
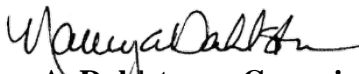


| | | | |
|--|---|---|----------------------------|
| <p>STATE OF ALASKA DEPARTMENT OF CORRECTIONS</p>  <p>POLICIES & PROCEDURES</p> | SECTION: Administration | | PAGE: Page 1 of 4 |
| | CHAPTER: 650 | NUMBER: 650.04 | P&P TYPE: Public |
| | TITLE: Acceptable Use of Criminal Justice Information (CJI) | | |
| | APPROVED BY:  Nancy A. Dahlstrom, Commissioner | | DATE: 01/28/2022 |
| ATTACHMENTS / FORMS: N/A | | AUTHORITY / REFERENCES: 13 AAC 68.300-345 AS 12.62.900 22 AAC 05.090-095 AS 28.15.151 22 AAC 05.155 AS 33.30.011 22 AAC 20.910 AS 33.30.021 AS 11.46.740 AS 40.25.120 AS 11.56.860 AS 44.28.030 AS 12.62.150-190 DOC P&P 202.01 FBI CJIS Security Policy. DOC P&P 202.15 SOA/OIT 5.10.2 ISP-172: Business Use and Access Control. SOA / OIT Policy 5.11.2 ISP-192: Encryption. SOA / OIT Policy 5.11.4 ISP-194: External E-Mail Encryption. DPS CJIS Systems Agency (CSA) Policy. | |

DISCUSSION:

Department of Corrections (DOC) employees, contractors, and vendors regularly use computer information systems and resources to collect, use, store, and share criminal justice information (CJI). To protect this information, our use of systems and resources must meet the high standards of our industry. This policy is designed to help fulfill that responsibility and to provide guidance on how resources should, and should not, be used while performing job duties and functions. Inappropriate use exposes DOC to risk including virus attacks, compromises of the network systems and services, and legal issues.

POLICY:

- I. It is the policy of the Department of Corrections (DOC) to have in place procedures for the acceptable use of computer equipment within the Department.

APPLICATION:

This policy applies to all employees, contractors, consultants, and temporary staff. This policy applies to all equipment that is owned or leased by DOC and connected to the DOC network.

DEFINITIONS:

| | |
|-------------------------------------|----------|
| SUPERCEDES POLICY DATED: | N/A |
| THIS POLICY NEXT DUE FOR REVIEW ON: | 01/28/27 |

| | | |
|---|--------------------------|-----------------------------|
| SECTION: Administration | | PAGE: Page 2 of 4 |
| CHAPTER: 650 | NUMBER: 650.04 | P&P TYPE: Public |
| TITLE: Acceptable Use of Criminal Justice Information (CJI) | | |

For definitions of key words or phrases used in this policy, please refer to the Definitions section of DOC P&P 650.00, CJI Terms & Definitions and/or CJI Acronyms.

PROCEDURES:

In accordance with SOA / OIT Policy 5.10.2 ISP-172: Business Use and Access Control:

I. E-mail:

- A. State of Alaska, DOC sponsored, email accounts are for business communications, both internally and externally. Use of third-party email system(s) for business purposes, or automatic forward of DOC e-mail to an e-mail address outside the SOA \ DOC network is prohibited.
- B. CJI shall only be transmitted in a secure fashion that conforms to the standards set out by the FBI in their CJIS Security Policy. When information is transmitted electronically, it shall be protected, confirm the receiving party has the authority (CJIS Security Clearance and business reason) to receive and access CJI \ Personally Identifiable Information (PII) \ Protected Health Information (PHI) and shall use SOA secure e-mail messaging as outlined within SOA / OIT Policy 5.11.4 ISP-194: External E-Mail Encryption.

II. Removeable Media:

Removable Media is defined as CD / DVD or USB Mass Storage (thumb or jump drive) that can electronically store data containing CJI \ PII \ PHI and easily be transported out of a secure facility. All confidential information including CJI \ PII \ PHI on removable media must be encrypted with certified FIPS 140-2 or FIPS 197 encryption; in accordance with SOA / OIT Policy 5.11.2 ISP-192: Encryption and FBI CJIS Security Policy 5.10 System and Communications Protections and Information Integrity; while physically transported from a secure office or facility.

III. Personal Computing Equipment Prohibited Use:

It is a security risk to process CJI on a personal computing device. In order to utilize a personal device, it must be approved in writing by the Commissioner or designee and a copy of the agreement provided to DOC CJIS Unit. The personal device shall not be connected to the SOA Network. Once no longer employed by DOC, or no longer used in conjunction with duties, the personal computing device must be wiped in accordance with Media Security; DoD 5220-22.M compliant three (3) pass random wipe.

Refer to SOA / OIT 5.10.2 ISP-172: Business Use and Access Control.

