XAVIER UNIVERSITY
IT Vulnerability Management

Effective: Targeted for 3/21/22
Last Updated: 1/28/22
Responsible University Office: Information Technologies
Responsible Executive: Associate Vice President and Chief Information Officer

Scope: This policy applies to all Information Technology Resources owned or operated by or on behalf of Xavier University. This includes but is not limited to all University network infrastructure, database servers, databases, applications, computer workstations, servers, network switches, routers, printers, scanners, copiers, digital telecommunications equipment, and personally owned devices connected to any Xavier University equipment.

A. REASON FOR POLICY

The purpose of this policy is to establish minimum requirements for the activity of remediating/controlling security vulnerabilities. This document defines the requirements to manage information and networked system vulnerabilities for Xavier University. The Vulnerability Management Policy outlines the tools and processes for identifying, risk rating, prioritizing, and remediating system vulnerabilities in an effort to manage residual risk within acceptable limits as defined by the University.

B. POLICY

All Xavier University owned Information Technology (IT) Resources must be scanned in a fashion and on a schedule appropriate for the risk profile of the assets or regulatory needs. The IT Resources that are included are subject to monthly vulnerability scanning. The Information Security Office will perform these scans and review third party assessments to identify software vulnerabilities, missing system patches, and improper configurations. In the case where the vulnerability creates a heightened risk of data exposure, Xavier may disconnect, disable, and/or block the device from the Xavier network until remediation or mitigation has taken place.

C. DEFINITIONS

Information Technology (IT) Resources: University network infrastructure, database servers, databases, applications, computer workstations, servers, network switches,

routers, printers, scanners, copiers, digital telecommunications equipment, and personally owned devices connected to any Xavier University equipment.

CVSS: The Common Vulnerability Scoring System (CVSS) provides a way to capture the principal characteristics of a vulnerability and produce a numerical score reflecting its severity. The numerical score can then be translated into a qualitative representation (such as low, medium, high, and critical) to help organizations properly assess and prioritize their vulnerability management processes.

Information Security Office: The Information Security Office is led by the Director of Information Security role and includes any position description with information security as a defined job duty.

D. PROCEDURES

Vulnerability Assessment and Scanning: Vulnerability assessments scan Xavier's network, servers and applications to evaluate Xavier's risk exposure and actions to be taken to mitigate those risks. Used effectively, it will help to ensure that all software, settings, and security configurations are up-to-date, as well as help detect systemic weaknesses or deficiencies. Vulnerability scans will be conducted monthly by the Information Security Office to identify software vulnerabilities, missing system patches, and improper configurations. Sources for cybersecurity vulnerability information, CVSS scores, and related risks and exposures include: The National Vulnerability Database and the Common Vulnerability Exposure Database.

Vulnerability Remediation and Mitigation: Remediation and mitigation will be prioritized based on the degree of associated severity and the impact on the confidentiality, integrity, or availability of the vulnerable system. It will be left to the System and Application Administrators to take the vulnerability that the Information Security Office identified and remediate or mitigate it. The timeline for remediation and mitigation will begin when the Information Security Office passes on the vulnerability report to the System Administrators. In the case where the vulnerability creates a heightened risk of data exposure, Xavier may disconnect, disable, and/or block the device from the Xavier network until remediation or mitigation has taken place. If remediation or mitigation is unavailable, then a request to the CIO will need to be made to either remove the system or device or obtain a vulnerability remediation exemption.

Timeline for remediation and mitigation:

Severity CVSS Base Score	**Critical (9-10)**	**High (7-8.9)**	**Other (<7)**
Action Plan By	1 week	2 weeks	1 month
Remediation Time By	2 weeks	1 month	2 months

Vulnerability Remediation Exemptions: The CIO or Director of Information Security is authorized to approve exceptions and take action as needed to ensure that systems with un-remediated vulnerabilities do not pose a threat to Xavier resources or assets. System owners can request an exception through Information Technologies by contacting the

helpdesk. If the exception is approved the System Owner and Application Administrators are responsible for monitoring the vulnerability on a regular and on-going basis.

Chief Information Officer (CIO): The CIO acts as required to ensure that un-remediated systems or applications do not pose a threat to Xavier information systems or resources. When a critical vulnerability is not remediated within the designated timeframe or is improperly remediated, the CIO may temporarily block the system or application from the network until such time as the remediation is effectively completed.

Information Security Office: The Information Security Office will conduct University-wide scans of devices connected to the Xavier network to identify and assess system and application vulnerabilities. They will aid in interpreting scan reports, reporting false positives, and troubleshooting scan issues. They will also issue alerts and advisories about any known vulnerabilities and the recommended remediation based on information received from vendors, reliable websites, and other trusted information security sources.

System Owner and Application Administrators: System and Application Admins are responsible for the assessment and timely application of vendor-supplied security patches as well as other remediation for systems under their management and supervision. This includes monitoring vulnerabilities identified by the Information Security Office and carrying out timely remediation. If remediation is unavailable, these admins will need to report it immediately to the Information Security Office to address the next steps in mitigating or accepting the risk.

E. EXHIBITS

None

F. HISTORY

No previous policy.

Other applicable policies and/or resources:

https://www.xavier.edu/policy/technology

Information Security Policy:

https://www.xavier.edu/policy/documents/XavierUniversityInformationSecurityPolicy.pdf