State of Nevada

Information Security Committee

Standard

Document ID	Title	Revision	Effective Date	Page
S.6.08.01	Malware Defenses	D	12/31/2020	1 of 2

1.0 PURPOSE

This standard establishes the minimum requirements for malware defense of 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

State Information Security Program Policy, 100
Information Security Officer (ISO) Roles and Responsibilities, S.3.03.01

6.0 STANDARD

6.1 Malware Defense Management

Each agency shall:

A. Guard against malware by implementing security and detection methods necessary for the operating environment of each device.

B. Develop malware defense procedures to be followed by all users.

C. Update malware defense software and definition files as new releases and updates become available. Review or update malware definition files daily.

D. Notify and give users direction when malware or a malware-related security alert has been received.

6.2 Malware Defenses For Technology Assets

A. State technology assets must utilize state agency standardized malware defenses. These state assets must be configured to automatically download and apply the latest malware definitions and protections from a centralized server.

B. Mobile and non-State owned devices will utilize updated malware defense protection appropriate to the Operating System, if such malware defense software is practicable.

C. Email systems shall not be deployed without malware defense software that scans all messages and attachments transferred through the system.

1. Email systems must specifically inspect email for malicious content and employ some form of blacklisting for senders or domains that are routinely responsible for the delivery of malware.

D. All public access servers shall not be deployed without malware defense software that scans all messages and attachments transferred through the system.

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).

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	8/08/2002	Initial release
B	8/06/2012	OIS biennial review, replaces standard 4.33
C	12/26/2018	Renumbering (133 to S.5.05.01) and compliance to ADA standards.
D	12/31/2020	Biennial review for alignment with the CIS Controls v7.1, Implementation Group 1 (IG1). Renumber and rename S.5.05.01 Virus Protection to S.6.08.01 Malware Defenses.