Standard: Vulnerability Management

Effective Date:	2016.12.04
Revision Date:	2020.02.06
Review Date:	2021.02.06
Approving Body:	Director, Information Security and Compliance
Authority:	Information Security Policy
Responsible Owner:	Director, Information Security and Compliance
Classification:	Public

Purpose

The Vulnerability Management Standard describes the acceptable standards for discovering and handling vulnerabilities for systems connected to the University's networks.

Who/what does the standard apply?

The requirements in this standard apply to all University owned systems connected to the University network.

Definitions

- **Authenticated Scan**: A type of scan that requires appropriate credentials to authenticate to a system to determine the presence of vulnerability without having to attempt an intrusive scan.
- **IST:** Information Services and Technologies unit at the University of Manitoba.
- **Network Vulnerability Scanning:** A process that scans all ports and services of target hosts or appliances to identify vulnerabilities and determine whether they can be exploited.
- **Operational:** A system is operational when the system is accessible to anyone other than the system's system administrator(s).
- **Server:** Specialized computers (virtual and physical) that operate within a client/server architecture to serve the requests of client computers on the network.
- **System:** Software, hardware and interface components that work together to perform a set of business functions.
- **Vulnerability:** A weakness in a system that renders it susceptible to attacks, causing security threats to an organization.
- **Vulnerability Scanning Program:** This program is developed and approved by Information Security & Compliance. Program components will include a vulnerability scan schedule, and requirements for ad-hoc vulnerability scans.

Compliance

Systems must align to the requirements and specifications outlined within this standard. Where systems and applications are unable to comply, please submit an Information Security Decision Request to the Director of Information Security and Compliance for review.

Specifications

Requirement	Specifications
All Windows and MacIntosh desktops, laptops and servers must utilize an antivirus application.	IST will provide an antivirus application for Windows and MacIntosh devices. The anti-virus application must be installed and maintained with the most up-to-date signatures.
Monitoring vulnerability advisories and intelligence feeds.	On at least a weekly basis a review of all information security vulnerability advisories issued by trusted organizations and system vendors for issues affecting University systems maintained by IST must be undertaken. All security advisory vulnerabilities issued by a vendor must be acted upon based on the risk criticality. Critical, High and Medium vulnerabilities should be remediated accordingly.
Periodic vulnerability scanning of servers.	All servers must be scanned with the scanning tool recommended by the Director, Information Security & Compliance at the interval specified in the Vulnerability Scanning Program. All new servers regardless of purpose, must be scanned before they are operational. Authenticated scans of servers may be requested by the Director of Information Security & Compliance. Critical, High and Medium vulnerabilities identified from the scans on servers must be reviewed with Information Security & Compliance for assessment and direction on the need for remediation and rescanning post-remediation.
Threat and Risk Assessments (TRA) completed.	A TRA must be completed when there is a new system introduced into the environment or there is a modification to an existing system. A TRA may be directly requested by Information Security & Compliance, the Access and Privacy Office, Internal Audit, the Office of the Auditor General, or a faculty, business unit or entity within the University.

References

Policy, Procedure or Standard	
Information Security Policy and Procedure	
Use of Computer Facilities Policy and Procedure	