OREGON DEPARTMENT OF FISH AND WILDLIFE POLICY
Information Services Division

Title:	**Mobile Communication Devices**	**ISD_610_03**
Supersedes:	None	
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 that have been issued a cell phone that has access to Internet, other computers, or has the ability to access or store agency data.	
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:	**March1, 2020**	**Approved:** Erica Klewer

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 (whether or not 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 hand held) 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.

III. POLICY

Mobile Computing Devices (MCD) are considered an extension of the agency computer network and therefore subject to the existing policies and practices as other computing devices. This policy provides additional considerations that are unique to the operations of MCD's within the agency.

A. Physical Security

Due to their small and portable design MCDs are more likely to dropped, damaged, lost, or stolen while in use. 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. Environmental protection cases are recommended and some MCDs may require a security cable and lock.

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. User authentication with MCDs (password strength, complexity, renewal) must comply with current security standards although the device may not have the capability to enforce the requirements.

All users shall have and use a unique login and authentication (password/pin/biometric) for any MCD. A single device may have multiple user accounts as long as it is logged out prior to use by another employee.

The standard exception to the required use of authentication is if an MCD device does not have the capability to support such features (e.g. simple on/off only).

C. Data Security

Data stored on or transmitted by a MCDs must be of asset classification L1 'Published' or L2 'Limited' only. 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 the Information Systems Division (ISD) that secures the information in transit and at rest.

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

D. User Configuration

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

E. Application Downloads

A modified cloud readiness assessment process is required prior to purchase or use of smartphone applications that is commensurate to the risk factors associated within mobile devices.

The use of smartphone apps must comply with all applicable laws, policies, procedures, and standards including without limitation: privacy laws and regulations, statewide and agency specific IT security policies, internal audit controls, risk management standards, and records management standards.

The cloud readiness assessment must be approved by the Information Systems Division and as applicable Enterprise Information Services. The purpose is to identify any potential business impacts and risks that includes confidentiality, business continuity, service management, incident management, change management, records management, intellectual property rights, data ownership, audits, and controls.

F. **Mobility Restrictions (as applicable)**

Employees are responsible for using MCDs in a safe practice in accordance with agency policies and safety practices in addition to national and state laws. Observe safe practices such as hands-free operation or by temporarily pausing other activities to use the MCD. At no time shall use of the MCD become a distraction that creates an unnecessary risk to the employee or other persons.

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

Lost devices or stolen MCDs can result in significant security concerns for the agency. Promptly follow the established procedures as you would for any computing devices. Reference the 'Incident Reporting' section of ISD_610_01 'Acceptable Use of State Information Assets' for additional information.

H. **Breach of Security**

Any breach of security (perceived or real) must be promptly reported the Information Systems Division within 1 hour to maintain data security and for a vulnerability assessment to be made by the InfoSec committee.

I. **Maintenance**

Batteries should be charged as instructed by the manufacturer to prevent premature battery failure, fire, or explosion. Never charge a device that is hot or overheated until it is cooled first. Never attempt to charge a device or battery that has been damaged.

J. **Mobile Device Management (where applicable)**

The deployment of any MCD will include Mobile Device Management software to provide additional security features, allow remote update to the device, and provide other administrative functions.

K. **Monitoring and Compliance**

The state owns all legal rights to inspect, monitor, control, transfer, or limit use of an MCD operated by the agency at any time.

L. **Asset Management**

The Administrative Services Division is the final authority for agency asset records and controls including those MCDs that meet the reporting threshold. Due to large variety of devices that are MCDs, not all devices are centrally tracked. However, as any state asset, the agency divisions are responsible for establishing proper asset controls.

M. **Lifecycle and Support**

The lifecycle for any device is determined by the expected useful life considering the overall cost of operation and business efficiencies including increasing failure rates, interoperability

issues (system to system), declining vendor support, high operating costs, security vulnerabilities, and other significant factors that place business operations at risk.

The device lifecycle is considered fully expired, regardless of age, when the product no longer has main stream support, has exceeded extended support, security patches are no longer made available, or is not compatible with other systems or software.

See policy ISD_610_04 'Information Technology Lifecycle' for additional information.

N. **Exclusions**

For the purpose of this policy, certain small portable electronics are not considered Mobile Computing Devices (MCDs). These are highly dedicated devices typically designed for a special purpose that include, but not limited to, emergency locators, two-way radios, or remote equipment controllers.

O. **Exception Process**

MCDs have a wide range of design, purpose, and uses. In addition, they also have limited configuration options as compared to a standard computer. As such, standard configurations for MCDs may restrict or prevent the use of certain functions or access to information. Exception requests can be submitted to the Information Systems Division administrator (or ISD deputy). 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 technology, and falls under the principle policy ISD_610_01 'Acceptable Use of State Information Assets'.