OUTDATED as of 9/1/2016
See Policy 4-004

I. OVERVIEW

A. This document provides guidance for the implementation of the following policy: Information Security Policy – Section H: IT Resource Security:

1. The University of Utah 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:

a) Protect any IT resource under their management from compromise. This includes installing antivirus and relevant security patches to address security issues.

b) Implement procedures that terminate an electronic session after a predetermined time of inactivity.

c) Configure the IT resources to reduce vulnerabilities to a minimum.

d) 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.

e) 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.

II. GUIDELINES

A. Exercise due care to prevent the exploitation of technical vulnerabilities.

B. 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.

C. Maintain a current and complete inventory of assets, which is a prerequisite for effective technical vulnerability management. The inventory should 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.

D. 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:

1. 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.

a) 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.

2. 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.

3. Develop a reasonable timeline (30 days or less) to react to notifications of potentially relevant technical vulnerabilities.

4. 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.

5. 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.

6. If a patch is available, the risks associated with installing the patch should be assessed (the risks posed by the vulnerability should be compared with the risk of installing the patch). The decision to install the patch or not should be made within 30 days of the patch being made available or identification of the associated vulnerability.

7. 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

   a) turning off services or capabilities related to the vulnerability;

   b) adapting or adding access controls, e.g. firewalls, at network borders;

   c) increased monitoring to detect or prevent actual attacks;

   d) raising awareness of the vulnerability;

8. Keep a log for all procedures undertaken in relation to this guideline.

9. Routinely monitor and evaluate your technical vulnerability management process to ensure its effectiveness and efficiency.

10. Address systems with the most risk, first.

11. 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.

   a) 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.

12. Establish and document a process to identify and assign a risk ranking to newly discovered security vulnerabilities.

   a) Notes: Risk rankings should 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-

OUTDATED as of 9/1/2016
See Policy 4-0001

supplied patch classified by the vendor as "critical," and/or a vulnerability affecting a critical system component.

13. 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:

a) Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes.

b) Installing a web-application firewall in front of public-facing web applications.

14. Anti-virus – Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).

a) Ensure that all anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software.

b) Ensure that all anti-virus mechanisms are current, actively running, and generating audit logs.

15. Log / document the actions taken to identify and respond to technical vulnerabilities. This protects both you and the University.

III. REFERENCES

A. Contact Information Security Operations for assistance in managing technical vulnerabilities and for receiving and/or interpreting Qualys reports.

B. NIST – Creating a Patch and Vulnerability Management Program, Special Publication 800-40 version 2.0 - http://csrc.nist.gov/publications/nistpubs/800-40-Ver2/SP800-40v2.pdf

OUTDATED as of 9/1/2016
See Policy 4-004