	DEPARTMENT OF CORRECTIONS **Information Technology Services**	
Title:	**Acceptable Use of Information Technology**	**DOC Policy: 60.1.1**
Effective:	**6/4/25**	**Supersedes: 8/5/22**
Applicability:	**All DOC Employees, Contractors, and Volunteers**	
Directives Cross-Reference	**DOC Policy 60.3.3 Mobile Device Management** **OAR 291-086 AIC Access to Information Technology**	
Attachments:	**None**	

I. PURPOSE

The purpose of this policy is to establish clear guidelines for the acceptable use of agency-owned technology resources and infrastructure. This policy ensures compliance with relevant Oregon Revised Statutes (ORS), Oregon Administrative Rules (OAR), and federal regulations including Criminal Justice Information Services (CJIS) requirements. It outlines responsibilities, usage standards, and enforcement measures to safeguard the security and integrity of agency systems, data, and operations.

In the event of a conflict between this policy and another Department of Corrections (DOC) Chapter 60 Information Systems policy, the policy with the most recent effective date shall take precedence. Furthermore, if there is a conflict between any Department of Corrections (DOC) Chapter 60 policy Information Systems and the Oregon Statewide Information Security Program Plan or the Oregon Statewide Information Technology Control Standards, the most restrictive policy shall govern.

II. DEFINITIONS

A. **Adult in Custody (AIC)**: Any person under the supervision of the Department of Corrections who is not on parole, probation, or post-prison supervision status.

B. **Agency-Owned Technology**: Includes desktop computers, laptops, virtual client hardware, tablets, smartphones, portable storage devices, servers, networks, cloud services, firewalls, routers, switches, and any other electronic device, system, or component purchased, leased, or managed by the Oregon Department of Corrections.

C. **Authorized Personnel**: Individuals granted explicit permission to access specific resources based on their job duties or contracted responsibilities.

D. **Communication Tools**: Email, instant messaging, video conferencing, and any other official methods used for internal or external business communication.

E. **Criminal Justice Information (CJI):** Criminal justice information is the abstract term used to refer to all of the FBI CJIS-provided data necessary for law enforcement agencies to perform their mission and enforce the laws including, but not limited to, biometric, identity history, biographic, property, and case or incident history data. In addition, CJI refers to the FBI CJIS-provided data necessary for civil agencies to perform their mission including, but not limited to, data used to make hiring decisions. The following categories of criminal justice information describe the various data sets housed by the FBI CJIS architecture:

1. Biometric Data – Data derived from one or more intrinsic physical or behavioral traits of humans typically for the purpose of uniquely identifying individuals from within a population. Used to identify individuals, to include fingerprints, palm prints, iris scans, and facial recognition data.

2. Identity History Data – Textual data that corresponds with an individual's biometric data, providing a history of criminal or civil events for the identified individual.

3. Biographic Data – Information about individuals associated with a unique case and not necessarily connected to identity data. Biographic data does not provide a history of an individual, only information related to a unique case.

4. Property Data – Information about vehicles and property associated with crime when accompanied by any personally identifiable information (PII).

5. Case or Incident History – Information about the history of criminal incidents.

F. **Criminal Justice Information Services (FBI CJIS or CJIS)**: The Federal Bureau of Investigation (FBI) division responsible for the collection, warehousing, and timely dissemination of relevant criminal justice information to the Federal Bureau of Investigation and to qualified law enforcement, criminal justice, civilian, academic, employment, and licensing agencies.

G. **Data Storage**: Physical or virtual repositories where agency-related data is stored. Examples include shared drives, local drives, cloud storage, and databases.

H. **Employee**: Any person employed full-time, part-time, or under temporary appointment by the Department of Corrections.

I. **Functional Unit Manager (FUM)**: Any person within the Department of Corrections who reports to either a Director, Deputy Director, an Assistant Director, or an

administrator and has responsibility for delivery of program services or coordination of program operations.

J. **Information Security Officer (ISO)**: The individual within the Department of Corrections who has the responsibility to establish and maintain information security policy, assess threats and vulnerabilities, perform risk and control assessments, oversee the governance of security operations, and establish information security training and awareness programs. The Information Security Officer also interfaces with security operations to manage implementation details and with auditors to verify compliance to established policies. The Information Security Officer is responsible for coordinating program requirements throughout the agency with designated points of contact.

K. **Internet Use**: Access to the internet for agency-sanctioned uses such as browsing, streaming, or file downloads.

L. **Non-Agency Device**: Any device such as a smartphone, tablet, laptop, etc. that has been purchased or provided by an entity other than the Oregon Department of Corrections.

