State of Nevada

Information Security Committee

Standard

Document ID	Title	Revision	Effective Date	Page
S.6.03.01	Software Patch Management	G	12/31/2020	1 of 3

1.0 PURPOSE

This standard establishes the minimum requirements for software patch management on technology assets, including both Operating System (OS) and non-OS software, 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

State Information Security Program Policy, 100
Software Inventory and Control, S.6.02.01

6.0 STANDARD

6.1 Keeping technology assets current with the latest available software patches and updates is a crucial part of protecting State technology assets and information. In order to protect these systems, state agencies must provide the following minimum protections for all technology assets within their area of responsibility:

A. Deploy and use automated software update tools on all technology assets and networks, to ensure that agency assets are running the most recent security updates provided by the software vendor for all Operating System (OS) and non-OS software, in order to maximum protection against security vulnerabilities and minimize impact on agency business operations.

B. Create a consistent maintenance window no less than semi-monthly for the deployment of software updates and patches, and ensure users are notified of the maintenance window timeframes.

C. Develop, test, and document procedures for deploying security patches and other necessary software patches and updates. This process of testing an update or patch must be developed to minimize security risks and disruption to the production environment.

1. If possible, a completely redundant test system with identical system load and hardware compatibility should be used to test the new code. When a completely redundant system is not available, testing should be done in a way that as closely as possible approximates conditions of the production system.

D. Ensure a process for reverting changes made and returning to the pre-update state is prepared in case of unexpected results that impact business processes.

E. Implement a process to deploy critical or actively exploitable security patches, beginning with testing occurring no later than 5 working days of release from the vendor.

F. Upgrade Operating Systems, commercial applications, software service packs, and other vendor-provided software that has reached end-of-support from the vendor to a currently supported version.

G. Utilize a standardized methodology for software updates established by the state agency and in accordance with state information security policy and standards.

6.2 Mobile Device Software Patch Management

A. Where possible, automated software updates must be enabled.

B. Agencies must have processes in place to monitor software updates available for mobile devices and must assure mobile device software is patched and updated.

7.0 DEFINITIONS

Patch or **Update**: An improvement to software, including security patches, software updates to firmware, cumulative software patches, and other software features.

Semi-Monthly: Occurring twice in a month.

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	6/25/2005	Initial release
B	6/08/2006	Added section 6.1
C	8/21/2007	Conversion of Interim Standard to Permanent Standard
D	4/26/2012	Renumbering and minor revisions, replaces standard 4.34
E	8/31/2017	Biennial review and update of the standard
F	12/26/2018	Renumbering (117 to S.5.07.01) and compliance to ADA standards
G	12/31/2020	Biennial review for alignment with the CIS Controls v7.1, Implementation Group 1 (IG1). Renumber and rename S.5.07.01 IT Operating System Patch Upgrade Management to S.6.03.01 Software Patch Management.