State of Nevada

Information Security Committee

Standard

Control No.	Rev.	Title	Effective Date	Page
117	E	IT System Patch & Upgrade Management	9/05/2017	1 of 3

1.0 PURPOSE

This standard establishes the minimum IT System Patch and Upgrade Management standard for information systems and IT resources that support the agency.

2.0 SCOPE

This standard applies to any entity, regardless of physical location, that operates, manages, or uses SilverNet services or equipment.

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 Consolidated Policy 100: Section 5.7
State Standard 112: Workstation Security

6.0 STANDARD

Keeping IT systems current with the latest available patches and updates is a crucial part of protecting State IT systems. In order to protect these systems, state entities must provide the following minimum protection for all IT systems within their area of responsibility:

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

B. 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. 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.

C. 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.

D. 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.

E. Operating Systems, service packs or commercial applications that have reached end-of-support from the vendor must be upgraded to a currently supported version.

F. IT System updates and maintenance will only be performed by personnel authorized by agency.

6 DEFINITIONS

IT System: Any Information Technology infrastructure or components used for the collection, organization, storage and communication of information.

Patch / Update: An improvement to hardware or software including cumulative patches and other features.

Semi-Monthly: Occurring twice in a month.

7 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	8/31/2017
State Chief Information Security Officer (CISO)	Signature on File	9/05/2017
State Chief Information Officer (CIO)	Signature on File	9/05/2017

Document History		
Revision	**Date**	**Change**
A	6/27/05	Initial release.
B	6/08/06	Added section 6.0.1
C	8/21/07	Conversion of Interim Standard to Permanent Standard
D	4/26/12	Renumbering and minor revisions, replaces standard 4.34
E	8/31/17	Biennial review and update of the standard.