Version:	Modified By:	Date:	Approved By:	Date:
1.0	Michael Hawkins	October 29, 2013	Dan Bowden	November 2013

Rule 4-004J Payment Card Industry (PCI) Patch Management (proposed)

01.1 Purpose

The purpose of the Patch Management Rule is to ensure that information about vulnerabilities and threats to the University of Utah's ("University") PCI systems and resources are obtained and evaluated, and appropriate measures taken to address the risks through the application of system patches.

01.2 Scope

The Patch Management Rule applies to all PCI systems and resources connected to the University's network. This includes network devices, servers, operating systems, desktops, laptops, applications and programs.

01.3 Rule Statement

The Information Security Office shall coordinate with IT support professionals to implement a patch management program to systematically manage vulnerabilities and threats to the University's information systems and resources, and ensure all related patches are installed in a timely manner.

01.4 Patch Management for PCI Systems

Area Statement: The Information Security Office shall report to University leadership the security posture relative to University information systems and resources having relevant and approved security patches are installed, as they become available based on system criticality and risk. Approved patches may have to be determined on a system-by-system basis with application vendors, IT support professionals, and Information Security coordination.

01.4.01 Testing Patches

All security-related patches, fixes and updates developed by in-house developers or provided by vendors, user associations and other trusted third parties shall be tested by the University's IT Professionals/Administrators prior to implementation. [Ref: CS171, PCI]

The IT Administrator shall perform, coordinate and support patching of systems. Specific responsibilities shall include:

- Monitoring vendor and government vulnerability alerts, web sites, and mailing lists. Also consideration should be given to subscribing to commercial vulnerability services that could provide the University with an early warning to potential vulnerabilities and threats.
- Working with appropriate system vendors to respond to system-specific security problems and concerns (i.e., operating system patches)
- Testing patches, fixes and workarounds, prior to distribution to IT professionals/administrators
- Notifying resource administrators of vulnerabilities as they are identified
- Providing technical assistance to IT professionals/administrators during the patch implementation process
- Monitoring via automated mechanisms, the patch implementation process to ensure patches are being loaded identifying, developing, purchasing and/or distributing security assessment tools

01.4.02 Installation of Patches

Resource administrators are responsible for installing available patches on the information resources under their control in a timely fashion. Security patches relevant to the protection of Restricted or Sensitive information (i.e. cardholder information) shall be installed within one month of release. [Ref: CS493, PCI]

[Rules] Resource administrators should use the following process to ensure that patches do not compromise the security of the information systems being patched:

- Obtain the patch from a known, trusted source
- Verify the integrity of the patch through such means as comparisons of cryptographic hashes to ensure the patch obtained is the correct, unaltered patch
- Apply the patch to an isolated test system and verify that the patch
    - Is compatible with other software used on systems to which the patch will be applied
    - Does not alter the system's security posture in unexpected ways, such as altering log settings
    - Corrects the pertinent vulnerability
- Backup production systems prior to applying the patch
- Apply the patch to production systems using secure methods, and update the cryptographic checksums of key files as well as that system's software archive

- Test the resulting system for known vulnerabilities
- Update the master configurations used to build new systems
- Create and document an audit trail of all changes
- Seek additional expertise as necessary to maintain a secure computing environment Install updates automatically without individual user intervention
- Employ automated mechanisms to make security alert and advisory information available throughout the organization

If a patch, fix or service pack cannot be applied because it damages other applications on the system, the risk posed by the unpatched vulnerability should be documented and the Information Security Office and the Information Owner should be notified.

When information systems are known to have vulnerabilities and cannot be patched, compensating controls shall be implemented to mitigate the risk.

01.4.03 Testing Information Systems

After operating systems changes (e.g., patches, upgrades, or new versions), applications and support processes shall be reviewed and tested including: application control and integrity procedures; support and development plans for operating system changes; proper notification of changes to user community, and updates to any applicable business continuity plans and/or recovery processes. [Ref: CS844, PCI]

01.4.05 Vulnerability Management Processes

The Information Security Office shall ensure that vulnerability assessments are conducted for the University's information systems and resources that include vulnerability scans that are conducted at least monthly.

Vulnerability remediation efforts, including patch implementations, shall be coordinated and processed according to the University's change management process (refer to the Change Management Policy). This includes meeting all testing and/or documentation requirements. Technical vulnerabilities, including vendor supplied patches, shall be classified using the following rating system. [Operational groups] shall remediate technical vulnerabilities or install patches using the following [schedules]: [Ref: CS845, PCI]

- **Immediate:** This classification applies to threats that are actively impacting the environment. Patches classified as immediate will be implemented without delay using emergency change control procedures.
- **Critical:** Critical patches are top priority for implementation because there are active known code and/or process issues related to the software. Critical patches should be implemented within 36 hours using emergency change control procedures. Important: Important Patches are to be implemented upon first available normal operational

opportunities. These patches have no existing negative impacts on operating results. Important patches will be implemented within seven (7) days using normal change control procedures.

- **Operational:** Operational patches are to be implemented upon the next operational patch promotion schedule. This classification is for enhancement patches that improve operations, but are not required for fixing inaccurate data or process results. Operational patches will normally be implemented within 30 days using normal change control procedures.

The Information Security Office shall be responsible for maintaining the documentation of the analysis produced by the technical vulnerability management processes, and is also responsible for escalating or de-escalating vulnerability classifications and communicating changes, as appropriate.

The Information Security Office and UIT shall be responsible for developing processes for asset management, classification and prioritization of systems in support of the technical vulnerability management processes. This includes a detailed asset inventory with appropriate documentation to facilitate prioritization and implementation of vulnerability remediation activities and the application of patched.

The Information Security Office shall ensure that baseline configuration is documented and maintained for the University's information systems and resources.

The vulnerability and patch management processes shall be reviewed on an annual basis.

01.5 Contacts

A. Policy Owner: Questions about this rule should be directed to the CISO, 801-213-3397 IT_policy@utah.edu

B. Policy Officer: Only the CIO, 801-581-3100, has the authority to grant exceptions to this rule.

01.6 References

A. Policy 4-002: Information Resources Policy
B. Policy 4-004: University of Utah Information Security Policy
C. Data Classification Model

01.7 Policy Meta-Data

A. Policy Owner
B. Audience
C. Status
D. Published Date
E. Effective Date
F. Next Review Date

01.8 Revision History