	DEPARTMENT OF CORRECTIONS **Information Systems**	
Title:	**Acceptable Use and Management of Criminal Justice Information**	**DOC Policy: 60.1.7**
Effective:	**11/1/16**	**Supersedes: N/A**
Applicability:	**All DOC employees, contractors, and volunteers**	
Directives Cross-Reference:	**OAR 107-009-0050 (DAS)**	
Attachments:	**None**	

I. PURPOSE

The purpose of this policy is to identify the required protection of Criminal Justice Information (CJI) 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 schedules.

This policy was developed using the FBI's Criminal Justice Information Services (CJIS) Security policy 5.5 dated 6/1/2016. The Department of Corrections policy sets standards; however, the CJIS Security policy shall always be the minimum standard. Although this policy may augment or increase the standards, it shall not detract from the CJIS Security policy standards.

II. DEFINITIONS

A. Criminal Justice Information (CJI): The abstract term used to refer to all of the FBI Criminal Justice Information Services provided 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. In addition, Criminal Justice Information refers to the FBI Criminal Justice Information Services provided data necessary for civil agencies to perform their mission including but not limited to data used to make hiring decisions.

B. DOC Local Agency Security Officer (LASO): The DOC person responsible for oversight and compliance with this policy.

C. Electronic Media: 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, thumb drives, or digital memory card.

D. Physical Media: Printed documents and imagery that contain Criminal Justice Information.

III. POLICY

A. Scope:

1. The scope of this policy applies to any electronic or physical media containing FBI Criminal Justice Information (CJI) while being stored, accessed or physically moved from a secure location from the department. This policy applies to any authorized person who accesses, stores, and/or transports electronic or physical media. Transporting Criminal Justice Information outside the department's assigned physically secure area must be monitored and controlled.

2. Authorized DOC staff shall protect and control electronic and physical Criminal Justice Information while at rest and in transit. The department will take appropriate safeguards for protecting Criminal Justice Information to limit potential mishandling or loss while being stored, accessed, or transported. Any inadvertent or inappropriate Criminal Justice Information disclosure and/or use will be reported to the DOC Local Agency Security Officer (LASO) and the DOC Information Security Officer (ISO). Procedures shall be defined for securely handling, transporting and storing media.

B. Media Storage and Access:

Controls shall be in place to protect electronic and physical media containing Criminal Justice Information while at rest, stored, or actively being accessed. To protect Criminal Justice Information, DOC staff shall:

1. Securely store electronic and physical media within a physically secure or controlled area. A secured area includes a locked drawer, cabinet, or room only accessible to authorized staff.

2. Restrict access to electronic and physical media to authorized staff.

3. Ensure that only authorized staff remove printed form or digital media from the Criminal Justice Information.

4. Physically protect Criminal Justice Information until media end of life. End of life Criminal Justice Information is destroyed or sanitized using approved equipment, techniques and procedures. (See Sanitization Destruction Policy)

5. Not use personally owned information system to access, process, store, or transmit Criminal Justice Information.

6. Not utilize publicly accessible computers to access, process, store, or transmit Criminal Justice Information. Publicly accessible computers include but are not limited to: hotel business center computers, convention center computers, public library computers, public kiosk computers, etc.

7. Not utilize unsecured, public Wi-Fi for accessing any Criminal Justice Information via DOC supplied mobile devices, include phones, tablets or laptops.

8. Store all hardcopy Criminal Justice Information printouts maintained by the department in a secure area accessible to only those employees whose job function requires them to handle such documents.

9. Safeguard all Criminal Justice Information by the department against possible misuse by complying with all DOC Acceptable Use and Protection policies (60.1.1 through 60.1.6).

10. Take appropriate action when in possession of Criminal Justice Information while not in a secure area:

    a. Criminal Justice Information must not leave the employee's immediate control. Criminal Justice Information printouts cannot be left unsupervised while physical controls are not in place.

    b. Precautions must be taken to obscure Criminal Justice Information 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 and/or privacy screens. Criminal Justice Information shall not be left in plain public view. When Criminal Justice Information is electronically transmitted outside the boundary of the physically secure location, the data shall be immediately protected using encryption.

        1) When Criminal Justice Information 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 Criminal Justice Information. In addition, storage devices include thumb drives, flash drives, back-up tapes, mobile devices, laptops, etc.

