University of CINCINNATI	Policy Title: **Vulnerability Management**	Policy Number: **9.1.2**
Category: Information Technology	**Effective Date:** 06/01/2023	**Policy Owner:** VP & CDO, Digital Technology Solutions
Policy applicable for: Faculty/Staff/Affiliates	**Prior Effective Date:** 06/24/2021	**Responsible Office:** Office of Information Security

Background

Vulnerability management is an essential component of any information security program and is vital to effective management of information systems and reduction of associated risk to the university. Vulnerability assessments are used as a means of identifying assets connected to the university's network and the weaknesses associated with them, as well as assessing the risk of those weaknesses. After identification, the next step is to address these vulnerabilities. The University of Cincinnati strives to continually improve its security posture through timely identification and remediation of vulnerabilities.

Policy

All university owned or operated information technology systems, computing and non-computing (IoT), and devices accessing the university network must be protected through the deployment and installation of software updates, patches, service packs, hot fixes and signatures in a timely manner. Responsible Personnel (i.e. Data Custodians, Data Stewards, System Owners and Administrators, or other university community members tasked with the operation or management of systems and servers which store or provide access to institutional data) must monitor for the latest update releases, ensure they are applied on a regular schedule, and check to ensure the completeness and effectiveness of their patching processes. All university information systems, devices and applications must be maintained according to manufacturer recommendations or follow a university approved maintenance schedule, which includes using only supported operating systems and applications. End-of-life operating systems and applications must be deprecated prior to the end-of-life date. Failure to do so may result in removal of access to university resources.

The Office of Information Security (OIS) will conduct periodic or continuous vulnerability assessments of university systems. Targeted vulnerability assessments may also be implemented on an as needed basis, determined, and administered exclusively by OIS, or an authorized entity discussed below. A centrally managed vulnerability assessment platform will be utilized and administered by OIS.

All steps must be taken to ensure the proper installation of patches and/or remediation of vulnerabilities. This includes rebooting, registry edits, and uninstallation of application and/or services as recommended.

All security patches must be installed unless testing against critical systems results in system instability or a reduction in essential functionality. Exceptions must be documented and a plan of action to eliminate the exception must be implemented. OIS reserves the right to deem any security patches critical and request immediate installation.

Prior to the implementation of a new system, or major change of an existing system in the university environment Responsible Personnel must perform a vulnerability scan using a university centrally managed vulnerability solution, remediate any vulnerabilities identified, and maintain proof of remediation on record.

Responsible Personnel must allow access to the university vulnerability management agent or allow for the ability to run appropriate level vulnerability scans. Use of any other network-based tools to scan or verify vulnerabilities must be approved in advance by OIS. Once vulnerability assessments have been conducted, OIS will communicate as described in the Vulnerability Management Procedure. It is the responsibility of university community members to cooperate fully with any vulnerability assessment being conducted and remediation guidance on systems for which they are accountable.

The Office of Information Security may engage with third parties to conduct internal or external vulnerability assessments or penetration testing as necessary. OIS reserves the right to remove or isolate vulnerable assets from the university's network at any given time without prior communication. Once the cyber threat is contained, OIS will work with the Responsible Personnel to seek a resolution.

Any exceptions to this policy must be documented by an approved Risk Acceptance Form (RAF) on file with the Office of Information Security. Additional mitigating controls may be required where appropriate.

Definitions

Responsible Personnel: Data Custodians, Data Stewards, System Owners and Administrators, or other university community members responsible for the operation and management of systems and servers which store or provide access to institutional data.

Vulnerability Remediation: the process of mitigating or reducing identified vulnerabilities on a system to bring the overall risk associated with that asset down to an acceptable level.

Contact Information

Office of Information Security	513-558-ISEC (4732)	infosec@uc.edu

Related Links

Vulnerability Management Procedure
Risk Acceptance Policy