

California State University Northridge	Information Technology Campus-wide Patch Management Process and Compliance-Review Procedure	Page 1 of 5	
		SOP#: ITIS 90-09-028	Revision#: Version 0.5

Prepared by: Leigh Lopez Date: April 8, 2009	Approved by: Chris Olsen Date: June 29, 2009
Last revised by: Chris Olsen Date: June 29, 2009	Last approved by: Chris Olsen, ISO Date: January 11, 2012

1.0 PURPOSE

This document provides the processes and guidelines necessary to 1) maintain the integrity of network systems and university data by applying the latest operating system and application security updates/patches in a timely manner, and 2) to establish a baseline methodology and time frame for patching and confirming patch-management compliance.

Desktops, laptops, servers, applications, and network devices represent access points to sensitive and confidential University data as well as to technology resources and services. Ensuring that security updates and patches are distributed and implemented in a timely manner is essential towards mitigating malware, exploitation, and other threats.

2.0 SCOPE

The processes addressed in this document affect all managed campus systems, including desktops, laptops, servers, network devices, and applications that connect to the campus network.

3.0 RESPONSIBILITY

	Role (Title)	Responsibility
1	Information Security Officer (ISO)	<ul style="list-style-type: none"> Review and approve changes to the patch management process.
2	Information Security Analyst/Administrator	<ul style="list-style-type: none"> Notify campus technical administrators when new patches are available. Coordinate the review of new patches with the campus patch test group and the patch server administrator. Discuss patch releases at campus Change Management meetings. Maintain the vulnerability scanning tool; conduct periodic scans of critical systems to identify known vulnerabilities.
3	Network Engineer/Analyst	<ul style="list-style-type: none"> Install patches; review network device hardware configurations.

California State University Northridge	Information Technology	Page 2 of 5	
	Campus-wide Patch Management Process and Compliance-Review Procedure	SOP#: ITIS 90-09-028	Revision#: Version 0.5

4	Application Developer/Administrator	<ul style="list-style-type: none"> Develop and install patches; identify known and potential vulnerabilities; confirm current patch levels are met.
5	Desktop Administrator	<ul style="list-style-type: none"> Install patches; generate and review patch reports at least monthly, remediate vulnerabilities on systems that cannot be patched to resolve known vulnerabilities.
6	Server Administrator	<ul style="list-style-type: none"> Install patches; generate and review patch reports at least monthly, remediate vulnerabilities on systems that cannot be patched to resolve known vulnerabilities.
7	Campus Patch Testing Group	<ul style="list-style-type: none"> Test patches; notify the IS office of adverse effects.
8	Change Management Review (CMR) committee	<ul style="list-style-type: none"> Review and approve centrally-deployed patches prior to deployment.

4.0 Process

4.1 Desktops and Servers

1. As made available, download patches from a trusted source; Microsoft, Adobe, Apple, Sun, HP, Compaq, etc.
2. Test patches to identify adverse effects.
3. Input a Change Management Request case and discuss at the weekly change management meetings. Follow the Emergency CMR process for critical security patches that require immediate attention.
4. Communicate to stakeholders.
5. Deploy patches campus-wide:
 - A. Windows Workstations:
 - i. Monthly patches: Deploy no later than during the second weekly maintenance window of each month.
 - ii. Out-of-band security patches: Deploy as soon as possible; no later than one week following release.
 - B. Macintosh Workstations:
 - i. Deploy as soon as possible; at least once per month.
 - C. UNIX/Linux Workstations:
 - i. Deploy as soon as possible; at least once per month.
 - D. Windows Servers:

California State University Northridge	Information Technology Campus-wide Patch Management Process and Compliance-Review Procedure	Page 3 of 5	
		SOP#: ITIS 90-09-028	Revision#: Version 0.5

- i. Monthly patches: Deploy no later than during the third weekly maintenance window of each month.
 - ii. Out-of-band security patches: Deploy as soon as possible; no later than one week following release.
- E. Macintosh/UNIX/Linux/SOLARIS Servers:
- i. At least once per month.
 - ii. Critical security patches that resolve a known vulnerability: Deploy as soon as possible following release and no later than one week following release.

