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

Rule 4-004I Payment Card Industry (PCI) Virus and Vulnerability Management (proposed)

01.1 Purpose

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

01.2 Scope

The Virus and Vulnerability Management Rule applies to all information systems 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 implement a virus and malware management program, a.k.a "Vulnerability Management" program, to systematically manage virus and malware threats to the University's information systems and resources.

01.4 Malicious Code and Viruses

Area Statement: The Information Security Office shall ensure that anti-virus software is installed on the University's information systems and resources and operating effectively, and the latest signatures are applied.

01.4.01 Responsibilities, Training and Actions

The Information Security Office shall be responsible for developing, implementing, maintaining and communicating a vulnerability management program to limit the introduction and spread of computer viruses, worms, Trojan horses, spam, spyware, denial of service attacks, etc., within the University's computing environments. This will be accomplished through meeting with Campus IT Professionals and organizational level infrastructure support groups. The Information Security Office is also responsible for reviewing and selecting approved virus detection software to be used by the University. [Ref: CS192, HIPAA]

[University personnel] shall be trained on the proper procedures for using virus detection software and responding to viruses, worms, Trojan horses, etc. This training information shall

be included in the overall training and awareness program that is the responsibility of the Information Security Office. [Ref: CS193, HIPAA]

Formal procedures shall be documented and communicated to Help Desk and support personnel informing them of their responsibilities when malicious code-related activity is reported. It shall be the responsibility of the Information Security Office to ensure that Help Desk and support personnel are adequately trained. In addition, escalation procedures shall be documented to ensure that notification of virus activity is sufficient to minimize the spread of malware. [Ref: CS194]

The Information Security Office shall be responsible for notifying any users who could be affected by an intrusion or malicious code activity. If communication to a third party is required, [University Communications, PR] shall review and authorize the communication. [Ref: CS196]

Users shall not intentionally write, generate, compile, copy, collect, propagate, execute or attempt to introduce any computer code designed to self-replicate, damage or otherwise hinder the performance of, or access to, any University information system or resource. [Ref: CS202]

Where the use of mobile code (JavaScript, VBScript, Java applets, ActiveX controls, Flash) is authorized, the configuration should ensure that the authorized mobile code operates according to a clearly defined security rule, and unauthorized mobile code should be prevented from executing.

The installation of software on University-owned or -leased information resources by unauthorized personnel is prohibited, unless prior written management approval has been given. [Ref: CS481, HIPAA]

If any user detects a virus on permanent or removable media, the following procedures should be followed: [Ref: CS485]

- Attempt to repair the virus with approved anti-virus software. If the virus cannot be repaired, isolate the affected computer immediately by disconnecting it from the network.
- Isolate all disks or other media that have been recently used on that computer.
- Do not allow these media to be mounted on other computers or network servers until they have been evaluated for possible infection by their respective IT support professional(s), and if appropriate, cleaned.
- Contact the appropriate technical support staff (e.g. LAN system administrator) or the Help Desk for assistance in virus diagnosis and treatment.
- Contact the Information Security Office to record the virus incident if:
    - External customers or third parties are involved

- The infected document or file was widely distributed
- The virus cannot be repaired
- The virus poses a serious threat to any University information system or resource

01.4.02 Anti-Virus Software

Signature-based anti-virus, spam, and spyware protection products shall be updated continually. These signatures shall be updated at least once a week to ensure systems scans can identify all known viruses. For regulated (PCI, HIPAA) systems, updates shall be installed as part of an automated network process (e.g. via login scripting). [Ref: CS195, PCI]

All University servers, workstations and laptop computers shall have approved virus detection or integrity software installed and active. For PCI systems, this software shall be configured to continuously monitor the systems and files for characteristics of viruses, worms, spyware, and Trojan horses, shall be capable of generating audit logs, and shall be installed in "auto-protect," "full-time" or "real-time" mode. This software shall be chosen from the University's [Approved Products list] which can be accessed by contacting the Chief Information Security Officer. [Ref: CS197, PCI]

Virus scans or integrity checks shall among several security control results evaluated as part of Risk Assessments performed prior to the first use of any new application or service supporting PCI, PHI, or other high risk business processes.

All outbound email shall be scanned, prior to leaving the University's network to ensure the University is not forwarding any viruses, worms or Trojan horses to clients or vendors. [Ref: CS199]

In addition, virus scans or integrity checks should be performed on all removable media received prior to the files being read using University-approved anti-virus software.

Electronic mail transmitted from the University or received via the Internet shall be scanned for viruses, worms and Trojan horses at the mail server, prior to being transmitted or delivered to its intended recipient. [Ref: CS201]

PCI Specific Rules: Virus scans of permanent media shall be performed at least daily on: [Ref: CS480, PCI]

- All servers connected to the University's network, including all third-party servers connected to the University's network
- All computers used for the distribution of files to third parties
- Any workstation that shares software with any other computer
- All computers running an application for which the loss of data or loss of the application poses a risk of embarrassment or monetary loss to the University

For all situations not covered above, virus scanning shall be performed at least weekly.

