STATE OF IDAHO
DEPARTMENT OF
ENVIRONMENTAL QUALITY

1410 North Hilton • Boise, ID 83706 • (208) 373-0502

C. L. "Butch" Otter, Governor
John H. Tippets, Director

DEQ POLICY STATEMENT
PS18-08

POLICY FOR MOBILE DEVICES

PURPOSE

Mobile devices provide safety and efficiency advantages, flexibility, and convenience for Idaho Department of Environmental Quality (DEQ) employees. The devices also pose risks to state data security, create potential for infection from viruses, and therefore, require high standards of accountability.

This policy establishes acceptable use, security, and confidentiality requirements for using mobile devices when conducting official DEQ business. Information stored on mobile devices or those accessing DEQ's network may be subject to audit, public records requests, or other legal processes such as discovery and subpoena.

STATEMENT OF POLICY

This policy applies to all DEQ employees using mobile devices purchased by DEQ or used to store or access DEQ data. The Idaho Technology Authority (ITA) establishes statewide information technology and telecommunications policies, standards, guidelines, and conventions and comprehensive risk assessment criteria for Idaho.

The following ITA policies and guidance apply to DEQ mobile device use:

- P4550—Mobile Device Management
- P1040—Employee Electronic Mail and Messaging Use
- P2120—Electronic Mail–Messaging
- P1050—Employee Internet Use
- P1060—Employee Personal Computer Use
- P4530—Cleansing Data From Surplus Computer Equipment
- G540—Mobile Devices
- G550—Cleansing Data From Surplus Computer Equipment
- G560—Passwords

This mobile device policy applies, but is not limited, to all devices and accompanying media in the following classifications:

- Laptop, notebook, and tablet computers
- Mobile and cellular phones

- Smartphones
- Personal digital assistants

Employees using mobile devices not purchased by DEQ (personal devices) but used to store or access DEQ data must sign a user agreement and comply with the mobile device security provisions of this policy.

POLICY AND APPROPRIATE USE

DEQ employees may request appropriate mobile devices to meet the agency's on-the-job communication needs. Not all DEQ positions warrant the use of mobile devices. If mobile devices are necessary, minimum standards must be complied with during use. To determine whether a DEQ-provided mobile device is necessary and to establish standards and requirements for using such devices, the guidelines below shall apply.

Eligibility

Requests for new mobile devices and service contracts must be approved by a supervisor (at minimum) using the Mobile Device Request Form before submitting to the director for final authorization. Eligibility considerations include the following:

- Senior management—May be expected to respond to work-related messages beyond normal working hours.
- Program or regional managers—May be required to provide immediate responses to senior management.
- Emergency responders—On call as part of the state's emergency response plan.
- Critical systems support personnel—Need to provide after-hours or crisis response support.
- Safety personnel—May be subject to health and safety risks.
- Highly mobile employees—Frequent travelers whose productivity can be enhanced by mobile device use.

Contracts and Equipment

All mobile device service contracts will be managed by Facilities Management in the State Office under the following guidelines:

- New service contracts and upgrades must be approved by the director (or director's designee) using the Mobile Device Request Form.
- Monthly invoices will be paid by Fiscal using charge codes provided by the staff member to whom the mobile device has been assigned.
- Facilities will keep an inventory of mobile devices currently in use and an inventory of mobile devices turned in.
- Equipment must be returned to Facilities when employees upgrade their phones, leave DEQ, or terminate their service contracts.
- Mobile devices will be reused when possible rather than purchasing new units.
- Cost must be considered when purchasing or upgrading any mobile device, and limits are identified on the Mobile Device Request Form.

- Purchases of carrying cases, screen protectors, chargers, or applications must be approved by the employee's supervisor before the purchase is made.
- Variations from the standard contract/user plan (e.g., additional features such as Mobile Hotspot) must be approved by the director (or director's designee).
- Device upgrades are on a 2-year basis. Lost or broken devices must be replaced with a device that has been returned to inventory or, if no such device is available, the least expensive device available at the time of replacement.

Policies for Use

The primary purpose of state-owned mobile devices is to conduct official DEQ business. Employees may use the device for occasional individual, nonpolitical purposes on personal time, if use does not violate the terms and conditions of this policy, violate any other ITA policy, or interfere with state business.

Any use beyond the following maximum monthly allotments must be justified and relate to work necessary to perform job duties:

- 600 total voice minutes or
- 400 total text messages (applies only to contracts with texting plans) or
- 2 GB data usage (applies only to contracts with data plans)

Any use below the following minimum monthly amounts (in all categories) must be justified; explain why the mobile device is necessary to perform job duties:

- 30 voice minutes
- 10 text messages
- 50 MB data usage

All other state policies and standards relating to internet, email, and equipment use apply to mobile device use. For devices capable of downloading applications, those applications must be consistent with all state usage policies and may not:

- Involve obscene, pornographic, profane, or sexually oriented material
- Be political in nature
- Involve gambling
- Violate any laws or policies

Mobile Device Security Requirements and Standards

All state- and personally owned mobile devices used to store or access DEQ data shall:

- Be password protected by PIN or BIOMETRIC
- Have screen lock and screen timeout functions
- Encrypt files in onboard and removable storage
- Be capable of being erased remotely and disabled if lost or stolen (user must notify DEQ Information Technology within 72 hours)
- Be protected from and scanned for viruses

Additionally, employees are prohibited from the following when using state-owned mobile devices:

- Texting while driving.
- Storing devices in an unsecure location.
- Returning, exchanging, or disposing of devices before all data are erased or otherwise made unreadable.
- Jailbreaking their state-owned mobile devices or otherwise gain root access for modifying a device.

MONITORING COMPLIANCE

DEQ uses Mobile Device Management software to monitor compliance with this policy. The software allows DEQ to remotely enforce all mobile device security requirements and standards and audit application downloads on state-owned devices. DEQ may inspect any and all files stored on mobile devices, on the state network, or any other storage medium used for state business to monitor compliance with this policy.

Facilities will monitor and audit monthly mobile device usage and will notify supervisors monthly about staff who are below minimum and/or above maximum usage levels. Supervisors will be responsible for following up with their staff to request necessary justification.

A DEQ employee can be held accountable for any unauthorized or illegal use of the mobile device as well as any breaches of policy, security, or confidentiality. Such violations of this policy may result in disciplinary action.

RESPONSIBILITY

DEQ's deputy director is responsible for maintaining this policy.

IMPLEMENTATION

This policy is effective immediately and will remain in effect for 5 years unless amended, replaced, or rescinded prior to expiration.

Dated this 19th day of September, 2018

John H. Tippets
Director