy and Procedures

1. Overview

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in a compromise of District's entire network. As such, all District employees (including contractors and vendors with access to District systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their password.

New policy developed with guidance of AK Department of Public Safety to address corrective action items identified in CJIS Audit.

CRIMINAL JUSTICE INFORMATION SECURITY (continued)

2. Purpose

The purpose of this policy is to establish a standard for the creation of strong passwords, the protection of those passwords, and the frequency of change.

3. Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any District facility, has access to the District network, or stores, processes, or transmits criminal justice information (CJI).

4. Policy

General

a. All user and administrative passwords must be changed at least every 90 days.
b. All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every 90 days.
c. Passwords must not be shared.
d. Where simple network management protocol (SMTP) is used, the community strings must be defined as something other than the standard defaults of "public," "private," and "system" and must be different from passwords used to log in interactively. A keyed hash must be used where available (e.g., SNMPv2).
e. All user-level, system-level, and CJI access passwords must conform to the guidelines described below.

Guidelines

General Password Construction

Passwords are used for various purposes at District. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, voicemail password, and local router logins. Since very few systems have support for one-time tokens (i.e., Dynamic passwords which are used once), everyone should be aware of how to select strong passwords.

Poor, weak passwords have the following characteristics:

- The password contains less than eight characters.
- The password is a word found in a dictionary (English or foreign)
- The password is a common usage word such as:
- Name of family, pets, friends, co-workers, fantasy characters, etc.
- Computer terms and names, commands, sites companies, hardware, software.
- The words "District," "or any derivation.
- Birthdays and other personal information such as addresses and phone numbers.
- Word or number patterns like aaabbb, 111222, zyxwvts, 4654321, etc.
- Any of the above spelled backward like nhoj, yrrehckcalb, yffulf, etc.
- Any of the above preceded or followed by a digit (e.g., secret1, 1secret).

New policy developed with guidance of AK Department of Public Safety to address corrective action items identified in CJIS Audit.

CRIMINAL JUSTICE INFORMATION SECURITY (continued)

Passwords must meet the following minimum requirements:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters, e.g., 0-9, !@#$%^&*()_+{}[]:";<>?,.?
- Are at least eight alphanumeric characters long
- Are not a dictionary word
- Are not based on personal information, names of family, etc.

Password Protection Standards

Do not use your user id as your password. Do not use the same password for different District accounts. Do not share District passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential District information.

Here is a list of "do not's"

- Don't share a password
- Don't hint at the format of a password (e.g., "my family name")
- Don't reveal a password on questionnaires or security forms
- Don't share a password with family members
- Don't use the "Remember Password" feature of applications
- Don't write passwords down and store them anywhere in your office.
- If someone demands a password, refer them to this document or have them call <*list name of Information Security Officer (ISO) or Agency POC*>.

If an account or password is suspected to have been compromised, report the incident to <*Name of ISO or POC*> and change all passwords.

Application Development Standards

Application developers must ensure their programs contain the following security precautions:

- Should support authentication of individual users, not groups.
- Must not store passwords in clear text or in any easily reversible form.
- Should provide some sort of role management, such that one user can take over the function of another without having to know the other's password.
- Should support Terminal Access Controller Access Control System+ (TACACS+), Remote Authentication Dial-In User Service (RADIUS), and/or X.509 with Lightweight Directory Access Protocol (LDAP) security retrieval, wherever possible.

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.

New policy developed with guidance of AK Department of Public Safety to address corrective action items identified in CJIS Audit.

CRIMINAL JUSTICE INFORMATION SECURITY (continued)

Unique Identifier Policy and Procedures

1. Purpose

The purpose of this policy is to ensure accountability of all users that access District network and network devices.

2. Scope

The scope of this policy is to define the creation of a unique identifier for individuals that access District network, network devices and criminal justice information (CJI).

3. Policy

General

District requires that each employee that has access to District network and/or applications for the purpose of storing, processing, and/or transmitting CJI shall be uniquely identified by use of a unique identifier. A unique identifier shall also be required for all persons who administer and maintain the system(s) that access agency and CJI information and/or network. District requires users to identify themselves uniquely before the user is allowed to perform any action on the network and/or applications. All user IDs shall belong to currently authorized users. Identification data shall be kept current by adding new users and disabling former users. Employees shall not share their IDs with other employees, supervisors, management, or family members at any time.

Guidelines

The unique identification can take the form of the following examples:

- User's full name (JohnWDoe)
- Form of full name (SASmith)
- Badge number (WV724966)
- Combination of name and badge number (jhardWV966)
- Serial Number (123456789)
- Other unique alphanumeric identifier

4. 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.

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

New policy developed with guidance of AK Department of Public Safety to address corrective action items identified in CJIS Audit.

CRIMINAL JUSTICE INFORMATION SECURITY (continued)

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 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)

New policy developed with guidance of AK Department of Public Safety to address corrective action items identified in CJIS Audit.

CRIMINAL JUSTICE INFORMATION SECURITY (continued)

- 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 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.

New policy developed with guidance of AK Department of Public Safety to address corrective action items identified in CJIS Audit.

