
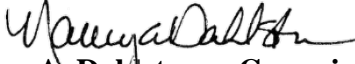


<b>STATE OF ALASKA</b> <b>DEPARTMENT OF CORRECTIONS</b>  <b>POLICIES &amp; PROCEDURES</b>	SECTION: <b>Administration</b>		PAGE: Page 1 of 5
	CHAPTER: <b>650</b>	NUMBER: <b>650.01</b>	P&P TYPE: <b>Public</b>
	TITLE: <b>Criminal Justice Information (CJI) Access</b>		
	APPROVED BY:  Nancy A. Dahlstrom, Commissioner		DATE: <b>01/28/2022</b>
ATTACHMENTS / FORMS: A. DOC Employee Network Access Form. B. Non-DOC Employee Network Access Form. C. Alaska Corrections Offender Management System (ACOMS) Access Form.		AUTHORITY / REFERENCES: 13 AAC 68.215 AS 33.16.180 22 AAC 05.155 AS 33.30.011 AS 12.62.160 AS 33.30.021 AS 33.05.010 AS 44.28.030 FBI CJIS Security Policy, Policy Areas 2, 5, 6 & 12. DPS CJIS Systems Agency (CSA) Policy. SOA/OIT Policy 5.6.1 ISP-131: Personnel Security. SOA/OIT Policy 5.6.2 ISP-132: Security Awareness and Training. SOA/OIT Policy 5.10.1 ISP-171: Identity Management. SOA/OIT Policy 5.10.8 ISP-178: Password Management.	

**POLICY:**

- I. It is the policy of the Department of Corrections (DOC) to have in place procedures regarding access to criminal justice information (CJI).
- II. It is the policy of the Department to utilize internal and external CJI systems and any criminal justice information or confidential information contained within those systems, in accordance with federal and state law.

**APPLICATION:**

This policy and procedure will apply to all Department employees, contractors, consultants, temporary staff, and any other related entity. This policy and procedure applies to all equipment that is owned or leased by DOC and / or is connected to the DOC network.

**DEFINITIONS:**

**Access to Criminal Justice Information** — The physical or logical (electronic) ability, right or privilege to view, modify or make use of Criminal Justice Information.

**Contractor** — A private business, agency or individual which has entered into an agreement for the administration of criminal justice or noncriminal justice functions with a Criminal Justice Agency or a Noncriminal Justice Agency.

SUPERCEDES POLICY DATED:	<b>N / A</b>
THIS POLICY NEXT DUE FOR REVIEW ON:	<b>01/28/27</b>

SECTION: <b>Administration</b>		PAGE: <b>Page 2 of 5</b>
CHAPTER: <b>650</b>	NUMBER: <b>650.01</b>	P&P TYPE: <b>Public</b>
TITLE: <b>Criminal Justice Information (CJI) Access</b>		

**Contracting Government Agency (CGA)** — The government agency, whether a Criminal Justice Agency or a Noncriminal Justice Agency, which enters into an agreement with a private contractor.

**Criminal Justice Agency (CJA)** — The courts, a governmental agency, or any subunit of a governmental agency which performs the administration of criminal justice pursuant to a statute or executive order and which allocates a substantial part of its annual budget to the administration of criminal justice. State and federal Inspectors General Offices are included.

**Criminal Justice Information (CJI)** — Criminal Justice Information is the abstract term used to refer to all data necessary for law enforcement agencies to perform their mission and enforce the laws, including but not limited to: biometric, identity history, person, organization, property (when accompanied by any personally identifiable information), and case/incident history data.

**Terminal Agency Coordinator (TAC)** — Serves as the point-of-contact at the local agency for matters relating to CJIS information access. A TAC administers CJIS systems programs within the local agency and oversees the agency’s compliance with CJIS systems policies.

**Unique Identification (unique ID):** can take the form of a full name, badge number, serial number, and /or other unique alphanumeric identifier. Agencies shall ensure that all user IDs belong to currently authorized users. Identification data shall be kept current by adding new users and disabling and/or deleting former users.

