Idaho Technology Authority (ITA)

ENTERPRISE GUIDELINES – G500 SECURITY PROCEDURES

Category: G540 – MOBILE DEVICES

CONTENTS:

I. 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. Mobile Device are further characterized as such if they are 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 devices.

II. RATIONALE

These guidelines are intended to assist agencies with the growing number of mobile devices in the workplace. The use of mobile handheld devices, such as Personal Digital Assistants (PDAs) and tablet computers within the workplace, is expanding rapidly. These devices are no longer viewed as coveted gadgets for early technology adopters, but instead have become indispensable tools that offer business advantages for the mobile workforce. While providing productivity benefits, the ability of these devices to store and transmit information through both wired and wireless networks poses potential risks to an organization's security. This guideline describes a framework for managing mobile and handheld devices. The approach is aimed at assisting the enterprise in administering policies for PDAs and other mobile devices.

III. GUIDELINE

A. Security Overview

Basic mobile device security policies:

1. Mobile devices connected to agency equipment should be password protected;
2. The wireless port on mobile devices should be disabled when not in use;
3. All mobile devices should have installed anti-virus software;
4. Mobile devices that do not have up-to-date anti-virus software should be scanned for viruses prior to connecting to the agency network;
5. Storing sensitive agency information is not recommended unless it is encrypted; and
6. Mobile devices should have the latest security patches installed on their operating system.
7. Mobile devices are inherently less secure devices; additional measures should be put in place to properly protect sensitive information. See Section G for more details.

B. Physical Security

Users are responsible for maintaining the physical security of their mobile devices. All Mobile devices should be kept out of sight and covered when stored in a vehicle.

Special care should be taken in crowds, meetings and security screening areas to maintain control over the device.

The mobile devices should display contact information so the device can be returned should it be lost. This can be a tag or label on the device.

Notify the appropriate security/network administrator immediately if device is lost, stolen or compromised.

C. Device Security

Any software installed on mobile devices that uses script files should not contain a user ID or password for the State's computer system.

Power-on authentication should be used on all mobile devices.

Devices, when unattended, should have some type of screen saver with password protection or keyboard locking program enabled.

Guidelines for the use of passwords are outlined in “Information Technology Enterprise Guideline G560 - Passwords

Mobile devices should be transported as carryon luggage whenever traveling by commercial carrier unless the carrier requires otherwise.

All mobile devices should be updated with the latest security patches, virus scanning software and virus data files. Patches and updates to virus data files should be installed through an automated process if applicable, and patches for high-risk vulnerabilities should be installed within forty-eight (48) hours of notification of availability.

Whenever available for a mobile device, firewall software should be installed, updated, and used on any mobile device used to connect to the State network from outside of the State (Internet) firewall.

At a minimum it is recommended a remote wipe capability should be used to eliminate state data from lost or stolen mobile devices. A Mobile Device Management solution is advised for automated management of Mobile Devices.

D. Data Security

If highly sensitive or confidential information is stored on a mobile device, the data should be encrypted. Another method to add an additional level of security would be to encrypt the data, store it on removable media, and store the media separate from the device or device case.

Mobile devices should be included in the surplus equipment and disposal lifecycle requirement to ensure all data is permanently removed from these devices before they are returned to the vendor or sent to surplus (See ITA Guideline G550 – Cleansing Data from Surplus Computer Equipment).

E. Communication and User Education

Implementing an effective mobile device policy also requires regular communication with the users. Any changes in the policy, IT provisioning, and support should be communicated to the users, along with short training sessions that allow time for participants to discuss experiences and share information. By both communicating policies and providing feedback mechanisms, mobile devices can be used in the agency safely and efficiently.

User education is critical. Educating the users about best practices, particularly regarding security, can help reduce risks. If properly structured, half-day workshops and shorter online training sessions, that focus on security threats and the actions users can take to protect themselves and the agency, can help reduce security risks. At a minimum, user education programs and policies should:

1. Give users some accountability. Users should be educated on the reasons that they should follow agency policies, not to circumvent or ignore security policies, and to observe common sense precautions.

2. Make it clear what is at stake, including the user's own information. If an agency loses a device with confidential data on it, it can cause problems

with the agency's reputation and customers. Many users also store personal information, such as credit card numbers or other sensitive data, on mobile devices, which gives them additional incentive to protect the information. Losing a laptop or even a PDA can also be extremely disruptive to the user if data is lost or temporarily inaccessible.

3. Give users the necessary tools and easy means to secure the devices. Make certain that tools are available and easy to use. For example, passwords and other authentication mechanisms should be easy to configure and use; encryption, if needed, should occur without unnecessary user intervention or decision-making.

4. Raise awareness by demonstrating real security risks. Training sessions should show users how susceptible mobile devices are to theft and loss and the steps they can take to reduce risks.

