

Idaho Technology Authority (ITA)

ENTERPRISE POLICY P4500 – Security – Computer and Operations Management

Category: P4550 – **MOBILE DEVICE MANAGEMENT**

CONTENTS:

- I. [Authority](#)
- II. [Abstract](#)
- III. [Definitions](#)
- IV. [Policy](#)
- V. [Exemption Process](#)
- VI. [Procedure Reference](#)
- VII. [Contact Information](#)
[Revision History](#)

I. AUTHORITY

Authority: Idaho Code § 67-5745(C)(3)

II. ABSTRACT

The purpose of this policy is to ensure that the use of mobile devices does not adversely affect the security of state information.

III. DEFINITIONS

1. Mobile Device: A handheld or tablet-sized computer that is easily carried and which can be used to access business information. These include, but are not limited to, Smartphones, BlackBerry™ devices, Personal Digital Assistants (PDAs), Enterprise Digital Assistants, notebook/netbook computers, Tablet PCs, iPads and other similar devices. This does not include simple mobile storage or memory devices.

2. User: Anyone with authorized access to State business information systems, including permanent and temporary employees or third-party personnel such as temporaries, contractors, consultants, and other parties with valid State access accounts.

3. Screen Lock: Mechanism to hide data on a visual display while the computer continues to operate. A screen lock requires authentication to access the data. Screen locks can be activated manually or in response to rules.

4. Screen Timeout: Mechanism to turn off a device or end a session when the device has not been used for a specified time period.

5. Sensitive Information: For the purpose of this policy, sensitive information includes state e-mail and any information defined as sensitive by any state statute, such as Title 28, Commercial Transactions, Chapter 51, Identity Theft.

6. Jailbreak: The process of modifying firmware or software to bypass security features to gain administrative or unrestricted access to a device.

IV. POLICY

This policy applies to any mobile device, state-owned or personally-owned, which accesses the state network, stores state e-mail or other state information and embodies the minimum requirements that must be met. Agencies may choose to adhere to stricter requirements.

Any employee, who has been allowed to use their personally owned device for work purposes, must sign a user agreement, as shown in Standard S2140, Mobile Device Security Capabilities.

If an agency does not utilize automated enforcement of this policy, they must conduct regular auditing of devices and processes of at least 10% of devices per year to ensure they meet this policy.

Agency directors shall attest to their agency's compliance and provide an outline of the tools used to ensure compliance.

Those devices without capabilities to meet these policies must be replaced by models which can by May 2014, IAW Standard S2140, Mobile Device Management.

- A. All mobile devices must be password protected.
- B. All mobile devices must have screen locking and screen timeout functions enabled.
- C. Implement encryption on all mobile devices.
- D. If a mobile device is lost or stolen or damaged, the device must be wiped remotely and disabled. At a minimum, all state data must be removed.
- E. The physical security of these devices is the responsibility of the employee to whom the device has been assigned. Devices shall be kept in the employee's physical presence whenever possible. Whenever a device is being stored, it shall be stored in a secure place. Users must notify their IT department within 72 hours if a device is lost, stolen, or damaged.
- F. Agencies must develop an internal policy regarding what applications their users are allowed to download and install on state-owned devices.

G. Mobile devices must have software which protects and scans for malicious software on the devices, in e-mail and in downloaded files. This software must have regular updates to maintain best possible protection.

H. As required by P4530 – Cleansing Data from Surplus Computer Equipment, mobile devices must be treated as any other computer before it is returned, exchanged or disposed.

I. Employees must not “jailbreak” their state-owned mobile devices or otherwise gain root access for modification of the device.

J. Employees shall not text while driving a state vehicle.

K. All other ITA Computer Usage, Internet Usage, and E-mail Usage policies apply for those using state-provided devices.

L. A user can be held accountable for any breaches of policy, security, or confidentiality resulting from their use of their mobile device. Such violations of this policy may result in disciplinary action.

V. EXEMPTION PROCESS

Refer to [Policy 1010 – Information Technology Policies, Standards, and Guidelines Framework](#).

VI. PROCEDURE REFERENCE

Refer to [Standard S2140, Mobile Device Management and other references](#)

- [P1040](#) - Employee Mail and Messaging Use
 - [S2120](#) - Electronic Mail - Messaging
- [P1050](#) - Employee Internet Use
- [P1060](#) - Employee Personal Computer Use
- [P4530](#) – Cleansing Data from Surplus Computer Equipment

VII. CONTACT INFORMATION

For more information, contact the Idaho Technology Authority Staff at (208) 332-1876.

REVISION HISTORY

07/01/13 – Changed “ITRMC” to “ITA”.

Date Established: June 27, 2012