STATE OF ALASKA DEPARTMENT OF CORRECTIONS POLICIES & PROCEDURES	SECTION: **Administration**		PAGE: Page **1** of **3**
	CHAPTER: **650**	NUMBER: **650.02**	P&P TYPE: **Public**
	TITLE: **CJIS Security**		
	APPROVED BY: **Nancy A. Dahlstrom, Commissioner**		DATE: **1/28/2022**
ATTACHMENTS / FORMS: **N/A**	AUTHORITY / REFERENCES: **22 AAC 05.155**, **AS 44.28.030**, **AS 33.05.010**, **DOC P&P 202.01**, **AS 33.16.180**, **DOC P&P 202.15**, **AS 33.30.011**, **DOC P&P 650.01**, **AS 33.30.021**, **DOC P&P 650.02**, **SOA/OIT Policy 5.7.3 ISP-143: Information Disposal.**		

POLICY:

I. It is the policy of the Department of Corrections (DOC) that any transportation of Criminal Justice Information (CJI) outside the Department's secure area must be monitored and controlled.

II. It is the policy of the Department to have in place procedures to ensure the protection of CJI stored on various forms of media, 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.

III. It is the policy of the Department that authorized Department personnel shall protect and control electronic and physical CJI while at rest and in transit. The Department will take appropriate safeguards for protecting CJI to limit potential mishandling or loss while being stored, accessed, or transported. Any inadvertent or inappropriate CJI disclosure and / or use will be reported to the Department of Corrections Criminal Justice Information Systems (CJIS) Unit, Local Agency Security Officer (LASO) and State CJIS Systems Agency (CSA). Procedures shall be defined for securely handling, transporting and storing media containing CJI.

APPLICATION:

This policy applies to any electronic or physical media containing Criminal Justice Information (CJI) while being stored, accessed, or physically moved from secure Department of Corrections locations. This policy applies to any authorized person who accesses, stores, and / or transports electronic or physical media.

DEFINITIONS:

Electronic media (also known as logical)- Includes memory devices in laptops and computers (hard drives) and any removable, transportable digital memory media, such as magnetic tape or disk (CD/DVD/Blue Ray), backup medium, optical disk, flash drives, external hard drives, or digital memory card.

Physical media- Includes files, printed documents, and imagery that contain CJI.

PROCEDURES:

I. Media Storage and Access:

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

B. To protect CJI, DOC personnel shall:

1. Take appropriate action when in possession of CJI while not in a secure area, such as:

a. Ensure that CJI not leave the employee's immediate control, and that CJI printouts are not left unsupervised while physical controls are not in place.

b. CJI shall not be left in plain, public view. Obscure CJI from public view, such as by means of an opaque file folder, or envelope, for hardcopy printouts. For electronic devices, use session locks and / or privacy screens.

c. When CJI is electronically transmitted outside the boundary of the physically secure location, the data shall be protected using encryption.

d. Protect CJI using IT approved encryption software or media when outside the boundary of the physically secure location.

2. Lock, or log off, the computer when not in the immediate vicinity of the work area.

II. Media Transportation and Dissemination:
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:

A. When CJI is in transit, physically or electronically,, outside the boundary of the physically secure location, the data shall be secured and/or protected using encryption.

B. DOC personnel shall:

1. Protect and control electronic and physical media during transport outside of controlled areas; and

2. Restrict the pickup, receipt, transfer, and delivery of such media to authorized personnel.

C. DOC personnel will control, protect, and secure electronic and physical media, during transport, from public disclosure by:

1. Use of privacy statements in electronic and paper documents;

2. Limiting the collection, sharing, and use of CJI;

3. Follow the least privilege and role-based rules for allowing access. Limit access to CJI to only those people, or roles, that require access; based on business need.

4. Securing hand-carried and shipped confidential electronic and physical copy documents by:

    a. Storing CJI in a locked briefcase or lockbox;

    b. Only viewing or accessing the CJI in a physically secure location by authorized personnel; and

    c. Shipment of electronic or physical media containing confidential or CJI shall be:

        i. Packaged in such a way as to not have any CJI information viewable;

        ii. Sealed with Tamper Evident (Security) tape or packaged in a locked, hardened shipping container;

        iii. Mailed or shipped, packages containing CJI material are to be sent by methods that provide for complete shipment tracking and history, signature confirmation upon delivery, and only release to authorized individuals;

        NOTE: DO NOT MARK "CONFIDENTIAL" ON THE PACKAGE TO BE MAILED.

5. Not taking CJI home, unless authorized by that staff member's Division Director; and

6. When disposing of confidential physical documents, a crosscut shedder or secure shred storage box shall be used.

III. Media Sanitation and Disposal:

A. In accordance with SOA / OIT Policy 5.7.3 ISP-143: Information Disposal, and the attached form (if necessary): Physical media shall be securely disposed of when no longer required, using formal procedures. Electronic media shall be forwarded to IT for disposed.

IV. Incident Reporting and Response:
All security incidents shall be reported to the CJIS Unit in accordance with DOC P&P 650.08 (CJIS Incident Reporting / Response).