DEPARTMENT OF CORRECTIONS

Information Technology Services

Title:	**Mobile Device Technology and Management**	**DOC Policy: 60.3.3**
Effective:	**8/5/22**	**Supersedes: Renumbered from 60.1.9 dated 9/6/19**
Applicability:	**All employees and all users of Oregon Department of Corrections Assets**	
Directives Cross-Reference:	**DOC Policy 60.1.1 Acceptable Use of Oregon Department of Corrections Computing Devices and Information** **DOC Policy 70.1.3 Criminal and Administrative Evidence Handling** **DOC Policy 30.3.4 Procurement Policy**	
Attachments:	**None**	

I. PURPOSE

The purpose of this policy is to establish a unified process for proper security, configuration and acceptable use standards concerning mobile devices, data, information, and the management of those mobile devices at the Department of Corrections (DOC).

II. DEFINITIONS

A. Data: Information in raw or unorganized form that refers to or represents conditions, ideas, or objects.

B. Data-at-Rest: When information is residing on the device with no active movement passing through the network.

C. Data-In-Transit: When information is being actively moved from one location to another.

D. Department Computing Devices: All electronic information devices, interconnections, and technical information of the department. Examples of systems include, but are not limited to:

1. Computers, printers, copiers, recorders, transmitters, data telecommunications connections and any similar connected devices.

2. All portable devices such as cell phones, smart phones, tablets, MP3 players, and any other devices as defined by the department.

3. Networking devices includes routers, switches, VPN concentrators, or any device interconnecting networks.

4. Large scale information systems which provide services to the department such as logon access, file servers, data warehousing, web access, web hosting, mail, and instant message services.

5. Applications such as Corrections Information System (CIS), Integrated Supervision Information Systems (ISIS), iSeries (DOC400), or any other systems accessed by or through these systems or systems devices. Methods include, but are not limited to, the internet, Internet Service Providers (ISP) and DOC hosted connections.

E. In-Application Purchasing: Extra content or subscription-based functionality purchased for applications previously downloaded.

F. Information: Information is data or knowledge that is transmitted, analyzed, edited, or reproduced in department systems by electronic, printed, written, verbal or media transmission means. Examples include, but are not limited to:

1. Documents, reports, statistics, files, records, and logs compiled or stored on DOC computing devices or applications.

2. E-mails or messaging system conversations and their attachments.

3. Audio and video files.

4. Images such as graphics, pictures, and photographs.

5. Programs (such as CIS (DOC400), ISIS, WebLEDS, etc.), software and macros.

6. Text and data.

G. Mobile Device Management (MDM): A management solution through software (either local or cloud-based) that provides policy, security or service management, software distribution or inventory collection.

H. Personal Identification Number (PIN): A sequence or pattern of characters (letters, numbers, special symbols) used to validate access to a device or application.

I. Publishing: Utilizing computing devices to create, edit, and disseminate information for use by department employees, contractors, volunteers, third party, and external entities (i.e., other state agencies and their employees, State of Oregon residents, cloud solution providers, etc.).

J. Rooting: The process of gaining access to the core operating system's central system and system files with the ability to change functionality and security of the mobile device.

K. Secured Public Wireless Access Point: A viewable internet connection which requires authentication in order to be granted internet access.

L. Unsecure Public Wireless Access Point: A viewable internet connection which requires no authentication to be granted internet access.

M. Wearable Technology: Refers to electronic technologies or computers that are incorporated into items such as clothing, or accessories which can be worn on the body. There are two types of wearable technologies:

1. One-way communication wearables: Wearable device that cannot send external information, cannot receive data, cannot make phone calls, or connect to the internet. In order to do so this wearable device must be physically connected to another device to transmit data.

2. Two-way communication wearables: Wearable device that can send data, receive data, make phone calls, and connect to the internet without being connected to another device.

III. POLICY

A. User Security

1. Users must comply with all applicable policies (i.e., DOC, DAS, State-level) when using department-owned mobile devices.

2. Users of department-owned mobile devices understand that all actions performed on such devices are monitored and there is no expectation of privacy.

3. Department users must maintain reasonable physical control of department-owned mobile devices at all times.

4. Users shall not allow non-DOC individuals or unauthorized DOC employees to maintain or use department-owned mobile devices.

5. Mobile device users shall not remove the MDM agent from department-owned mobile devices.

6. Department users shall not download non-approved software on department-owned devices.

7. Users cannot transfer department mobile devices between employees without first obtaining approval through management and Information Technology Services (ITS) for transfer of ownership in the departments MDM solution.

B. Mobile Device Acceptable Usage

1. All users assigned a DOC-owned mobile device must adhere to the acceptable use standards in DOC Policy 60.1.1, Acceptable Use of Oregon Department of Corrections Computing Devices and Information.

2. Users must sign the Device Agreement and Statement of Responsibility Guidelines on the back of the DOC form CD1503, Oregon Department of Corrections Wireless Communications Device Order/Change Form prior to initiating the purchase request process or utilizing a mobile device.

C. Wearable Technology

1. Wearable technology that is personally purchased, owned, and has two-way communication capabilities is not authorized to connect to department-owned mobile devices or be worn while inside department correctional institutions.

