# Idaho Technology Authority (ITA)

# ENTERPRISE POLICY P4500 – Security – Computer and Operations Management

**Category: P4550 – MOBILE DEVICE MANAGEMENT**

**CONTENTS:**



## 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. A Mobile Device is further characterized as such if it is not otherwise protected, monitored, or managed by traditional automated enterprise tools used for workstations, servers and other traditional IT systems. This definition excludes simple mobile storage or memory devices.

**2. Simple Mobile Storage or Memory Device:** A device such as a simple mobile phone that is meant for phone communications or a device for use of portable storage such as an external hard drive or USB storage device.

**3. 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.

**4. 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.

**5. Screen Timeout:** Mechanism to lock the screen of a device or end a session when the device has not been used for a specified time period.

**6. Sensitive Information:** Sensitive information includes state e-mail and any information defined as sensitive by any state statute, such as Idaho Code § 28-51 (Commercial Transactions, Identity Theft).

**7. Jailbreak:** The process of removing software restrictions imposed by Apple iOS, by way of running software exploits that permit root access to the file system. This allows the download and installation of additional applications, extensions, and themes that are unavailable through the official Apple App Store.

**8. Root or Rooting:** The process of allowing users of smartphones, tablets, and other devices running the Android mobile operating system to attain privileged control (known as root access) over various Android subsystems.

**9. Industrial Control Systems (ICS):** A generic term used to describe any system that gathers information on an industrial process and modifies, regulates, or manages the process to achieve a desired result. Examples of industrial control systems include: SCADA (Supervisory Control and Data Acquisition), PCS (Process Control Systems), AS (Automation System), SIS (Safety Instrumentation System), or any other automated control system.

**10. Internet of Things (IoT):** An expansion on modern ICS devices to be "smarter". These devices can assume a variety of forms, often with limited or proprietary operating systems, and often serves an individual and well-defined purpose. IoT devices often communicate together in a network, or with internet-facing services to provide "smart" or intelligent capabilities to a system otherwise lacking. These devices may be sensors, aggregators, communication channels, eUtilities, decision triggers, or other primitives; as defined by NIST Special Publication 800-183 "Network of 'Things'". Examples include: sensors such as thermostats, microcontrollers or microprocessors like Arduino or Raspberry Pi, electronic medical implants, and appliances such as "smart" toasters and televisions.

**11. Sideloading:** the process of transferring data between two local devices, in particular between a computer and a mobile device such as a mobile phone, smartphone, PDA, tablet, portable media player or e-reader.Sideloading typically refers to media file transfer to a mobile device via USB, Bluetooth, WiFi or by writing to a memory card for insertion into the mobile device.

**12. Tethering:** Tethering, or phone-as-modem (PAM), is the sharing of a mobile device's internet connection with other wirelessly connected computers. Connection of a mobile phone or tablet computer with other devices can be done over wireless LAN (Wi-Fi), over Bluetooth or by physical connection using a cable, for example through USB. If tethering is done over WLAN, the feature may be branded as a mobile hotspot, which allows the smartphone to serve as a portable router or portable wireless access point for devices connected to it.

**13. Multifactor Authentication Solution:** Method of computer access control in which a user is granted access only after successfully presenting several separate pieces of evidence to an authentication mechanism – typically at least two of the following categories: knowledge (something they know), possession (something they have), and inherence (something they are).

## IV. POLICY

This policy applies to any mobile device, state-owned or personally-owned, which accesses the state network, state email, or accesses, creates, modifies, transmits, stores, or views any state data. Exempt from this policy are devices defined as "Internet of Things" (IoT) devices, industrial control systems (ICS), simple mobile and storage devices, and personally owned mobile devices that use State Multifactor Authentication solutions but in no other way meet the applicability criteria of this policy. Agencies may choose to write stricter interagency policy, and or follow ITA Enterprise Guideline G540 (Mobile Devices) for further reference.

Those devices without capabilities to meet these policies must be replaced by models which can, in accordance with ITA Enterprise Standard S2140 (Mobile Device Security Capabilities).

All mobile devices must be protected with a password, PIN, or biometric authentication method that is enabled to protect data and applications on the mobile device.

All mobile devices must have screen lock and screen timeout functions enabled.

The physical security of a mobile device is the responsibility of the user.

A user must notify their IT department if they discover a mobile device is lost, stolen, or has transferred to another user's responsibly

A mobile device must be protected from malicious software on the device.

A mobile device must also be scanned for vulnerabilities

A mobile device must receive regular updates to software and firmware.

A mobile device must be subject to a Data Loss Policy.

A mobile device must be wiped before it is disposed, returned or exchanged.

Jailbreaking, rooting, or otherwise gaining unauthorized administrative access to the device is prohibited.

Sideloading, tethering, or installing apps from sources other than an app store, is prohibited unless authorized by agency for specific state business requirements. State agency must document these specific authorization justifications.

Any user, to be permitted to use a personally-owned mobile device for work purposes must: a.) receive management approval and b.) sign an agreement indicating their understanding of the increased responsibilities, as well as, the personal and business risks involved in using a personally-owned mobile device during state business. Agencies are free to develop a custom agreement for these purposes; however, a sample is provided in ITA Enterprise Standard S2140 (Mobile Device Security Capabilities).

## V. EXEMPTION PROCESS

Refer to ITA Enterprise Policy P1010 (Information Technology Policies, Standards, and Guidelines Framework).

## VI. PROCEDURE REFERENCE

- ITA Enterprise Standard S2140 (Mobile Device Security Capabilities)
- ITA Enterprise Guideline G540 (Mobile Devices)
- NIST Special Publication 800-183 (Network of 'Things')

## VII. CONTACT INFORMATION

For more information, contact ITA Staff at (208) 332-1876.

## REVISION HISTORY

05/09/17 – Refined scope definitions in Section III; updated Section IV. Policy; updated Section VI. Procedure Reference.

07/01/13 – Changed "ITRMC" to "ITA".

Date Established: June 27, 2012