F. Agency Policies

Agencies are encouraged to create a more restrictive mobile device policy that fits the needs of the individual agency. Provided below are a few example topics an agency may wish to include in their own policy:

1. Identifying applications their users are permitted to download and install devices

2. Identifying what data is authorized or restricted from mobile devices, to include sensitive information

3. Identifying means of connectivity authorized for use on mobile devices. This may include mobile device connectivity through Wi-Fi, Bluetooth, or the external communication ports on the mobile device.

G. Tiered Mobile Device Management Model

It has been recognized that some agencies may have a business need for a more dimensional or dynamic mobile device management program centered around data as opposed to a device type. If an agency meets all the below requirements, they are permitted to implement this tiered mobile device management model. This tiered model will be accepted as compliant with ITA policy and standards if all requirements are met and the model is implemented.

An agency may, at their discretion, implement a tiered model of security controls across all in-scope mobile devices given the following requirements are met:

1. An agency must have classified all data as per ITA Enterprise Policy P4130 (Information Systems Classification) and ITA Enterprise Guideline G505 (Data Classification and Labeling Guideline)
2. An agency must have technical controls in place to manage and enforce flow of classified data throughout the network and endpoints (e.g. data

loss prevention (DLP), encryption, mobile device management (MDM), etc.)
3. The tiered model must have stricter requirements than those outlined in this policy
4. The tiered model must be data-centric (i.e. the classification of the device is determined by the highest classification of data the user of the device regularly interacts with)
5. An agency must recognize and consider the staffing and resource overhead to properly manage and administer a tiered model for mobile device management as opposed to a "flat" model

Requirements by Classification:

Classification 1: Public

A user of a mobile device in this classification never uses the device for state business and they only interact with openly available websites, documents, or information that do not require a public records request to access. A mobile device in this classification is personally-owned and is only permitted to connect to state-operated networks that are unauthenticated and open to the public. No mobile device management client is required and no policies are enforced on this device.

Classification 2: Limited

A user of a mobile device in this classification regularly interacts with data classified as limited, such as internal email, which may or may not be exempt from public record requests. A mobile device in this classification may be personally-owned or state-owned. A mobile device management client is required to monitor and manage policy enforcement. The following controls must be implemented:

- Device password required
- Enable screen lock and inactivity timeout after 10 minutes
- Device wipe and reset after 10 consecutive incorrect passwords
- Anti-virus software
- Web content filtering
- Encryption of data at-rest (including SD card if present)
- Encryption of data in-transit (where possible)

Classification 3: Restricted

A user of a mobile device in this classification regularly interacts with data classified as restricted, such as technical network or security information, administrator passwords, or personally identifiable information (PII). This classification of information is often exempt from release via public records requests. A mobile device in this classification must be state-owned and

must have a mobile device management client installed. In addition to the lower classification controls, the following additional controls must be implemented:

- Application whitelisting
- Data loss prevention
- Restrict the use of external media, such as SD cards, to only those necessary for operation
- Restrict use of a mobile device from being used as removable storage
- Restrictions and controls on use of synchronization and backup applications (e.g. Dropbox, iCloud, OneDrive, and OneDrive for Business)
- Wireless hotspot and tethering capabilities must be enabled on a per-device basis and only after an appropriate business case has been filed and approved by a supervisor

Classification 4: Critical

A user of a mobile device in this classification interacts with, during normal business, data classified as critical, that if disclosed could result in significant penalties, serious injury, disability, or loss of life. This classification of information is exempt from public record requests. A mobile device in this classification must be state-owned and must have a mobile device management client installed. To ensure the upmost security and confidentiality of critical information, the following controls must be implemented in addition to those in lower classifications:

- Persistent VPN connections on all cellular networks or non-State administered networks
- Restrict wireless networks to only those necessary for operation
- Restrict personal area networks (PAN), such as Bluetooth and near-field communications (NFC), to only those necessary for operation, only when required, and only for the required duration.
- Restrict access to hardware (e.g. cameras, microphones) to only what is necessary for operation
- Wireless hotspot and tethering capabilities must be enabled on a per-device basis and only after an appropriate business case has been filed and approved by a supervisor. Functions should only be enabled when required and only for the required duration.

Requirements for Classifications Limited through Critical

- Device must be securely wiped and reset before being reissued
- Device must be secured before being issued to a user
- Mobile device management client is required
- Device password is required before fully booting

- Device password is required; swipe, pattern, and PIN are not secure enough
- Screen locks and inactivity timeouts are required as per P4550 (Mobile Device Management) policy.
- Sideloading of applications must be disabled and prohibited
- Anti-virus, web content filtering, and encryption (at-rest and in-transit) are required

Reference Appendix A for a graphical representation of these classifications and required controls.