2. Wearable technology that is department or state-sanctioned, such as a state provided insurance wellness initiative device (i.e., pedometer), is allowed as long as it has one-way communication only.

D. DOC Mobile Device Hardware Acquisitions

1. Department users must make requests for new mobile devices through proper supervisory channels according to business need and discretionary approval.

2. All department-owned mobile devices will either include a purchased case or be issued with a protective case, to be included in the total cost of the device. ITS Telecommunication staff will ensure the case provides adequate protection to limit potential damage to the mobile device.

3. All mobile device and accessory purchases must use authorized suppliers and follow DOC policy 30.3.4, Procurement.

E. DOC Mobile Device Application Acquisitions

1. Department users must make requests for new mobile device applications through proper supervisory channels according to business need.

2. To request non-standard mobile applications, users must fill out a Non-Standard Application Request Form and have their manager sign the document.

3. New non-standard mobile application requests must be reviewed for potential risk to department assets and network.

4. Applications must not use passwords that are transmitted in clear-text format, or any easily reversible format locally stored on the mobile device.

5. All free and purchased mobile applications must be registered through the department's MDM solution for proper distribution and license tracking.

6. Business units will be responsible for additional fees incurred beyond purchasing the original application to gain additional functionality (In-Application Purchasing).

F. Mobile Device Management Registration

1. Department-owned mobile devices and users must be registered and provisioned in the department approved MDM solution.

2. Device registration and provisioning process must be followed as defined in approved TSA documentation.

G. Mobile Device Security

1. Mobile Device Security Configuration Settings

   a. Department-owned mobile device security configuration must be approved by the Chief Information Officer and implemented by the department MDM Administrator.

   b. The Security Configuration Settings must be reviewed at least once annually, when changes to the Security Configuration Settings are requested, or when the department MDM solution is upgraded.

2. Mobile Device Maintenance

   a. All department-owned mobile devices must be upgraded to the latest version of mobile operating system after testing and approval of the update by Information Technology Services (ITS).

   b. All department-owned mobile devices must comply with department password and personal identification number (PIN) requirements.

   c. Department-owned mobile devices must be connected to State of Oregon provided wireless access points. If state-owned access points are not available, users must connect to a password protected wireless access point.

   d. Department-owned mobile devices must not connect to unsecure public wireless access points known as "hotspots".

   e. Devices must not be wirelessly or physically connected to any port on DOC computing devices, except for the transfer of photos and files from authorized mobile devices to the computing device.

   f. Users shall not circumvent department security configurations by modifying the operating system, known as "rooting or jailbreaking the device".

H. Data Security

1. All department-owned mobile devices shall have disk encryption enabled during data-in-transit or data-at-rest.

2. Level 3 and Level 4 data as defined in the DOC Records Retention and Information Security Classification Schedule, shall not be downloaded or stored on department-owned mobile devices.

I. Information Security Incident Management

1. Lost or Stolen Mobile Devices

    a. When a Department mobile device user loses their device or becomes aware that it may be stolen, they must report the incident to their Functional Unit Manager, their site Technical Support Analyst, and the Information Security team via e-mail at dlitssecurityconfidential@doc.state.or.us immediately.

    b. The Information Security Office will determine the severity level of the incident once it is identified.

    c. The Technical Support Analysts will execute the process of wiping the device.

    d. Help Desk, once notified, will initiate suspension of device use with the mobile carrier.

2. Damaged and Returned Mobile Devices

    a. When a department mobile device is damaged, the user will return the mobile device to their local Technical Support Analyst for either repair, recycle, excess, or reuse.

    b. Any mobile user returning a device that is damaged and is found to be negligent in handling their mobile device may be subject to disciplinary action.

    c. When a department mobile device is no longer required for any reason, the user will return the mobile device to their local Technical Support Analyst for either recycle, excess, or reuse.

    d. Technical Support Analysts will execute sanitizing the device before removing the device from inventory. The only exception is when the device is pulled for investigative purposes.

J. Investigation Requests

1. ITS Security will assist in investigative inquiries as requested by functional unit managers, Employee Services, or the Special Investigations Unit (SIU). Functional unit managers should work with Employee Services, SIU, or both when making an investigative inquiry request.

2. All requests must be sent to ITS Security via email at dlitssecurityconfidental@doc.state.or.us to initiate the investigative inquiry request for final CIO or designated representative approval. ITS Security staff will accomplish all requested tasks based on both the request and information available. Once completed, ITS Security staff will notify either Employee Services, SIU, or both and provide the location where the information is stored.

3. All investigative inquires must be as specific as possible; period of time to review and content requested are two examples. ITS may not have all the information requested due to vendor storage limitation or data loss.

4. In the event that an Employee Services or SIU investigative inquiry divulges criminal behavior or violation of the law, ITS Security will halt the investigation immediately. ITS Security will work with the Special Investigation Unit and follow policy 70.1.3, Criminal Evidence Handling.

IV. IMPLEMENTATION

This policy will be adopted immediately and without further modification.

Certified: _signature on file_____
Julie Vaughn, DOC Rules Coordinator

Approved: _signature on file_____
Heidi Steward, Acting Director