**PROCEDURES:**

I. General Procedures:

All users requesting access to DOC CJI (physical or electronic) or unescorted access to a secure office, in accordance with 13 AAC 68.215, shall undergo a state of residency and an FBI Nationwide fingerprint background check. All requesters shall fill out a DPS Personnel Security Clearance Form and User Agreement, obtain two copies of fingerprints, and submit for processing as listed in II below.

- A. If the background check reveals a felony conviction of any kind, access to CJI will be denied.
- B. Applicants with a record of misdemeanor offense(s) and/or fugitive will receive an initial denial of their application. A review of extenuating circumstances, offense severity, age of the offense and any other factors supporting a possible variance. A recommendation will be forwarded to DOC Commissioner or designee for final determination. Please refer to Section III. Appeal Process
- C. If a conviction of record is found on a contractor, Contracting Government Agency (CGA), or temporary hire, agency shall be formally notified, and system access shall be delayed pending review of the criminal history record information.

II. CJI Clearance and Access Procedures:

- A. All DOC employees shall:

SUPERCEDES POLICY DATED:	<b>N / A</b>
THIS POLICY NEXT DUE FOR REVIEW ON:	<b>01/28/27</b>

SECTION: <b>Administration</b>		PAGE: <b>Page 3 of 5</b>
CHAPTER: <b>650</b>	NUMBER: <b>650.01</b>	P&P TYPE: <b>Public</b>
TITLE: <b>Criminal Justice Information (CJI) Access</b>		

1. Submit a DOC Employee Network Access Form (Attachment A) and ACOMS Access Form (Attachment C), per instructions on form, prior to accessing any Department CJI or information system.
2. Submit DPS Personal Security Clearance Form and User Agreement and two copies of Fingerprints to local APSIN TAC.
3. Complete security awareness and/or APSIN Test within six (6) weeks of appointment of station and biennial thereafter.

B. All Non-DOC employees shall:

1. Fill out and submit a Non-DOC Employee Network Access Form (Attachment B) and, if needed, ACOMS Access Form (Attachment C), per instructions on form, prior to accessing any Department CJI or information system.
2. Submit DPS Personal Security Clearance Form and User Agreement and two copies of Fingerprints to DOC CJIS Unit
3. Complete Security Awareness training prior to gaining authorization to access to CJI or secure facility, and bi-annually thereafter.
4. Have appropriate signed agreement(s) on file:
  - a. Any CJA receiving access to CJI shall enter into a signed written agreement with the appropriate signatory authority. The written agreement shall specify the CJI, information systems, and services to which the agency will have access, and the policies to which the agency must adhere.
  - b. A Non-Criminal Justice Agency designated to perform criminal justice functions for a CJA shall be eligible for access to the CJI. Access shall be permitted when such designation is authorized pursuant to executive order, statute, regulation, or interagency agreement.

C. All Contractors \ Vendors accessing CJI shall:

1. Fill out and submit a Non-DOC Employee Network Access Form (Attachment B) and, if necessary, ACOMS Access Form (Attachment C), per instructions on form, prior to accessing any DOC CJI or Information Systems.
2. Submit DPS Personal Security Clearance Form and User Agreement and two copies of Fingerprints to DOC CJIS Unit
3. Read, sign, and submit the FBI Security Addendum
4. Complete Security Awareness training prior to gaining authorization to access to CJI or secure

SUPERCEDES POLICY DATED:	<b>N / A</b>
THIS POLICY NEXT DUE FOR REVIEW ON:	<b>01/28/27</b>

SECTION: <b>Administration</b>		PAGE: <b>Page 4 of 5</b>
CHAPTER: <b>650</b>	NUMBER: <b>650.01</b>	P&P TYPE: <b>Public</b>
TITLE: <b>Criminal Justice Information (CJI) Access</b>		

facility, and bi-annually thereafter.

### III. Appeal Process

DOC shall process all appeals through the Commissioner’s Office, or designee, within six weeks of receipt.

