Vulnerability Management Policy

Statement of Policy
Washington University in St. Louis (WashU) is committed to conducting all university activities in compliance with all applicable laws, regulations, and university policies. WashU has adopted this policy to outline the security measures required to protect electronic information systems and related equipment from unauthorized use.

Objective
This policy and associated guidance covers a well-defined and organized approach for vulnerability management to reduce infrastructure risks and integrate with patch management. To ensure confidentiality, integrity, and availability of WashU systems Office of Information Security (OIS) and Information Technology (IT) will develop a documented vulnerability management process for the efficient and effective assessment and mitigation of IT infrastructure risks.

Applicability
This policy is applicable to all WashU IT infrastructures - shared and distributed.

Audience
The audience for this policy is all WashU faculty, staff, and students. It also applies for all other agents of the university with access to WashU information and network for contracted services. This includes, but not limited to partners, affiliates, contractors, temporary employees, trainees, guests, and volunteers. The titles will be referred collectively hereafter as “WashU community”.

Roles & Responsibilities

Policy
The OIS will document, implement, and maintain a vulnerability management process for WashU. The process will be integrated into the IT flaw remediation (patch) process managed by IT.

Appropriate vulnerability assessment tools and techniques will be implemented. Selected personnel will be trained in their use and maintenance. The OIS will periodically test the
security posture by scanning the information systems owned and managed by WashU with vulnerability tools. The frequency of the scans will be scheduled based upon the level of risk and data classification.

The OIS will analyze the scans and their reports for vulnerability impact for WashU. The OIS will deliver a formal report that will identify the vulnerabilities requiring remediation or mitigation based on risk, patch requirements, and classification documented in the Vulnerability Management Operational Process. Reference the Vulnerability Management Standard for remediation and mitigation timelines. The OIS will assist with remediation or mitigation planning as needed.

The information obtained from the vulnerability scanning process will be shared with appropriate personnel throughout the organization on a "need to know" basis to help eliminate similar vulnerabilities in other information systems.

**Policy Compliance**

Systems that are not remediated or granted an exception within the 90 days will be escalated to the area business director and recommended that the vulnerable device be removed from the network until such a time that the device can be brought into compliance.

The OIS will measure the compliance to this policy through various methods, including but not limited to, reports, internal/external audits, and feedback to the policy owner. Exceptions to the policy must be approved by the OIS in advance. Non-compliance will be addressed with management, Area Specific Compliance Office, Human Resources, or the Office of Student Conduct.

**Related Policies**

None

**Reference**

*Security Controls* - NIST 800-53 Controls – WU_SSP_Controls_Workbook_DOT Rev3- RA-5 Vulnerability Scanning. (Refer to implementation Standard.)

**Policy Review**

This policy will be reviewed at a minimum every three years.

**Title:** Vulnerability Management Policy
**Version Number:** 1.0
**Reference Number:** RA-01.03
**Creation Date:** February 7, 2019
**Approved By:** Security and Privacy Governance Committee
**Approval Date:** May 5, 2019
Status: Final
Scheduled Review Date: June 1, 2022
Revision Date:
Revision Approval Date:
Policy Owner: Office of Information Security