Refer to SOA / OIT 5.7.3 ISP-143: Information Disposal

IV. Contractor Computer Equipment Authorization:

Refer to SOA / OIT 5.10.2 ISP-172: Business Use and Access Control.

V. International Travel Restrictions

| | |
|-------------------------------------|-----------------|
| SUPERCEDES POLICY DATED: | N/A |
| THIS POLICY NEXT DUE FOR REVIEW ON: | 01/28/27 |

| | | |
|---|--------------------------|-----------------------------|
| SECTION: Administration | | PAGE: Page 3 of 4 |
| CHAPTER: 650 | NUMBER: 650.04 | P&P TYPE: Public |
| TITLE: Acceptable Use of Criminal Justice Information (CJI) | | |

Coordinate with Department Technology Officer (DTO) and submit an International Travel Cyber Security Form. User shall work with OIT to establish a loaner and travel email. User shall not connect to DOC's Offender Management System or remotely process CJI while traveling internationally.

<http://oit.alaska.gov/policy/international-travel-policy/>

VI. Criminal Justice Information (CJI) Protection (ref. AK DOC P&P 650.03):

All employees, contractors, consultants, and temporary staff shall:

- A. Protect CJI in all formats, including oral, paper, and electronic;
- B. Protect CJI against unauthorized access or disclosure by ensuring that only those people who have a clearly demonstrated need to know or use the CJI are given access;
- C. Follow established procedures for media handling;
- D. Securely store all removable media when not in use; and
- E. Follow established guidelines when transporting media.

VII. Proper Access, Use and Dissemination of Criminal Justice Information (CJI) and Criminal History Record Information (CHRI):

- A. The access, use, and dissemination of CJI, CHRI, and PII obtained from a DOC CJI System(s) are governed by both state and federal laws; additional restrictions on the access, use, and dissemination of CJI may be listed in each agency's User Agreement. Although certain information is not confidential when it is obtained from another source (e.g., court record, newspaper, etc.), the same information is confidential when accessed through DOC CJI Systems.
- B. Confidential photographs obtained from DOC CJI System(s) may only be accessed, used, or disseminated by a criminal justice agency for a criminal justice purpose as outlined in AS 28.15.151(f) and AS 12.62.160(b)(4). Release of a photograph to an unauthorized person(s), or the press, of a person who is the subject of a story (such as a person who has been involved in an incident, or who is the victim of a crime), is not authorized.
- C. FBI CJIS data, data received from other states, and / or NLETS data, obtained through a DOC CJI System, shall be handled consistent with access, use, and dissemination policies in the FBI CJIS Security Policy, the National Crime Information Center (NCIC) Operating manual, and the NLETS user Policy Manual. The information cannot be accessed, used, or disseminated except as specifically authorized by a federal law, or by a state statute that has been approved by the US Attorney General under P.L. 92-544.
- D. The CSA, FBI and DOC CJIS Unit may audit users at any time to determine if the user accessed, used, or disseminated CJI from or through a DOC CJI System. Therefore, users must know what state or federal law authorizes them to access, use or disseminate CJI before doing so.
- E. Criminal justice information and the identity of recipients of criminal justice information are confidential and exempt from disclosure under AS 40.25. The existence or nonexistence of criminal

| | |
|-------------------------------------|-----------------|
| SUPERCEDES POLICY DATED: | N/A |
| THIS POLICY NEXT DUE FOR REVIEW ON: | 01/28/27 |

| | | |
|--|-----------------------|--------------------------|
| SECTION: Administration | | PAGE: Page 4 of 4 |
| CHAPTER: 650 | NUMBER: 650.04 | P&P TYPE: Public |
| TITLE: Acceptable Use of Criminal Justice Information (CJI) | | |

justice information may not be released to or confirmed to any person except as provided in this section and AS 12.62.180 (d).

VIII. Enforcement:

- A. Violations of this policy include but are not limited to: accessing data to which the individual has no business reason or legitimate right; 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.
- B. Any violation of this policy may result in suspension of user login account(s), corrective or disciplinary action, civil or criminal prosecution, up to and including termination of employment as outlined in DOC P&P 202.01, Code of Ethical and Professional Conduct, and DOC P&P 202.15, Standards of Conduct.
- C. Alaska Statute (AS) 11.56.860 states that:

A person who is or has been a public servant commits the crime of misuse of confidential information if the person learns confidential information through employment as a public servant; and while in office or after leaving office, uses the confidential information for personal gain or in a manner not connected with the performance of official duties other than by giving sworn testimony or evidence in a legal proceeding in conformity with a court order.

As used in this section, "confidential information" means information which has been classified confidential by law. Misuse of confidential information is a class A misdemeanor.

| | |
|-------------------------------------|-----------------|
| SUPERCEDES POLICY DATED: | N/A |
| THIS POLICY NEXT DUE FOR REVIEW ON: | 01/28/27 |