- A. DOC Designated APSIN TAC will receive a denial for any misdemeanor conviction, along with an appeal, from DPS. APSIN TAC shall conduct research and interview applicant to process the appeal.
  - 1. APSIN TAC shall forward the completed appeal to [doc.cjis@alaska.gov](mailto:doc.cjis@alaska.gov)
  - 2. A CJIS Unit Ticket created
- B. For DOC staff appeals, CJIS Unit shall forward to HR for hiring packet and nexus review.
  - 1. HR appends recommendation **APPROVE or DENY**.
  - 2. Replies to CJIS Unit Notification, CJIS Unit Ticket Updated

*Note: Appeals for contractors and vendors remain with CJIS Unit and are forwarded directly to Commissioner or designee when complete.*
- C. CJIS Unit shall forward to Division Director
  - 1. Division Director Reviews and appends recommendation **APPROVE or DENY**.
  - 2. Replies to CJIS Unit Notification, CJIS Unit Ticket Updated
- D. CJIS Unit reviews to ensure compliance with FBI CJIS Security Policy and CSA
  - 1. CJIS Unit Reviews and appends recommendation **APPROVE or DENY**.
  - 2. CJIS Unit Updates Ticket
- E. CJIS Unit Notifies Commissioner or Commissioner Designee of pending appeal.
- F. Commissioner or Commissioner Designee shall:
  - 1. Review and make decision to **APPROVE or DENY**.
  - 2. Signs the Appeal Document
  - 3. CJIS Unit Ticket Updated
- G. CJIS Unit submits final decision to DPS for consideration.
- H. CJIS Unit logs the appeal and decision.

### IV. Accounts:

- A. All users shall be assigned a unique ID:
- B. Users **shall keep confidential** their assigned credentials (User ID and Password)
- C. Passwords shall:
  - 1. Be a minimum length of eight (8) characters on all systems.

SUPERCEDES POLICY DATED:	<b>N / A</b>
THIS POLICY NEXT DUE FOR REVIEW ON:	<b>01/28/27</b>

SECTION: <b>Administration</b>		PAGE: <b>Page 5 of 5</b>
CHAPTER: <b>650</b>	NUMBER: <b>650.01</b>	P&P TYPE: <b>Public</b>
TITLE: <b>Criminal Justice Information (CJI) Access</b>		

2. Not be a dictionary word or proper name.
3. Not be the same as the User ID.
4. Expire within a maximum of 90 calendar days.
5. Not be identical to the previous ten (10) passwords.
6. Not be displayed when entered.

V. Account Validation:

- A. Information system access will be granted for all personnel for no more than one (1) calendar year, expiring on December 31<sup>st</sup> each year. Information system access expiration notices will be emailed to the Agency Designated TAC by December 1<sup>st</sup>. A response to the expiration notice must be received prior to December 31 of the current year in order to retain their access. If no response to the expiration email is received, access will end on December 31<sup>st</sup> for all users associated with the agency. A valid response will extend information system access for the agency users through December 31<sup>st</sup> of the following year without interruption:
  1. Agency designated TAC will be provided a list of **active** agency users and asked to check Valid, No Longer Need Access, Left Agency, and \ or Unknown for each user.
- B. Information system access will be revoked sooner than December 31<sup>st</sup> if DOC is notified by agency to do so or user violates any terms of the access agreement.
- C. It is the responsibility of the agency designated TAC to disable and or notify DOC when an end-user leaves services with your agency and or no longer has a business need, for access within a timely manner.

VI. Penalties / Sanctions for Misuse:

Use of any CJI or information system including electronic or physical files for any use other than the performance of the employee's job duties is prohibited and subject to penalty. Any misuse of CJI or dissemination of information not specifically authorized may result in disciplinary action, civil action for actual damages and/or criminal penalties. Refer to DOC policy and procedure 202.15 (Standards of Conduct).

SUPERCEDES POLICY DATED:	<b>N / A</b>
THIS POLICY NEXT DUE FOR REVIEW ON:	<b>01/28/27</b>