        2) When encryption is employed, the cryptographic module used shall be certified to meet Federal Standards.

11. Lock or log off computer when not in immediate vicinity of work area to protect Criminal Justice Information. Not all personnel have same Criminal Justice Information access permissions and need to keep Criminal Justice Information protected on a need-to-know basis.

12. Establish appropriate administrative, technical and physical safeguards to ensure the security and confidentiality of Criminal Justice Information.

C. Media Transport:

1. Controls shall be in place to protect electronic and physical media containing Criminal Justice Information while in transport (physically moved from one location to another) to prevent inadvertent or inappropriate disclosure and use.

2. Dissemination to another agency is authorized if:

    a. The other agency is an authorized recipient of such information and is being serviced by the accessing agency, or

    b. The other agency is performing personnel and appointment functions for criminal justice employment applicants.

3. DOC staff shall:

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

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

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

    a. Use of privacy statements in electronic and paper documents.

    b. Limiting the collection, disclosure, sharing and use of Criminal Justice Information.

    c. Following the least privilege and role based rules for allowing access. Limit access to Criminal Justice Information to only those people or roles that require access.

    d. Securing hand carried confidential electronic and paper documents by:

        1) Storing Criminal Justice Information in a locked briefcase or lockbox.

        2) Only viewing or accessing the Criminal Justice Information electronically or document printouts in a physically secure location by authorized personnel.

        3) For hard copy printouts or Criminal Justice Information documents:

            - Package hard copy printouts in such a way as to not have any Criminal Justice Information viewable.

            - That are mailed or shipped, DOC staff must document procedures and only release to authorized individuals. DO NOT MARK THE PACKAGE TO BE MAILED CONFIDENTIAL. Packages containing Criminal Justice Information material shall be sent by methods that provide for complete shipment tracking and history, and signature confirmation of delivery. This includes the US Postal Service, United Parcel Service, and FedEx Corporation.

e. Not taking Criminal Justice Information home or when traveling unless authorized in writing (letter or email) by the DOC Local Agency Security Officer. When disposing confidential documents, use a cross-cut shredder.

D. Electronic Media Sanitization and Disposal:

The department 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.). In accordance with DAS policy 107-009-005, the department shall maintain written documentation of the steps taken to sanitize or destroy electronic media. The department shall ensure the sanitization or destruction is witnessed or carried out by authorized staff. Physical media shall be securely disposed of when no longer required, using formal procedures.

E. Breach Notification and Incident Reporting:

The department shall promptly report incident information to appropriate authorities. 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.

F. Roles and Responsibilities:

If is improperly disclosed, lost, or reported as not received, the following procedures must be immediately followed:

1. DOC staff shall notify their supervisor or the DOC Local Agency Security Officer. An Information Security Incident Report form, CD1581 (found in policy 60.1.6), must be completed and submitted within 24 hours of discovery of the incident. The submitted report shall contain a detailed account of the incident, events leading to the incident, and steps taken/to be taken in response to the incident.

2. The supervisor will communicate the situation to the DOC Local Agency Security Officer to notify of the loss or disclosure of Criminal Justice Information records.

3. The DOC Local Agency Security Officer will ensure the CJIS System Agency Information Security Officer (CSA ISO) and the DOC Information Security Officer is promptly informed of security incidents.

4. The CJIS System Agency Information Security Officer (in accordance with CJIS Security Policy 5.5) will:

    a. Establish a security incident response and reporting procedure to discover, investigate, document, and report to the CJIS System Agency (CSA), the affected criminal justice agency, and the FBI CJIS Division Information Security

Office major incidents that significantly endanger the security or integrity of Criminal Justice Information.

b. Collect and disseminate all incident-related information received from the Department of Justice, FBI CJIS Division, and other entities to the appropriate local law enforcement Point of Contacts within their area.

c. Act as a single point of contact for their jurisdictional area for requesting incident response assistance.

G. Penalties:

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.

H. Questions:

Any questions related to this policy may be directed to the DOC Local Agency Security Officer.

IV. IMPLEMENTATION

Each DOC staff member must take required biennial CJIS training to fully implement this policy.

Certified: signature on file
Birdie Worley, Rules Coordinator

Approved: signature on file
Brian Belleque, Deputy Director