CRIMINAL JUSTICE INFORMATION SECURITY (continued)

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 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 IT staff, 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.

New policy developed with guidance of AK Department of Public Safety to address corrective action items identified in CJIS Audit.

CRIMINAL JUSTICE INFORMATION SECURITY (continued)

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.

User Account – Access Validation Policy

1. Purpose

To establish requirements for user accounts and access validation for all networking processing, storing, or transmitting criminal justice information (CJI) to ensure the security of system access and accountability.

2. Scope

All accounts shall be reviewed annually by the local agency security officer (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 CJI. The [LASO or his/her designee] may also conduct periodic reviews.

3. Policy

All guest accounts (for those who are not official employees of District) with access to <District > 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.

The LASO or his/her designee should 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. In those instances, the individual going on extended leave should have a manager-approved request from the designated account administrator or assistant.)

The LASO or his/her designee must be notified if a user's information system usage or need-to-know changes (e.g., 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 (CJA only).

The LASO or his/her designee will remove or disable all access accounts for separated or terminated employees immediately following separation from the agency, and will notify the CJIS ISO with DPS of the separation of all authorized personnel.

New policy developed with guidance of AK Department of Public Safety to address corrective action items identified in CJIS Audit.

CRIMINAL JUSTICE INFORMATION SECURITY (continued)

Primary responsibility for account management belongs to the LASO or his/her designee. The LASO or his/her designee shall:

- Modify user accounts in response to events like name changes, accounting changes, permission changes, office transfers, etc.
- Periodically review existing accounts for validity, and
- Cooperate fully with an authorized security team that is investigating a security incident or performing an audit review.

4. Enforcement

Any violation of this policy may result in network removal, access revocation, corrective or disciplinary action, and termination of employment.

Physical Security Policy

This is not a template, but instead guidance to provide ideas of what can be included in your policy, depending on your agency's operations. Items noted as "if applicable" are only applicable if the agency electronically processes Criminal Justice Information (CJI) (e.g., storage, file servers, emails, data tracking, scanning, etc.)

Specifics on what the FBI requires for physical security can be found in the FBI CJIS Security Policy, Policy Area 9: Physical Protection.

For a physically secure location (meaning the agency controls all access points of its building, facility, etc., and/or network), the physical security policy must include at minimum:

- Identification of the perimeter of the physically secure location
    - E.g., signage that indicates "authorized personnel only" or otherwise indicates a restricted area
- Access control points (except those areas that are officially designated as publicly accessible)
    - E.g., who maintains, distributes, and authorizes access (keys, door codes, etc.)
- Access control authorization
    - The agency must keep a current list of personnel with authorized access to the physically secure location or controlled areas
- Access control for the display medium
    - Agency must prevent unauthorized personnel from viewing CJI (e.g., positioning monitors
- Monitoring physical access (if applicable)
    - Physical access to the information system(s) that process CJI must be monitored and the agency must be able to detect and respond to physical security incidents (see also "Security Incident Response" policy)

New policy developed with guidance of AK Department of Public Safety to address corrective action items identified in CJIS Audit.

CRIMINAL JUSTICE INFORMATION SECURITY (continued)

- Visitor control (if applicable)
  - How the agency authenticates and escorts visitors at all times (except in areas that are designated as publicly accessible)
- Delivery and removal of information system items (if applicable)
  - How agency authorizes and controls these items entering and exiting the physically secure location
- Access control for transmission medium (if applicable)
  - If the agency transmits CJI outside of its physically secure location (e.g., electronically backing up CJI in off-site areas such as the Cloud, permitting remote access into the agency network, etc.), the agency shall control physical access to information system distribution and transmission lines within the physically secure location.

For a controlled area (meaning a place where the agency cannot control all access points but can store CJI in a controlled area such as a cabinet, room, or storage container), the physical security policy must address at minimum:

- How the agency limits access to the controlled area
- How the agency secures the area when unattended
- Instructions for preventing unauthorized personnel from viewing CJI (e.g., locking all files containing CJI in a file room that only authorized personnel have a key to access)
- Following encryption requirements in FBI CJIS Security Policy Section 5.10.1.2 for electronic storage (if applicable)

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.

New policy developed with guidance of AK Department of Public Safety to address corrective action items identified in CJIS Audit.

CRIMINAL JUSTICE INFORMATION SECURITY (continued)

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 <Insert Agency's desired point-of-contact, such as immediate supervisor or IT helpdesk>. S/he shall note, in as much detail as possible, what was occurring that lead up to the discovery of the incident.

1. *<Insert Agency Name's appropriate investigative authority>* shall conduct an investigation to determine what caused the purported incident.
2. If a security incident is declared, District will take the following steps:
3. For an incident involving physical breaches (building break-ins, stolen items, etc.), District shall do the following:
    a. <List Agency Name's procedures>
4. For an incident involving logical breaches (hacking, social engineering, ransomware, etc.), District shall do the following:
    a. <List Agency Name's procedures>
5. Within forty-eight (48) hours of a declared security incident, the DPS CJIS ISO shall be notified at DPS.AUDIT@ALASKA.GOV and/or by calling 907-334-0857.
6. 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.