M. **Remote Access**: Any connection to agency networks or resources from an external or non-agency-controlled network.

N. **Removable Media**: Portable data storage medium that can be added to or removed from a computing device or network. Examples include optical discs (CD, DVD, Blu-ray); external hard drives; flash memory devices (USB, Flash Drive, Thumb Drive); flash memory cards (Secure Digital, CompactFlash, Memory Stick, MultiMediaCard); and other external or removable disks.

O. **Security Systems Officer**: A Department of Corrections employee designated by the institution functional unit manager, with sufficient authority to coordinate the facility's efforts to maintain adequate and secure access to security electronic systems.

P. **Work-in-Progress (WIP) Data**: Data accumulated from one or more sources to be used towards the completion of assigned work.

III. POLICY

A. Acceptable Use of Information Technology

Department of Corrections provides access to information technology for the sole purpose of assisting employees in performing their assigned duties. Users of Department of Corrections information technology are responsible for their conduct and behavior while utilizing agency resources. Department of Corrections-provided information technology and all data contained or processed within are considered state assets and must adhere to the following acceptable uses.

1. Acceptable Use

    a. Agency-Owned Technology Devices

        A. Devices must be used only for official Department of Corrections business, unless limited personal use is specifically authorized by applicable policy.

        B. Installation of non-agency-approved software or altering device configurations is prohibited without prior IT approval.

        C. Users are responsible for the security and proper handling of assigned devices, including timely reporting of loss or damage.

        D. Devices must be used in compliance with all applicable policies, laws, and regulations.

        E. Authorized personal use must not interfere with work responsibilities, compromise security, violate state regulations, or incur additional costs to the agency.

    b. Agency-Owned Technology Infrastructure

        A. Users must not tamper with, alter, or compromise networks, servers, cloud resources, or other infrastructure components.

        B. Any unauthorized attempt to breach network security or access restricted areas of the infrastructure is strictly prohibited.

        C. All employees must promptly report any unusual activity or suspected security incidents to the IT security team.

    c. Communication Tools

        A. Official agency communication tools are reserved for work-related correspondence.

        B. Confidential or sensitive information must be communicated only through approved and secure channels.

        C. Personal use of agency communication tools is discouraged and may be permissible only if it does not interfere with duties or incur costs.

        D. All data transmitted over agency communication tools is considered state data, discoverable, and subject to records retention schedules.

    d. Data Storage

        A. Users must use the home drive (H:\) for the storage of WIP Data or business-related items that are considered personal use such as Human Resource forms, certifications, travel records, etc.

        B. Users must use their location-based drive (P:\) for the storage of completed work or group work where access to the data is limited to your assigned physical location.

C. Users must use the agency-based drive (U:\) for the storage of completed work or group work where access to the data is agency-wide or involves more than one physical location.

D. State-managed cloud storage is provided for the storage of data utilized in Department of Corrections collaboration tools such as Microsoft Teams and as the storage location for media such as audio and video recordings or pictures.

E. Removable media devices must not be used for the retention of state data. These devices must adhere to strict inventory control, utilize encryption technology, and require a use case that is approved by the Department of Corrections Information Security Officer.

Removable media device requests will be rejected when another storage location listed in this section would suffice.

F. All data stored in any agency data storage location is considered state data, discoverable, and subject to records retention schedules.

e. Internet Use

A. The internet is a work tool and must be used responsibly, following all cybersecurity best practices.

B. Accessing illegal, inappropriate, or malicious websites and downloading unauthorized content is strictly prohibited.

C. Employees must exercise caution to avoid phishing schemes or malware infections.

D. Employees in a direct supervision area are to utilize systems in break areas for personal browsing.

i. Internet browsing while working in a direct supervision area is restricted to agency-related duties specific to the post.

ii. Employees working in a direct supervision area will be provided time away from their post to complete required computer-based trainings.

f. Non-Agency Devices

A. Non-agency devices must not be used for agency work.

B. Non-agency devices must not be brought into the secure perimeter of a facility without signed approval from the functional unit manager and the Department of Corrections Information Security Officer.

C. Approved non-agency devices must meet agency security standards including up-to-date antivirus and operating systems and adhere to DOC Policy 60.3.4 Non-Agency Mobile Devices.

Approved non-agency devices fall under the same rules, policies, and requirements as state-issued devices.

D. The agency reserves the right to revoke non-agency device usage privileges at any time, without reason.

g. Security Electronics Systems

A. Security electronic systems (for example, camera systems, perimeter alarms, door controls) are strictly for operational, investigational, and safety purposes.

B. Each institution will assign a Security Systems Officer who is responsible for:

i. Ensuring that security electronic systems are kept up to date and software updates are performed regularly by authorized personnel.

ii. Authorizing system access to specific employees for the purpose of maintaining, monitoring, or acquiring data from the security electronic systems.

iii. Maintaining and regularly reviewing access lists to ensure appropriate employees have the correct level of access to security electronic systems to perform their work.

