State of Nevada

Information Security Committee

Standard

Document ID	Title	Revision	Effective Date	Page
S.6.16.01	Account Monitoring and Control	A	12/31/2020	1 of 2

1.0 PURPOSE

This standard establishes the minimum requirements for account monitoring and control, 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
Data Sensitivity, S.3.02.01
Mobile and Non-State Device Security Management, S.4.02.02
User Identification and Authentication, S.5.01.01
Secure Software Configuration, S.6.05.01
Data Protection, S.6.13.01

6.0 STANDARD

6.1 Disable Dormant Accounts

A. User accounts that are inactive on the system for 30 days or more should be disabled.

B. Service accounts must be disabled after an agency-specified period of inactivity.

6.2 Inactive Session Locks

A. All technology assets must be logged off or locked when an account is logged in and the employee leaves the immediate physical area of the asset.

B. All technology assets that are inactive for a period of fifteen minutes must automatically initiate a screen saver or other locking mechanism, protecting the asset by requiring authorized credentials to unlock access. Agencies may enforce a more restrictive lock out policy where applicable.

1. Mobile devices will have an inactivity timeout of no more than 15 minutes that will set the mobile device into a power-off or locked state if applicable.

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