Whenever possible, virus scans shall be scheduled to occur automatically. [Ref: CS482, PCI]

Audit logs of scan results shall be kept for six (6) months. These logs shall note the date and times that scans occurred and any findings that were noted. [Ref: CS483]

Virus detection software shall be configured as follows: [Ref: CS484, PCI]

- At system start up, the software should perform a scan of the system that includes the Master Boot Record, any other local boot records, and also perform an integrity check of the anti-virus software itself.
- The software should clean infected files automatically. If a repair is not possible, the software should deny access to the infected file.
- The memory resident portion of the software should be loaded and enabled at system startup and:
    - Scan all files when opened, copied, moved, created or downloaded
    - Check floppies for boot viruses upon access and check floppies when rebooting the computer
    - If possible, end users should not be able to disable, change the settings or circumvent the anti-virus software
    - Forward an alert message to a virus management administration server for analysis

The University shall provide spam protection as part of its email infrastructure. The following controls shall be implemented for control of spam: [Ref: CS590]

- Email servers should be configured to prevent mail relay.
- Spam filtering software should be implemented on all email servers.
- The University should provide users with a method to report unsolicited email or other unwanted email communications.
- The University should include spam response and reporting procedures as part of security awareness training.
- The security incident response procedures should provide for the response to spam related incidents.
- Internal mass emails should be only sent after appropriate approvals by management. The UIT Strategic Communications team can help facilitate this.

01.4.03 Vulnerability Management

The University shall protect IT Resources commensurate with the assessed level of risk and utilize security baseline settings to ensure that IT resources are available for use and free from malware. IT Resource Administrators and users managing IT resources shall:

- Protect any IT resource under their management from compromise. This includes installing antivirus and relevant security patches to address security issues.
- Implement procedures that terminate an electronic session after a predetermined time of inactivity.
- Configure the IT resources to reduce vulnerabilities to a minimum.
- Periodically verify audit and activity logs, examine performance data, and generally check for any evidence of unauthorized access, the presence of viruses or other malicious code.
- Cooperate with ISPO and ISO by providing support for and/or review of administrative activities as well as allowing the performance of more sophisticated procedures such as penetration testing and real-time intrusion detection.
- Exercise due care to prevent the exploitation of technical vulnerabilities.
- Identify the primary IT Administrator responsible for overall security of each IT Resource. The IT Administrator responsible for overall security must be registered and accurate in the Point of Contact (POC) database (https://db.it.utah.edu/poc/) for each system or device. The POC receives vulnerability scans for those devices as well as reports of unusual network activity coming from or to those devices.
- Maintain a current and complete inventory of assets, which is a prerequisite for effective technical vulnerability management. The inventory shall include the software vendor, version numbers, current state of deployment (e.g. what software is installed on what systems), and the person(s) within the organization responsible for the software.
- Take appropriate and timely action in response to the identification of potential technical vulnerabilities. Use the following to establish an effective management process for technical vulnerabilities:
    - Define and establish the roles and responsibilities associated with technical vulnerability management, including vulnerability monitoring, vulnerability risk assessment, patching, asset tracking, and any coordination responsibilities required.
    - If the IT Resource Administrator assigns another individual some or all of the vulnerability management tasks, the IT Resource Administrator still retains responsibility for vulnerability management and must confirm that the required activities are taking place.

        - Review (at least weekly) technical bulletins and advisories to identify relevant technical vulnerabilities and to maintain awareness about them. Update information resources based on changes in the inventory, or when other new or useful resources are found.
    - Develop a reasonable timeline (30 days or less) to react to notifications of potentially relevant technical vulnerabilities.
    - Once a potential technical vulnerability has been identified, identify the associated risks and the actions to be taken. Such action could involve patching of vulnerable systems and/or applying other controls, depending on the nature of the vulnerability.
    - Depending on how urgently a technical vulnerability needs to be addressed, carry out any action following established change management procedures or by following information security incident response procedures.
    - If a patch is available, the risks associated with installing the patch shall be assessed (the risks posed by the vulnerability shall be compared with the risk of installing the patch). The decision to install the patch or not shall be made within 30 days of the patch being made available or identification of the associated vulnerability.
    - Test and evaluate patches before they are installed to ensure they are effective and do not result in side effects that cannot be tolerated; if no patch is available, consider other controls, such as
        - turning off services or capabilities related to the vulnerability;
        - adapting or adding access controls, e.g. firewalls, at network borders;
        - increased monitoring to detect or prevent actual attacks;
        - raising awareness of the vulnerability;
    - Keep a log for all procedures undertaken in relation to this guideline.
    - Routinely monitor and evaluate your technical vulnerability management process to ensure its effectiveness and efficiency.
    - Address systems with the most risk, first.
    - Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release.
        - Note: IT Resource Administrators may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for example, public facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.

- Establish and document a process to identify and assign a risk ranking to newly discovered security vulnerabilities.
    - Notes: Risk rankings shall be based on industry best practices. For example, criteria for ranking "High" risk vulnerabilities may include a CVSS base score of 4.0 or above, and/or a vendor supplied patch classified by the vendor as "critical," and/or a vulnerability affecting a critical system component.
- For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods:
    - Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes.
    - Installing a web-application firewall in front of public-facing web applications.
- Anti-virus – Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).
    - Ensure that all anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software.
    - Ensure that all anti-virus mechanisms are current, actively running, and generating audit logs.
- Log / document the actions taken to identify and respond to technical vulnerabilities. This protects both you and the University.

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.

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