	DEPARTMENT OF CORRECTIONS **Information Technology Services**	
Title:	**Agency Mobile Devices**	**DOC Policy: 60.3.3**
Effective:	**10/6/25**	**Supersedes: 8/5/22**
Applicability:	**All Users of Oregon Department of Corrections Mobile Device Assets**	
Directives Cross-Reference:	**ORS 162.305 Tampering with Public Records** **ORS 192 — Records; Public Reports and Meetings** **DAS Policy 107-004-050 Information Asset Classification** **DOC Policy 10.1.9 Public Records Management** **DOC Policy 60.1.1 Acceptable Use of Information Technology** **DOC Policy 60.3.1 Information Technology Asset Management**	
Attachments:	**None**	

I. PURPOSE

The purpose of this policy is to establish required guidelines for the proper security, configuration, management, and acceptable use of mobile devices owned, leased, or otherwise under the control of the Oregon Department of Corrections.

II. DEFINITIONS

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

B. Agency Mobile Device: Any device meeting the definition of Mobile Device in this policy that has been purchased and provided by the Oregon Department of Corrections.

C. Functional Unit Manager: Any person within the Department of Corrections who reports either to the Director, an Assistant Director, or an administrator, and who has responsibility for the delivery of program services or the coordination of program operations. In a correctional facility, the functional unit manager is the superintendent.

D. Messaging: Text- or image-based communications between or among computers or mobile devices over a physical, wireless, or cellular network. Messaging includes Short Message Service (SMS) or texts, Multimedia Messaging Service (MMS) or texts with an attach file, Rich Communication Services (RCS) messaging, Apple iMessage, Skype, and Microsoft Teams. For the purpose of policy, video-based communication is not included in this definition.

E. Mobile Device: A portable computing device that can easily be carried by a single individual, is designed to operate without a physical connection, possesses local data storage, and includes a self-contained power source.

F. Mobile Device Management (MDM): Centralized administration and control of mobile devices specifically including cellular phones, smart phones, and tablets. Management includes the ability to configure device settings and prevent a user from changing them; remotely locating a device in the event of theft or loss; and remotely locking or wiping a device. Management also includes distribution of software and updating installed software.

G. Non-Agency Mobile Device: Any mobile device that has been purchased or provided by an entity other than the Oregon Department of Corrections.

H. Privileged Information: Criminal Justice Information (CJI) as defined in DOC Policy 60.1.1 Acceptable Use of Information Technology and non-CJI that is classified as Level 3 (Restricted) or higher per Department of Administrative Services Policy 107-004-050.

I. Qualified Need: A documented business or medical necessity, certified by the employee's functional unit manager or medical provider, for which no reasonable alternative exits.

J. Third-Party Account: A user account, not provided by the Department of Corrections, which is used to access a service.

K. Wearable Technology: Consists of devices that can be worn and contain information technology. Examples of wearable technology are fitness trackers, smart watches, and smart glasses.

III. POLICY

A. Device Usage

1. General

   a. Mobile devices are issued solely for official Department of Corrections business. Their use is a privilege and may be revoked without notice.

   b. Users should have no expectation of privacy when using agency devices. All data stored or transmitted on agency devices is subject to audit and may be disclosed in response to public records requests under ORS 192.

   c. The possession of an agency mobile device does not automatically entitle the employee to additional compensation. Policies and practices related to compensation are provided by the Employee Services Division or the employee's manager.

2. Acceptable Use of Agency Mobile Devices

    a. All users with an agency mobile device must adhere to the acceptable use standards in the department's policy on Acceptable Use of Information Technology (DOC Policy 60.1.1).

    b. Employees, contractors, and volunteers are responsible for exercising good judgment regarding the reasonable usage of agency mobile devices and their capabilities.

3. Unacceptable Use of Agency Mobile Devices

    a. Installing software outside of the processes defined by Department of Corrections Information Technology Services.

    b. Using agency mobile devices to access public message boards or social media without prior, signed authorization from the Department of Corrections Communications Unit Manager or designee.

    c. Unauthorized distribution of state data and information.

    d. Circumventing any security features of the device or preventing software updates from installing.

    e. Allowing another person to handle or use the device while unlocked for reasons other than:

        A. The support of the device as performed by Department of Corrections Information Technology Services;

        B. The investigation of the device as performed by Department of Corrections Special Investigation Unit; or

        C. Other approved uses of the device as documented in processes, procedures, or knowledge base articles.

    f. Conducting activities for political or religious causes, or any activity meant to foster personal gain.

    g. Any use of the device for purposes that are unlawful, disruptive, or contrary to Department of Corrections policy.

4. Third-Party Accounts

a. Third-party accounts must not be associated with agency mobile devices.

b. Any third-party account found to be associated with an agency mobile device may become discoverable during an investigation or public records request.

c. Continued use of third-party accounts on agency mobile devices by a user will result in loss of privileges and the agency mobile device will be confiscated.

5. Bluetooth Services

a. Except for items listed in this policy under Allowed Devices,:

A. Use of non-agency Bluetooth devices without an approved, qualified need is forbidden; and

B. Bluetooth services must be turned off when not in use.

b. If a user has an approved, qualified need to connect an agency mobile device to a non-agency Bluetooth device, they must:

A. Acquire written authorization from their functional unit manager;

B. Submit a request to the Department of Corrections Service Desk; and

C. Receive authorization from the Department of Corrections Information Security Office.

c. Allowed Devices

A. The following devices are allowed for Bluetooth connectivity to agency mobile devices:

i. Wireless Bluetooth communications devices such as earbuds or headsets; and

ii. Vehicle communication or navigation systems with data sharing (contacts, text, etc.) disabled.

