State of Nevada

Information Security Committee

Standard

Document ID	Title	Revision	Effective Date	Page
S.6.05.01	Secure Software Configuration	A	12/31/2020	1 of 3

1.0 PURPOSE

This standard establishes the minimum requirements for secure software configuration on mobile devices, workstations, desktops, servers, and other technology assets, as required to implement the CIS Controls v7.1, Implementation Group 1.

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 Information Security Officer (ISO) have the responsibility to ensure the implementation of and compliance with this standard.

5.0 RELATED DOCUMENTS

NRS 603A Security and Privacy of Personal Information
State Information Security Program Policy, 100
Mobile and Non-State Device Security Management, S.4.02.02
User Identification and Authentication, S.5.01.01
Software Inventory and Control, S.6.02.01
Software Patch Management, S.6.03.01
Malware Defenses, S.6.08.01
Wireless Access Control, S.6.15.01

6.0 STANDARD

6.1 Establish Secure Software Configurations

A. State agencies must establish, implement, and maintain documented security configuration standards for all authorized software, including operating systems (OS) and non-OS software.

B. Documented configuration management procedures must include processes for the request, approval, implementation, and documentation of all software configuration changes.

6.2 Secure Software Configuration Tools and Communications

A. Configuration and management tools must meet all minimum software security requirements, must be controlled for access only by authorized users, and must use secure communications protocols.

6.3 Authorized Credentials

A. Technology assets used to access, process, transmit, or store State data will be protected by requiring authorized credentials, in accordance with appropriate State and agency security policies, standards, and procedures (PSPs).

B. If a technology asset cannot be protected by requiring authorized credentials, it will not be allowed to access the State internal networks, nor connect to any state system or other technology resource that is attached to the State internal network.

6.4 Mobile Device Remote Wipe

In addition to the above minimum requirements for technology assets, all mobile devices authorized or used for State business, including both State and Non-State devices, will be configured to meet additional security requirements for mobile devices.

A. Mobile devices will be configured to remotely erase the device after 10 unsuccessful attempts to login.

B. Mobile devices not supporting a remote wipe after 10 unsuccessful login attempts must use equivalent or better whole device encryption, in accordance with State-approved encryption controls. and as defined in NRS 603A Security and Privacy of Personal Information and the CIS Controls v7.1, Implementation Group 1.

6.5 Other Non-State Device Configuration

All other (non-mobile) Non-State devices authorized or used for State business will be configured to meet these minimum security requirements.

7.0 DEFINITIONS

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).

State of Nevada

Information Security Committee

Standard

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	12/31/2020	Initial release to align with CIS Controls v7.1, Implementation Group 1 (IG1)