

# Information Technology Resource Management Council (ITRMC)

## **ENTERPRISE GUIDELINES – G500 SECURITY PROCEDURES**

**Category: G540 – MOBILE DEVICES**

### **CONTENTS:**

- I. [Definition](#)
- II. [Rationale](#)
- III. [Security Overview](#)
- IV. [Physical Security](#)
- V. [Device Security](#)
- VI. [Data Guidelines](#)
- VII. [Communication and User Education](#)
- VIII. [Time Line](#)

### **I. DEFINITION**

Mobile Devices – For the purposes of this policy, includes Pocket PCs, Tablet PCs, Laptop PCs, Notebook Devices, Personal Digital Assistants (PDAs) and other mobile computing 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. 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 not considered a secure computing device. It is recommended that only non-confidential information be stored on the device and the password protection feature enabled.

#### **IV. 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.

#### **V. 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 passwords 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 carry on 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. Agencies are responsible for installing the patches,

virus scanning software and virus data files on their devices. Patches and updates to virus data files should be installed through an automated process if applicable. Agencies should install patches for high-risk vulnerabilities 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.

## VI. DATA GUIDELINES

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 surplus (See ITRMC Guideline G550 – Removal of State of Idaho Data from Surplus Computer Hard Drives and Electronic Media).

## VII. 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.

### **Procedure Reference**

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

Guidelines for the use of operating systems on Mobile Devices is addressed in " Enterprise Standards –Software – Desktop and Notebook, Standard S2100 – Operating Systems (OS).

### **VIII. TIME LINE**

Effective Date: October 24, 2005