OREGON DEPARTMENT OF FISH AND WILDLIFE POLICY
Information Services Division

Title:	Mobile Computing Devices	ISD_610_03
Supersedes:	Mobile Communication Devices dated March 1, 2020	
Applicability:	This policy applies to all employees, contractors, consultants, volunteers, temporary workers, and other users at the Oregon Department of Fish and Wildlife, including those users affiliated with third parties who access the department's network or network services.	
Reference:	ISD_610_01 Acceptable Use of State Information Assets ISD_630_01 Security of Information Systems ISD_640_01 Information Technology Lifecycle	
Effective Date:	Jan 1, 2024	**Approved:** 

I. PURPOSE

The purpose of this policy is to provide expectations of use for state-owned smartphone, tablet, or other hand-held portable devices collectively known as Mobile Computing Devices (MCDs).

II. DEFINITIONS

A. **Confidentiality:** A security principle to ensure information is accessible only to those authorized for a specific intended purpose.

B. **Hands-free:** An add-on attachment or built-in feature (temporarily or permanently installed) that enables a person to keep both hands free to perform other duties while operating the MCD.

C. **Mobile Computing Device (MCD):** A portable electronic device (typically handheld) that can perform similar functions as a computer through use of an operating systems and application code. May also include specialized functions for communications and geographic location.

D. **Sensitive Information**: Any information where the loss, misuse, modification, or unauthorized access would adversely affect the interest of the agency, or the privacy individuals.

E. **Smartphone:** A handheld device that integrates mobile phone capabilities with the more common features of a handheld computer or PDA, including access to Internet, email, and calendar.

F. **User:** All state employees (and their agents), volunteers, vendors and contractors, including those users affiliated with third parties who access state information assets, and all others authorized to use state information technology for the purpose of accomplishing the state's business objectives.

III. POLICY

Mobile Computing Devices (MCDs) are any portable electronic device (typically handheld) that can perform similar functions as a computer through use of an operating systems and application code. They are considered an extension of the agency computer network and therefore subject to all existing policies and practices as other computing devices. This policy provides additional considerations that are unique to the operations of MCDs within the agency.

A. Physical Security

MCDs must be adequately protected to prevent damage or loss as they are more likely to be broken, misplaced, or stolen while in use. Environmental protection cases or security cables should be considered. In addition, protective measures are necessary to avoid exposure to extreme temperatures, direct exposure to sunlight, rain, or other harsh environmental conditions unless designed or adapted for these conditions. MCDs must be adequately secured during transport and properly stored when not in use.

B. Passwords/PIN/Biometrics

Use of a password or other locking methods is required for all MCDs to secure the device when not in active use unless an exception has been approved by the Information Systems Division (ISD). User authentication with MCDs (password strength, complexity, renewal) must comply with current agency and state security standards although the device itself may not have the capability to enforce the requirements.

Shared MCDs require unique and individual accounts specific to each user unless a standard operating practice or an exception has been approved by ISD.

Shared MCDs that are based on an Android or Apple operating system and configured to function within a work group (e.g. data collection) may have only one method of authentication or locking the device. In these specific situations, sharing of the passcode (or other method) among the users to secure the device is permitted under this policy.

C. Data Security

At no time shall a MCD store or transmit documents of asset classification L3 'Restricted' or L4 'Critical' unless the device uses an encrypted technology approved by ISD that secures the information in transit and at rest.

Information with an asset classification of L2 'Limited' may also be restricted from use with any MCD as determined by the information asset owner.

Only updates provided by the device service provider/manufacturer or those approved by ISD are allowed. No modification ('jailbreak', 'hijacking') to the MCD operating system, applications, or physical device is permitted.

D. **User Configuration**

Users may adjust any device settings that are intended for the normal and typical operation of the MCD by the user. For example, the brightness, volume, and screen layout.

However, users may not modify any system configuration settings that provides network access, security, account management, or usage logs.

E. **Software Applications or Cloud Services**

Prior to the use of any new application or cloud service, a request must be submitted for review to ISD. Per state policy, a determination will be made if the cloud application or service requires a review by contract services and/or requires the completion of the Enterprise Information Services (EIS) cloud readiness workbook. Certain risk thresholds will require additional approval by Division of Administrative Services (DAS)/EIS per statewide policy.

The purpose is to identify any potential business impacts related to product licensing, compliance to terms and conditions, system compatibility, security compliance, and other operational standards that represents a risk to the state.

ISD has pre-approved certain applications and cloud services for general use within the agency. These may be found in the Oregon Department of Fish and Wildlife (ODFW) application store or documented on the Software Account Management (SAM) application.

F. **Legal and Standards Compliance**

The use of any MCD and associated applications and cloud services must comply with all applicable laws, policies, procedures, and operational standards that are specific or unique to mobile computing such as, but not limited to, laws pertaining to use while driving and Mobile Device Management (MDM) security features.

G. **Safe Use**

Users are responsible for using MCDs in accordance with agency safety practices in addition to national and state laws. Observe safe practices while using MCDs such as hands-free operation or by temporarily pausing other activities. At no time shall the user operate the MCD so it becomes a safety hazard or distraction to the user or other persons.

H. **Reporting a Lost/Stolen Device**

Lost devices or stolen MCDs must be reported in accordance with the 'Incident Reporting' section of ISD_610_01 'Acceptable Use of State Information Assets'. Failing to report can result in a significant risk to the agency.

I. **Battery Maintenance**

Users shall practice appropriate safety protocols throughout the lifecycle of the MCDs to prevent battery failure, fire, or explosion. Batteries should be charged only as instructed by the manufacturer. Never charge a device that is hot or overheated until it has cooled. Never

attempt to charge a device or battery that has been damaged. Properly dispose of Lithium-Ion batteries using a certified recycler, do not discard in trash.

J. **Mobile Device Management**

The deployment of any MCD will include Mobile Device Management (MDM) software to provide additional security features, allow remote update to the device, and provide other administrative support functions. Users shall not alter attempt to alter or disable any MDM functions.

K. **Exclusions**

Certain small portable electronics do not process or store data and are not considered MCDs under this policy. These are highly dedicated devices typically designed for very specific business purpose that includes, but not limited to, emergency locators, two-way radios, or remote equipment controllers.

L. **Exception Process**

Exception requests can be submitted to the ISD administrator, or ISD deputy, when standard configurations for MCDs may limit business use or otherwise restrict the use of certain functions or access to information. Exceptions must be approved and documented in writing prior use.

IV. POLICY GROUP

This policy is part of a suite of Information Technology policies that collectively sets the expectations and use of computing devices and related technologies under the main policy ISD_610_01 'Acceptable Use of Information Systems'.