State of Nevada

Information Security Committee

Standard

Control No.	Rev.	Title	Effective Date	Page
112	B	Workstation Security	4/26/2012	1 of 2

1.0 PURPOSE

This standard establishes the minimum criteria for securing State information technology workstations.

2.0 SCOPE

This standard applies to all state entity employees, contractors, and all other authorized users, including outsourced third parties, who have access to, use, store, transmit or manage state data or information within or for the Executive Branch of Nevada State Government.

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 or 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 Consolidated Policy, 100, Section 4.2

6.0 STANDARD

Computer workstations must be adequately protected against unauthorized access. State entities must provide the following minimum protection for all computer workstations.

A. Personally owned computer equipment must not be connected to SilverNet, or any State of Nevada network without specific written authorization from the employee's appointing authority.

B. All workstations must be logged off or locked when an account is logged in and the employee leaves the immediate physical area of the workstation. All workstations that are inactive for a period not to exceed fifteen minutes must automatically initiate a password protected screen saver or other locking mechanism.

C. All workstations must utilize state entity standardized anti-virus software. Workstations must be configured to automatically download the latest anti-virus definitions from a centralized server.

D. All workstations must utilize a standardized methodology for Operating System (OS) updates established by the state entity and in accordance with state policy and standard.

E. Only state entity approved software may be installed on a state workstation. All requests for non-standard software require approval authorization from the state entity appointing authority.

F. Remote access to SilverNet connected workstations initiated from outside SilverNet will be permitted only from an approved EITS VPN connection. Any remote access software or hardware that initiates or attempts to initiate a connection outbound from SilverNet is prohibited, unless the remote connection occurs through an approved EITS VPN connection.

G. Workstation user accounts must be granted the minimum set of privileges required to perform typical work-related functions of the employee. Accounts with administrator-level privileges will only be utilized for the minimum period of time required to accomplish specific tasks that require administrative privileges.

H. Maintenance of workstation hardware and software will only be performed by the state entity's authorized IT support employees or approved contractor IT support personnel. Attempts by unauthorized personnel to access workstations will be immediately reported to the employee's supervisor and the agency ISO.

I. All workstations will undergo electronic media sanitization before the workstation is transferred, donated or otherwise disposed of by appropriate entity IT personnel. This sanitization will overwrite all information on electronic media with a minimum of three (3) passes with random information overwritten on each pass. Workstations that contain confidential or personal identification information (PII) during their service life must utilize a minimum of seven (7) passes with random information overwritten on each pass.

J. Workstations must not be utilized to act in a capacity as a server for any production application or environment.

7.0 EXCEPTIONS/OTHER ISSUES

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**	**Date**
State Information Security Committee	Approved by Committee	10/27/2011
State Chief Information Security Officer (CISO)	Signature on File	2/21/2012
State Chief Information Officer (CIO)	Signature on File	4/26/2012

Document History		
Revision	**Date**	**Change**
A	2/21/12	Initial release.
B	4/25/12	Office of Information Security biennial review, replaces standard 4.140200