Information System Vulnerability Management Policy

Current Version	Compliance Date	Approved Date
2.3	05/31/2018	05/08/2018

1. Purpose

The operating system or environment for all information systems must undergo a regular vulnerability assessment.

This policy reflects the University's commitment to identify and implement security controls that mitigate Information Systems (IS) risks to reasonable and acceptable levels. IS are assets of the University and require the assignment of security responsibilities to the appropriate individuals or departments.

2. Policy

Vulnerabilities to the operating system or environment for information systems must be identified and corrected to minimize the risks associated with them.

To ensure these vulnerabilities are adequately addressed, the operating system or environment for all information system resources must undergo a regular vulnerability assessment.

The frequency of these vulnerability assessments will be dependent on the operating system or environment and the information system and data classification. See Information System Vulnerability Management Standard.

3. Roles and Responsibilities

The **IS Administrator** is responsible for the following:

a. Subscribing to US-CERT notifications informing of recently released software patches and upgrades.
b. Subscribing to receive alerts from software vendors when software patches or updates are made available.
c. Using only OUHSC provided vulnerability scanning tools.
d. Reviewing monthly vulnerability scan reports to identify vulnerabilities due to missing operating system and/or software patches and/or configuration vulnerabilities.
e. Deploying all available updates and/or configuration changes that address the vulnerabilities identified during the monthly maintenance window. The IS Administrator is encouraged to use centralized tools provided by campus IT such as SolarWinds Patch Management, WSUS, and Group Policy.
f. Making an attempt to test updates, where possible, prior to deployment.
g. If reboots are required, perform those reboots during this window, to complete installation of the updates.
h. Requesting and justifying all exceptions to update/patch installation, to IT Security.
i. Verifying that identified vulnerabilities are remediated by examining the next available vulnerability scan report.
j. Removing outdated software versions, as newer versions are made available, or as necessary.
k. Remediating identified vulnerabilities, in accordance with the *OUHSC Vulnerability Management Standard.*

OUHSC IT Operations is responsible for the following:

a. When serving as the IS Administrator for patch maintenance, using SolarWinds Patch Management, WSUS, and Group Policy to deploy applicable patches.
b. Providing monthly vulnerability reports to Departmental Tier One(s).
c. Scheduling and performing monthly vulnerability scans.

OUHSC IT Security is responsible for the following:

a. Notifying IS Administrator if vulnerabilities are not mitigated in accordance with the *OUHSC Vulnerability Management Standard*.

On occasion, emergency updates are released that require remediation before the scheduled monthly maintenance plan. Emergency update deployments on distributed IT can occur as determined and planned by the software vendor and/or by the IS Owner and IS Administrator(s). Upon approval of the emergency change request by the IS Owner, emergency updates can be remediated outside of the monthly maintenance window. In case(s) of inability to reduce vulnerability, mitigation controls are to be put in place until the patch/configuration change is applied. IS Administrator(s) are responsible for submitting remediation plans to Information Security Services within two weeks of vulnerability discovery when patch(es) cannot be applied.

4. Enforcement

This policy is authorized and approved by the OUHSC Dean's Council and Senior Vice President and Provost and enforced by the Chief Information Officer. Internal Audit and other authorized departments of the University may periodically assess Business Unit compliance with this policy and may report violations to the University Administration and Board of Regents.

5. Scope

This policy applies to all OUHSC Information Systems and the individuals identified above.

6. Regulatory References

- HIPAA 45 CFR 164.308(a)(1)(ii)(B)
- Section 501(b) of the Gramm-Leach-Bliley Act ("G–L–B Act")
- State of Oklahoma Information Security, Policy Procedures Guidelines – Section 9.15 Control of Operational Software
- Payment Card Industry Data Security Standard
- Family Educational Rights and Privacy Act (FERPA): 20 U.S.C. §1232g; 34 CFR Part 99

7. Review Frequency

This policy is scheduled to be reviewed, updated, and modified as necessary, but at least annually.

8. Revision, Approval and Review

8.1 Revision History

Version	Date	Updates Made By	Updates Made
2.0	03/14/2007	Campus IT	
2.1	06/09/2016	Campus IT	Format change.

			Added roles and responsibilities.
2.2	03/12/2018	IT Security	Updated roles and responsibilities.
2.3	03/26/2018	Subject Matter Experts	Minor revisions
2.3	05/07/2018	Randy Moore	Minor revisions to correct reformatting issues with spaces

8.2 Approval History

Version	Date	Approved By
2.0	03/14/2007	Dean's Council
2.3	05/08/2018	Information Security Review Board

8.3 Review History

Date	Reviewed By
11/21/2014	Campus IT
06/09/2016	Campus IT
05/07/2018	Campus IT
05/08/2018	Information Security Review Board