Idaho Technology Authority (ITA)

ENTERPRISE STANDARDS S2000 – SOFTWARE – DESKTOP, NOTEBOOK & MOBILE DEVICES

Category: S2140 – **MOBILE DEVICE SECURITY CAPABILITIES**

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**.** 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.

Encryption: Transformation of information into a form that cannot be read or interpreted by others without knowledge of how it was transformed. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it.

II. RATIONALE

Mobile devices must be able to be appropriately secured to prevent sensitive information from being lost or compromised, to reduce the risk of spreading viruses, and to mitigate other forms of abuse of the State of Idaho's computing and information infrastructure.

III. APPROVED STANDARDS

Mobile devices that connect to the state network and/or state e-mail, must

A. Support Password protection.

B. Have screen locking and screen timeout functions.

C. Have the ability to encrypt files in onboard storage or removable storage.

D. Be capable to be wiped remotely and disabled if the device is stolen or lost, if the device is wireless.

E. Be able to be managed in a way that agencies can control or limit what applications are able to be downloaded and installed.

F. Have the ability to be protected from and scanned for viruses.

IV. APPROVED PRODUCTS

A. State-purchased devices which meet the above criteria are approved.

B. Personally-owned devices which meet the above criteria may be used if the owner acknowledges, and signs an agreement, that their personal data on the device may be wiped if lost or stolen.

V. JUSTIFICATION

Smartphones have dramatically grown in popularity and have commonly found their way into the government workplace. With government-issued devices, such as the BlackBerry™, iPhone™, Droid™ and others, public sector employees use smartphones to access email, browse the Internet, access business applications and a myriad of other purposes. While a great deal of productivity, efficiency and convenience can be derived from smartphone use, the potential for security incidents and data breaches is a practical concern for the state. With widespread adoption on the consumer side, state officials are now faced with a new dilemma – requests by employees to use their personal devices for state business. In an effort to address these requests, make the work lives of employees less complicated, and perhaps

reduce state IT acquisition costs, we must balance the risks with the rewards of increased mobile device usage.

VI. TECHNICAL AND IMPLEMENTATION CONSIDERATIONS

The number and variety of mobile devices is increasing rapidly, making it more difficult for agencies to manage them, or to develop expertise in configuring and maintaining them. While the easiest way to approach mobile device management might be to limit agency users to one or two types of devices, agency users, to include executive-level users, can justify the use of different devices based on ease of use and increased efficiencies. IT staffs find it difficult to learn how to manage the devices, much less find the time to do so, particularly if an agency has many different types of mobile devices.

VII. EMERGING TRENDS AND ARCHITECTURAL DIRECTIONS

There are a growing number of companies which offer mobile management solutions which have been developed to help businesses manage multiple devices and which improve security. Some of these solutions even allow the personal use of a device to be managed separately from the business use (e.g., if lost, the business information will be wiped clean, but the personal information will remain intact). Agencies may want to consider using a solution if they have authorized the use of different devices in their agency.

VIII. PROCEDURE REFERENCE

Yet to be developed.

IX. REVIEW CYCLE

X. CONTACT INFORMATION

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

REVISION HISTORY

07/01/13 – Changed “ITRMC” to “ITA”.

Date Established: April 27, 2011

Appendix to S2140

Example of User Agreement for Enterprise use of Personal Mobile Device

Agency Name		
Personal Mobile Device - State Network Use Agreement		
Agreement Statements	Initial	
I understand that using my personal mobile device for state business, to include e-mail, is my choice.		
I will protect my mobile device to the best of my ability to help ensure state information is protected from theft or other exploitation.		
I understand that, if my mobile device is lost or stolen, it must be remotely wiped of all information since otherwise it may expose sensitive state information to theft or exploitation.		
I agree that I will not dispose of my mobile device, return it to my provider , or give it to another individual without ensuring that my agency's IT shop has had a chance to wipe any sensitive state information.		
I agree to always using a secure pin or password to help protect the information on my mobile device and to prevent unauthorized use of the mobile device.		
I agree to notify my agency's mobile device manager or IT help desk immediately upon realizing that my mobile device has been stolen or irretrievably lost.		
Signature		
Date		