4.2 Network Hardware/Devices (Routers, Switches, etc.)

1. Download patches as available. Patch notifications originate from vendors (Cisco, Aruba, and Enterasys) and Governance Flash Reports (GFRs).
2. Test (where a test environment is available).
3. Adhere to the campus Change Management Review (CMR) process for release to production.
4. Implement.
5. Review device configurations to identify known and potential vulnerabilities. Retain documented evidence of the review for a period of at least one year.

4.3 CSUN-Developed Patches: Review to Identify Known or Potential Vulnerabilities

1. Identify the need for patch code based on incident/problems reports, enhancement requests and periodic vulnerability assessments/reviews (recorded via the case management system).
2. Develop and test the patch code in a non-production environment.
3. As noted below, request a vulnerability scan from the Office of Information Security (email to it.security@csun.edu) to identify known vulnerabilities. Conduct a review of the code to identify known or potential vulnerabilities not discoverable from the vulnerability assessment (such as hardcoded account credentials).
 - Applications that interface with protected data;
 - Mission Critical applications;
 - Other applications as deemed appropriate by the application owner.
4. Follow a Change Management Review (CMR) process to release the patch into production. To join a weekly Wednesday IT CMR meeting, email rca@csun.edu.
5. Retain documented evidence for a period of at least one year of identified vulnerabilities and remediation actions taken.

California State University Northridge	Information Technology Campus-wide Patch Management Process and Compliance-Review Procedure	Page 4 of 5	
		SOP#: ITIS 90-09-028	Revision#: Version 0.5

4.5 Exceptions

1. Systems or applications that cannot be patched to resolve a known vulnerability will have the justification documented by the device/application owner and the necessary compensating control(s) implemented.
 - a. Justification
 - i. No vendor patch available;
 - ii. Patch provided by vendor creates instability within the system; instability outweighs the risk.
 - b. Compensating Controls
 - i. Network segmentation;
 - ii. Access Control Lists;
 - iii. Intrusion Prevention Systems.

2. Systems that transmit or store protected data and cannot be patched to resolve a known vulnerability will be brought to the attention of the data owner (typically the IT Manager/Director for that college or department) and to the campus Information Security Officer, and the necessary compensating control(s) will be implemented.


4.6 Patch-Compliance Review Procedure

1. Desktop and server administrators will generate and review patch management/compliance reports at least monthly from the campus patch servers.
2. In reviewing the patch reports, desktop and server administrators will identify un-patched machines that connect to the campus network and either patch or define an exception.
3. The Information Security Office will conduct vulnerability scans of known critical systems at least annually. Critical systems with un-patched vulnerabilities will be brought to the attention of the system/application administrator(s) for mitigation.
4. An authorized external vendor will conduct vulnerability scans to identify known and potential vulnerabilities with campus systems that interface with credit card data. Vulnerabilities will be brought to the attention of the system/application administrator(s) for mitigation.

4.7 Periodic Vulnerability Assessments/Reviews of Campus-Developed Applications to Identify Known and Potential Vulnerabilities

Per the below timeframes, conduct periodic vulnerability assessments/reviews to identify known and potential vulnerabilities, as follows.

- o Applications that interface with protected data: every 2 years;
- o Other enterprise-level applications: every 3 years;

	Information Technology	Page 5 of 5	
	Campus-wide Patch Management Process and Compliance-Review Procedure	SOP#: ITIS 90-09-028	Revision#: Version 0.5

- Request an application-level vulnerability scan from the Information Security Office by submitting a request through the campus case management system or sending an email to it.security@csun.edu.
- Review the application code to identify known and potential vulnerabilities not discoverable from the automated vulnerability scan (for example: hard coded unencrypted credentials). Remediate vulnerabilities disclosed in the vulnerability scan report.
- Retain documented evidence for a period of at least one year of identified vulnerabilities and remediation actions taken.

5.0 DEFINITIONS:

6.0 REFERENCES:

Network Device Standards: 90-09-036

Server Security Standards: 90-09-030

Application Development Standards: 90-09-029

7.0 FURTHER INFORMATION:

Payment Card Industry (PCI) Data Security Standards (DSS)