C. Disseminating data related to security electronics systems is strictly prohibited without express authorization from the Professional Standards Unit (PSU).

Security electronics data provided to employees in the Legal Affairs Unit, a Hearings Officer, or Legal Information Officer is exempt from the above prohibition when done in the course of the employee's official Department of Corrections work.

D. Unauthorized access, tampering, copying, deletion, or manipulation of security electronic devices or the data they contain is grounds for disciplinary action, including dismissal and possible legal proceedings.

2. Acceptable Uses of Criminal Justice Information Services

a. Access to CJIS data in any form is granted solely to authorized employees for official law enforcement and corrections functions.

b. Unauthorized viewing, distribution, or misuse of CJIS data is prohibited and may result in criminal penalties.

c. CJIS information must be handled in accordance with FBI CJIS security policy, including encryption and secure transmission requirements.

d. The most recently enacted FBI CJIS security policy supersedes any Department of Corrections policy regarding the collection, processing,

maintenance, use, sharing, dissemination, or disposition of criminal justice information (CJI).

3. AIC Use of Information Technology

   Use of information technology within the agency by adults in custody falls under OAR 291-086 AIC Access to Information Technology ("Rule 86").

B. Access and Authorization

Access to Department of Corrections information technology is strictly controlled, and supervising managers are responsible for ensuring their employees are limited to the access necessary to perform their duties.

1. Access for Authorized Purposes

   a. Employee access to information technology must align with job duties, contractual obligations, or official agency volunteer duties. Authorized access levels will be routinely verified to ensure employees have the correct level of access to perform their work.

   b. Unauthorized attempts to gain higher-level privileges are subject to disciplinary action.

2. Access for Non-Employees

   a. Contractors, vendors, and volunteers must complete mandatory security training before receiving limited access.

   b. All access must be reviewed and approved by the supervising manager.

3. Access Requests

   a. Supervising managers must submit initial access requests through the Department of Corrections Service Desk, detailing the access needed.

      The Department of Corrections Service Desk will assist with user authorization requests ensuring appropriate forms are properly completed and submitted to the Department of Corrections Information Technology Services (ITS) Profiles Team.

   b. Additional access modifications may be performed by the employee's local Technical Support Analyst (TSA).

4. Access Terminations

   a. Immediate revocation of access is required upon reassignment, administrative leave, or termination of employment or contract.

   b. Managers must inform the Department of Corrections Service Desk of any employee changes requiring access adjustments within 48 hours of the change.

5. Account Activation or Termination

The Department of Corrections Information Technology Services (ITS) Profiles Team will create, modify, or terminate accounts according to agency onboarding or offboarding policies and processes.

6. Remote Access

    a. Remote connections to agency systems for employee use must be encrypted, use multi-factor authentication, and require a state-issued system.

    b. Remote access may be revoked at any time for misuse or other determination by the supervising manager or the Department of Corrections Information Security Officer.

C. Employee Responsibilities and Expectations

1. Compliance and Legal Standards

    Employees are responsible for following all applicable state and federal laws, as well as agency policies, procedures, and rules while utilizing information technology.

2. Data Security and Privacy

    a. Users must maintain confidentiality of sensitive information and handle all data in accordance with privacy laws and regulations.

    b. Personally identifiable information (PII) or protected health information (PHI) must be handled in compliance with legal and regulatory requirements.

3. Password Management

    a. All passwords must meet agency complexity requirements and be changed periodically.

    b. Employees must never share passwords, write them down, or store them in an unencrypted file.

D. Hardware and Software Management

1. Department of Corrections Information Technology Services (ITS) is responsible for procuring, deploying, and managing hardware and software.

2. Unauthorized installations, upgrades, or modifications on agency devices are not permitted.

3. All software must be licensed and approved by the agency; pirated or unlicensed software is strictly prohibited.

E. Monitoring and Accountability

1. The agency reserves the right to monitor all usage of agency-owned or managed technology resources.
2. Audit logs, system alerts, and usage reports may be used to enforce policy compliance.

F. Training and Support

1. Mandatory security awareness and acceptable use training must be completed by all employees upon onboarding and annually thereafter.
2. Additional training is required for specialized roles with elevated access.
3. Technical support and guidance will be provided by the Department of Corrections Service Desk to ensure secure and compliant use of agency technology resources.

IV. ENFORCEMENT

Any use of department technology not explicitly authorized by this policy is considered unacceptable use. Failure to comply with this policy may lead to disciplinary action, including dismissal and possible legal proceedings.

V. IMPLEMENTATION

This policy will be adopted immediately without further modification.

Certified: __signature on file_____
Julie Vaughn, Rules Coordinator

Approved: __signature on file_____
Michael Reese, Director