IV. PROCEDURE REFERENCE

- ITA Enterprise Policy P4550 (Mobile Device Management)
- ITA Enterprise Standard S2140 (Mobile Device Capabilities)
- ITA Enterprise Guideline G560 (Passwords)
- ITA Enterprise Policy P1060 (Employee Personal Computer Use)
- ITA Enterprise Guideline G550 (Cleansing Data from Surplus Computer Equipment)
- ITA Enterprise Policy P4130 (Information Systems Classification)
- ITA Enterprise Guideline G505 (Data Classification and Labeling)

V. CONTACT INFORMATION

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

REVISION HISTORY

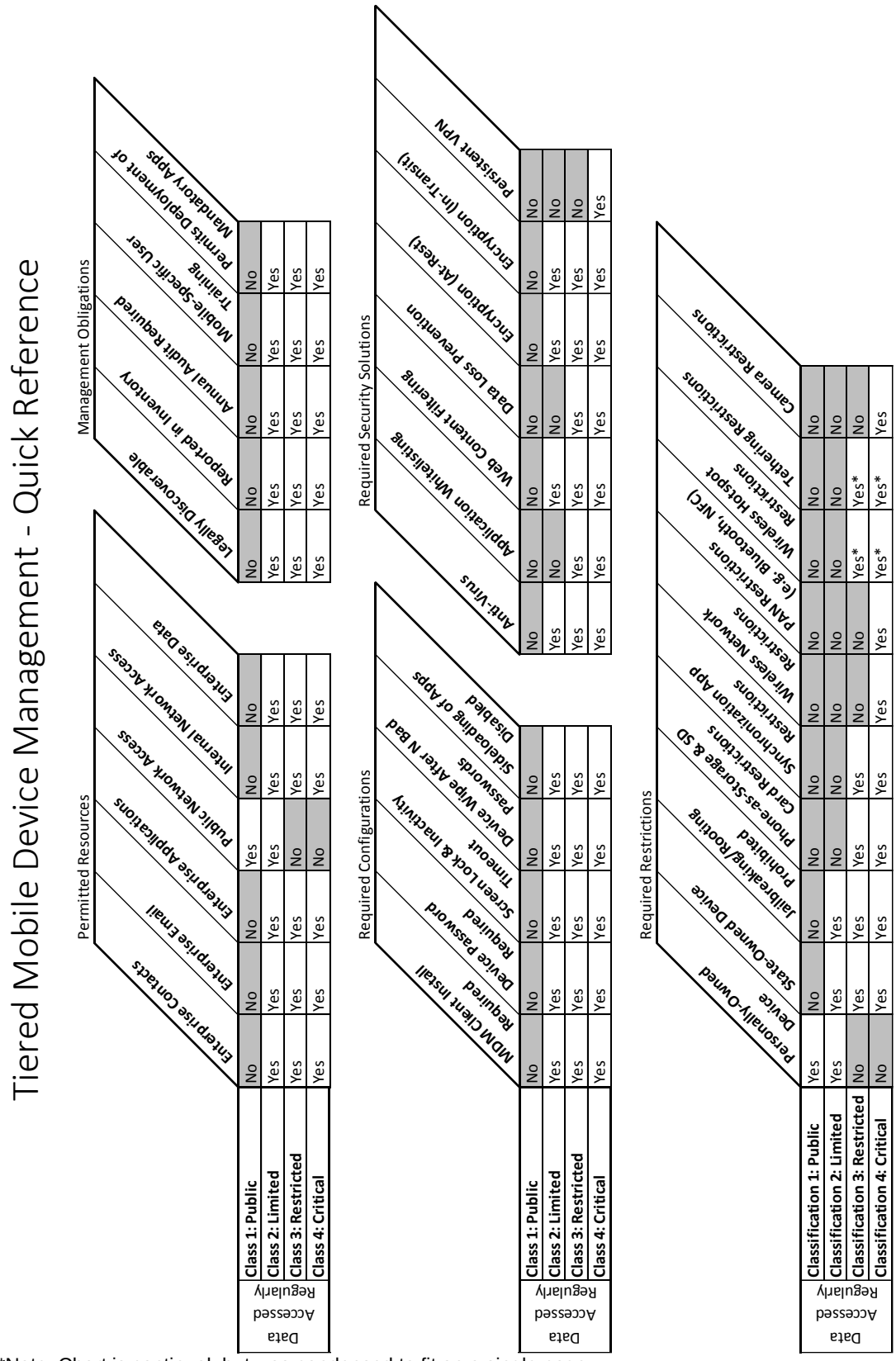
04/18/2017 – Restructured document, added Tiered Mobile Device Model and Agency Policy section.

07/01/2013 – Changed “ITRMC” to “ITA”.

6/16/2009 – Added Procedure Reference, Contact Information, and Revision History to this guideline; changed the layout and deleted Timeline.

Effective Date: October 24, 2005

APPENDIX: A



*Note: Chart is continual, but was condensed to fit on a single page