


**STATE OF ALASKA
DEPARTMENT OF CORRECTIONS**



POLICIES & PROCEDURES

SECTION: Administration		PAGE: Page 1 of 4
CHAPTER: 650	NUMBER: 650.01	P&P TYPE: Public
TITLE: Criminal Justice Information (CJI) Access		
APPROVED BY:  Nancy A. Dahlstrom, Commissioner		DATE: 05/06/2020
ATTACHMENTS / FORMS: A. DOC Employee Network Access Form 603.02A B. Non-DOC Employee Network Access Form 603.02B		AUTHORITY / REFERENCES: AS 12.62.160 13 AAC 68.215 22 AAC 05.155 AS 33.05.010 13 AAC 68.220 AS 33.30.011 13 AAC 68.330

POLICY:

- I. It is the policy of the Department of Corrections (DOC) to have procedures in place for accessing criminal justice information (CJI).
- II. It is the policy of the Department that all CJI, CJI systems (CJIS), and confidential information is utilized in accordance with federal and state law.

APPLICATION:

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

DEFINITIONS:

Access to CJI:

The physical or logical (electronic) ability, right, or privilege to view, modify, or make use of CJI.

Contractor:

A private business, agency or individual which has entered into an agreement for the administration of criminal justice or noncriminal justice functions.

Contracting Government Agency (CGA):

The government 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.

CJA User Agreement:

A signed terms-of-service agreement that establishes each CJA user's responsibilities, the forms and methods of acceptable use, penalties for violations and disclaimers.

SUPERCEDES POLICY DATED:	N/A
THIS POLICY NEXT DUE FOR REVIEW ON:	04/05/2025

SECTION: Administration		PAGE: Page 2 of 4
CHAPTER: 650	NUMBER: 650.01	P&P TYPE: Public
TITLE: Criminal Justice Information (CJI) Access		

Criminal Justice Information (CJI):

The abstract term used in reference 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.

Escorted Access:

A level of access that requires an approved CJIS cleared user to accompany a non-cleared, or limited security user, while around CJI and / or accessing a Secure Facility.

Terminal Agency Coordinator (TAC):

Serves as the point-of-contact at the local agency for matters relating to CJIS access. A TAC administers CJIS programs within the local agency and oversees the agency’s compliance with CJIS policies.

Unescorted Access:

The ability to freely move around a secure facility and / or directly access CJI.

User Identification (user ID):

Can take the form of a full name, badge number, serial number, or another 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. Background Check:

In accordance with 13 AAC 68.215, all users requesting access to DOC CJI or unescorted access to a secure office shall undergo a state of residency and FBI national fingerprint-based background check complying with the requirements enumerated in Section II below.

A. If a background check reveals a felony conviction, access to CJI will be denied.

B. A misdemeanor conviction and / or fugitive record will result in an initial denial of the application. After 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 the Commissioner or designee for final determination.

C. If a contractor, CGA, or temporary hire has any type of criminal record, the 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:

1. Submit a DOC Employee Network Access Form (Attachment A) per instructions on form and prior to accessing any Department CJI or information system.

SUPERCEDES POLICY DATED:	N/A
THIS POLICY NEXT DUE FOR REVIEW ON:	04/05/2025

SECTION: Administration		PAGE: Page 3 of 4
CHAPTER: 650	NUMBER: 650.01	P&P TYPE: Public
TITLE: Criminal Justice Information (CJI) Access		

2. Submit Department of Public Safety (DPS) Personal Security Clearance Form and User Agreement and two copies of fingerprints to the local TAC.
3. Complete Security Awareness training and / or APSIN test within six (6) weeks of appointment of station and biennially thereafter.

B. All Non-DOC employees shall:

1. Fill out and submit a Non-DOC Employee Network Access Form (Attachment B) per instructions on form and prior to accessing any Department CJI or information systems.
2. Submit DPS Personal Security Clearance Form and User Agreement and two copies of fingerprints or CJIS / APSIN Certification if obtained through your agency to DOC CJIS Unit.
3. Complete Security Awareness training prior to gaining authorization to access CJI or a secure facility, and biennially 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 system, 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) per instructions on the form, prior to accessing any DOC CJI or information system.
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 a secure facility, and bi-annually thereafter.

SUPERCEDES POLICY DATED:	N/A
THIS POLICY NEXT DUE FOR REVIEW ON:	04/05/2025

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

III. Accounts:

- A. All users shall be assigned a unique user ID:
- B. Users shall keep their assigned credentials (user IDs and passwords) confidential.

IV. Account Validation:

- A. Information system access will be granted for no more than one (1) calendar year, expiring on December 31st each year. Information system access expiration notices will be emailed to the agency designated TAC by December 1st. A response to the expiration notice must be received prior to December 31st of the current year in order to retain access. If no response to the expiration email is received, access will end on December 31st for all users associated with the agency. A valid response will extend information system access for agency users through December 31st of the following year without interruption:
 - 1. The agency designated TAC will be provided a list of active agency users. The TAC will verify a status of: Valid, No Longer Need Access, Left Agency, and \ or Unknown for each user.
- B. Information system access will be revoked sooner than December 31st if DOC is notified by an agency to do so, or if a 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 the agency's services or no longer has a business need for access, within a timely manner.

V. 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 P&P 202.15 (Standards of Conduct).

###

SUPERCEDES POLICY DATED:	N/A
THIS POLICY NEXT DUE FOR REVIEW ON:	04/05/2025