



State of Nevada

Information Security Committee

Standard

Control No.	Rev.	Title	Effective Date	Page
117	D	IT Operating System Patch & Upgrade Management	7/26/2012	1 of 2

1.0 PURPOSE

This standard establishes the minimum IT Operating System Patch and Upgrade Management standard for an information system and the IT resources that support the mission of the agency.

There are many legitimate cases for upgrading or patching the operating system of a computing resource, e.g., security patches, performance patches, maintenance upgrades, etc. When these conditions occur the process of reviewing the effects of the patch or upgrade should be thoroughly tested and reviewed prior to making the change.

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 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
Microsoft Security Update Guide, Second Edition
Creating a Patch and Vulnerability Management Program, NIST 800-40, Version 2.0

6.0 STANDARD

6.0.1 Each agency shall develop, maintain and test procedures for handling security patches and other necessary software patches and updates.

6.0.2 The process of testing and approving the update or patch must be developed to minimize security risks and disruption to the production environment.

6.0.3 Critical patches must be implemented as soon as possible.



State of Nevada

Information Security Committee

Standard

Control No.	Rev.	Title	Effective Date	Page
117	D	IT Operating System Patch & Upgrade Management	7/26/2012	2 of 2

- 6.0.4 Agencies must demonstrate a process in progress for vendor designated critical security patches within 72 hours (3 working days) from the date of vendor release. Each agency shall develop a process to implement contracted vendor critical security patches within 3 working days from the date of vendor release.
- 6.0.5 Operating Systems that have reached their end-of-life and the vendor no longer provides patches, fixes, and other updates must be upgraded.
- 6.0.6 When the lifecycle of an operating system or service pack is no longer eligible for support, security updates, and non-security hot fixes, the operating system must be upgraded.

7 DEFINITIONS

None

8 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).

<i>Approved By</i>		
Title	Signature	Date
State Information Security Committee	Approved by Committee	7/26/2012
State Chief Information Security Officer (CISO)	Signature on File	7/26/2012
State Chief Information Officer (CIO)	Signature on File	7/26/2012

<i>Document History</i>		
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