State of Nevada
Information Security Committee

Standard

Document ID	Title	Revision	Effective Date	Page
S.4.02.02	Mobile and Non-State Device Security Management	C	12/31/2020	1 of 3

1.0 PURPOSE

This standard establishes the minimum requirements for the administrative and physical security of mobile and non-State devices that connect with the state's networks and systems or contain state data or information.

2.0 SCOPE

This standard applies to all state agencies and authorized users meeting the criteria identified in the State Information Security Program Policy, Section 1.2, Scope and Applicability.

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.

5.0 RELATED DOCUMENTS

NRS 242.057 Information System defined.
State Security Program Policy, 100
Data Sensitivity, S.3.02.01
Software Inventory and Control, S.6.02.01
Software Patch Management, S.6.03.01
Secure Software Configuration, S.6.05.01
Malware Defenses, S.6.08.01
Data Protection, S.6.13.01
Wireless Access Control, S.6.15.01
Account Monitoring and Control, S.6.16.01
Mobile and Non-State Device Agreement Form, S.4.02.02.1F

6.0 STANDARD

6.1 Mobile and Non-State Device Management

A. The Mobile and Non-State 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 accessed or stored on the device. This form must be signed by the employee, approved by the appropriate manager, and kept on file with the agency ISO or ISO designee.

B. Mobile and Non-State Device Agreement Form must be re-submitted if:

1. The mobile or non-State device is replaced or upgraded.

2. The employee departs the agency or changes their position.

3. There is significant change of authorized applications or data.

C. Mobile and Non-State Devices will not be connected to any State 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 and Non-State Device Agreement Form.

1. Once approved, all provisions of the State Information Security Program Policy and standards apply to a mobile or non-state device in all respects as if it were a non-mobile or State device.

D. The Agency ISO or ISO designee must audit agency mobile device agreements on file, including a review of mobile devices against agency accounts with mobile device access enabled, no less than annually. All accounts found with mobile device access enabled should have mobile device agreements on file which match the mobile devices in use by authorized individuals.

6.2 Physical Security

A. Appropriate care will be taken by employees and agency management to ensure that any physical loss of a mobile or non-State device used for State business is minimized.

1. Employees will not leave any mobile or non-State device unattended and will physically secure the device when not actively in use.

2. 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.

3. Any mobile or non-State device used for State business that is, or is suspected to be, lost or stolen must be reported immediately to the agency ISO.

B. Biometric access controls are recommended for all mobile devices that:

1. Have such capability, and

2. Will be used to process or maintain confidential or sensitive data.

7.0 DEFINITIONS

Mobile Device: Any hardware technology asset not installed and used solely at a single, permanent location, whether a Non-State Device or a State device, that:

- has the potential to contain State data, including contact information, email, organizational data, state data, etc., or
- has the potential to connect with another technology asset 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, standards, and procedures that reference information systems.

The term **Mobile Device** does not include devices that solely utilize web-based connectivity for access to State email systems.

Non-State Device: Refers to and includes devices not owned or leased by the State, or otherwise not under the full management and control of the State.

Technology Assets: As defined in CIS Controls v7.1, the term “Technology Assets” (also referred to therein as “Hardware Technology Assets” or “Hardware Assets”) collectively refers to equipment and devices that have the potential to store or process information, whether connected to the network or not.

8.0 RESOURCES

Center for Internet Security (CIS), CIS Controls v7.1 Guide

9.0 EXCEPTIONS

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	Approval Date
State Information Security Committee	Approved by Committee	11/19/2020
State Chief Information Security Officer (CISO)	Signature on File	11/24/2020
State Chief Information Officer (CIO)	Signature on File	11/30/2020

Document History

Revision	Effective Date	Change
A	5/01/2016	Initial release – Formerly EITS Standard 113
B	12/26/2018	Renumbering (138 to S.4.02.02) and compliance to ADA standards.
C	12/31/2020	Biennial review for alignment with CIS Controls v7.1, Implementation Group 1 (IG1)