State of Nevada

Information Security Committee

Standard

Control No.	Rev.	Title	Effective Date	Page
138	A	Mobile Device Security	05/01/2016	1 of 4

1.0 PURPOSE

This standard provides guidance to ensure the security of Mobile Devices (MD) that interface with the State of Nevada's network and / or contain official State of Nevada information.

2.0 SCOPE

This standard applies to all state employees, contractors, or other individual that operates, manages or uses SilverNet.

3.0 EFFECTIVE DATES

This standard becomes effective at the time of approval of the State Chief Information Officer (CIO).

4.0 RESPONSIBILITIES

The agency head and appointed agency Information Security Officer (ISO) have the responsibility to ensure the implementation of and compliance with this standard. Agency managers are ultimately responsible for access to the systems, delegation of administrative tasks and disseminating this standard.

5.0 RELATED DOCUMENTS

State Security Policy 100, Section 4.2.2, Laptops and Other Mobile Computing Devices
State Security Policy 100, Section 4.2.3, Personally Owned Equipment and Software
Form 139, Mobile Device Agreement Form
http:// it.nv.gov/governance/state-policy-procedures/

6.0 STANDARDS

A. Mobile Device Management

1) The Mobile Device Agreement Form, which outlines responsibilities for both the agency manager and the employee, must be properly filled out, listing the specific applications to be installed and the specific State data to be carried on the Mobile Device. This form must be signed by the employee, approved by the appropriate manager, and kept on file with the employee's current Acceptable Use Agreement and with the agency ISO or ISO designee.

2) Mobile Device Agreement Forms must be re-submitted if:

    a. The MD is replaced or upgraded.
    b. The employee departs the agency or changes their position.
    c. There is significant change of authorized applications or data.

3) Personally owned Mobile Devices (MD) will not be connected to any State of Nevada device or network, directly or indirectly, unless determined by the agency management to be a

business necessity, and explicitly authorized through approval of a Mobile Device Agreement Form. Once approved, all provisions of the standard apply to a personally owned MD in all respects as if it were a State-owned MD.

4) The Agency ISO or ISO designee must audit agency MD agreements on file against agency email accounts with MD access enabled, no less than annually. All email accounts found with MD access enabled should have MD agreements on file which match the MDs in use by authorized individuals.

B. Physical Security

1) Appropriate care will be taken by employees and agency management to ensure that any physical loss of an MD is minimized.

   a. Employees will not leave any MD unattended, and will physically secure an MD when not actively in use.
   b. Any Mobile Devices that are not in use on a daily basis, or that are left in the office overnight will be physically secured in a locked cabinet, container or secured area.
   c. Any Mobile Devices that are, or are suspected to be, lost or stolen must be reported immediately to the agency ISO.

2) Biometric access controls are recommended for all Mobile Devices that:

   a. Have such capability, and
   b. Will be used to process or maintain confidential or sensitive data.

C. Data Security

1) Mobile Devices used to store State data will be password protected, in accordance with appropriate State, and agency security policies, standards, and procedures (PSPs). If the MD cannot meet the requirements, then it will not be allowed to access the State of Nevada internal network, nor connect to any device that is attached to the State of Nevada internal network.

2) Mobile Devices will have an inactivity timeout of no more than 10 minutes that will set the MD into a power-off or locked state if applicable. After the inactivity timeout occurs, it will be necessary to re-authenticate to gain access to the functions of the MD.

3) Confidential, restricted or internal use data will only be maintained on Mobile Devices if said data is encrypted in accordance with the identified data classification level. Examples of these types of data include, but are not limited to: Internal-use only memorandums, documents listed as confidential, HIPAA/privacy act protected information.

4) Mobile Devices that contain restricted or confidential data must meet authentication requirements for the identified data classification level. Data will not be stored,

transported or otherwise maintained on a device that is not in compliance with the identified data classification level.

5) Mobile Devices must be reviewed for the Operating System (OS) version and patch level no less than once every six months, if applicable, and the OS will be upgraded with any appropriate patches at that time. All Mobile Devices will utilize updated anti-virus protection appropriate to the OS, if such anti-virus software is applicable. Mobile Devices should also contain appropriate firewall software or hardware, if such firewall software is applicable.

6) All state data that passes through a wireless Mobile Device connection will be encrypted to ensure secure transport, as wireless communications from MD generally pass through networks in a readable state, and are able to be intercepted by others.

D. Handheld Email Devices

1) All handheld email devices must be registered with the agency ISO or ISO designee utilizing the Mobile Device Agreement form prior to email activation.

2) Handheld email devices that contain confidential information will not have such information stored or otherwise maintained on a device that is not in compliance with State and agency mobile device security controls required for confidential data.

3) Handheld email devices will have a feature to remotely erase the device after 10 unsuccessful attempts to login.

7 DEFINITIONS

Mobile Device: Any handheld electronic device that is capable of containing State data, including contact information, email, organizational data, etc. or is capable of connecting with a Personal Computer (PC), Server, or Laptop via cable or wireless access to transfer data between the two devices. Mobile Devices are an “information system” as specified in NRS 242.057, and as such are required to meet all laws, policies, and procedures that reference information systems.

Handheld Email Device: A subset of Mobile Devices, defined as any handheld electronic device that connects or registers to a central email service.

Both of these terms, **Mobile Device** and **Handheld Email Device**, do not include devices that solely utilize web-based connectivity for access to State email systems.

8.0 EXCEPTIONS/OTHER ISSUES

Requests for exception to the requirements of this Information Security Standard must be documented, provided to the Office of Information Security (OIS), and approved by the State Chief Information Security Officer (CISO).

Approved By		
Title	**Signature**	**Date**
State Information Security Committee	Approved by Committee	5/1/2016
State Chief Information Security Officer (CISO)	Signature on File	5/25/2016
State Chief Information Officer (CIO)	Signature on File	6/13/2016

Document History		
Revision	**Date**	**Change**
A	05/01/16	Initial release – Formerly EITS Standard 113