B. Additions to the list of allowed devices must be reviewed and approved by the Assistant Director of Operations or designee and the Assistant Director of Administrative Services or designee.

6. Audio and Video Services

a. Audio and video capturing services on agency mobile devices must only be used for official Department of Corrections business requirements.

b. Use of the camera feature, including video, is prohibited in areas displaying, storing, or transmitting confidential information including personally identifiable information (PII) or personal health information (PHI).

B. Device Management

1. Only devices provided by Department of Corrections Information Technology Services which have appropriate approvals will be made available to users.

   a. Requests for agency mobile devices must be submitted through the Service Desk.

   b. Contract Workers must provide justification within the submission to the Service Desk demonstrating the need for an agency mobile device to effectively perform the duties of their position.

   c. Tablets are available for limited, special-use cases that are evaluated individually by the Department of Corrections Information Security Officer or designee. If there is already a solution in place that would satisfy the use case, that solution will be used in lieu of a tablet.

2. The Department of Corrections will implement a Mobile Device Management solution to configure and manage all agency mobile devices.

   a. Information Technology Services will manage all mobile software through the Mobile Device Management solution. Unapproved software will be removed without notice.

   b. Users with an approved qualified need for non-standard software must submit a Service Desk request.

3. Per the department's policy on Information Technology Asset Management (DOC Policy 60.3.1), devices must be:

   a. Used as long as practicable and supported by the manufacturer; and

   b. Returned to Information Technology Services personnel when the device is no longer needed or has not been used for a period of 30 days. An exception may be requested through the Service Desk if the user is going to be on a planned leave of absence extending beyond 30 days.

4. Maintenance

a. All broken, damaged, or malfunctioning agency mobile devices must be reported to the Service Desk for repair.

b. Agency mobile devices that cannot be repaired will be submitted for e-waste or destruction and a replacement device will be provided.

C. Device Security

1. Security Configuration

   a. All agency mobile devices will be equipped with a secure configuration developed in accordance with state and federal regulations, guidelines, and policies.

   b. Attempts to bypass security configurations on an agency mobile device will result in loss of privilege and the agency mobile device will be confiscated.

   c. Mobile devices, including software, services, and connections, must only be used by authorized Department of Corrections employees.

2. Passwords and Personal Identification Numbers (PINs)

   a. All agency mobile devices must be protected by a password or PIN that complies with or exceeds the department's standards for complexity.

   b. Password and PIN requirements will be configured by the agency's Mobile Device Management solution.

   c. Users are required to provide Department of Corrections Information Technology Services with the passcode to unlock the device when exchanging or relinquishing a device.

3. For asset-recovery or incident-response, location services will be enabled and logged for all agency mobile devices.

4. Hot Spots

   a. Hot spot (also known as connection sharing) use is for temporary connectivity and not to be used as the primary method for connecting Department of Corrections systems.

   b. Hot spots on agency mobile devices must:

      A. Utilize a secure password that is at least 14 characters long and requires uppercase letters, lowercase letters, numbers, and at least one symbol;

B. Not be used within the secure perimeter of a Department of Corrections institution unless the regularly provided Department of Corrections Ethernet and Department of Corrections Wi-Fi are inoperable;

C. Only be utilized to connect Department of Corrections equipment to the Internet; and

D. Be disabled when not in use.

5. Patch Management

   a. Software upgrades and security patches must be applied in a timely manner.

   b. Repeated failure to install software upgrades and security patches will result in loss of privileges and the agency mobile device will be confiscated.

6. Agency mobile devices must be configured to disable automatically after 10 unsuccessful password attempts or when reported lost or stolen.

7. User Security

   a. Users will ensure agency mobile devices are locked or turned off whenever the device is unattended for any length of time.

   b. Users will not share their password or PIN, except as outlined in this policy.

   c. Users will not allow adults in custody to view agency mobile device screens for any reason.

   d. Lost or stolen agency mobile devices must be immediately reported to the employee's direct supervisor and the Service Desk.

8. Inactivity

   a. Devices must be set to lock after a maximum of 3 minutes of inactivity.

   b. Devices must not be left unsupervised while on Department of Corrections property or during work hours.

D. Data Security

1. Requirements

a. Information Technology Services will maintain a list of approved, enterprise-level applications for remotely transmitting, accessing, processing, or storing privileged information.

b. Users will not:

A. Use an agency mobile device to transmit Department of Corrections data to unauthorized recipients;

B. Store privileged information locally on the agency mobile device; or

C. Transmit, process, or access privileged information using an agency mobile device, except from within approved, enterprise-level applications.

2. Data Retention

a. Public Records

A. All data on agency mobile devices are state data and public record.

B. Users must be aware of state and Department of Corrections retention schedules and the department's policy Public Records Management (DOC Policy 10.1.9) when utilizing an agency mobile device for the storing of any data such as pictures, audio, video, files, messages, etc.

b. Deletion of Data

A. Per ORS 162.305, it is a Class A Misdemeanor to knowingly destroy, conceal, remove, or falsely alter a public record without lawful authority.

B. Routine deletion is permitted after the data has been moved to agency approved storage locations in compliance with retention schedules.

3. Messaging

a. All text messages are automatically captured in record repository.

b. Acceptable uses of text messaging are:

A. Providing a status on location;

B. Requesting a call or meeting; and

C. Discussing a publicly known, agency-related subject without the use of private information.

c. Agency provided email and instant messaging systems must be used instead of text messaging when conducting official business.

E. Non-Agency Wearable Technology: See the department's policy on Non-Agency Mobile Devices (DOC Policy 60.3.4).

IV. IMPLEMENTATION

This policy will be adopted immediately and without further modification.

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.

Certified: _____signature on file_____
Julie Vaughn, Rules Coordinator

Approved: _____signature on file_____
Michael Reese, Director