University of CINCINNATI	*Policy Title:* **Vulnerable Electronic Systems**	Policy Number: **9.1.2**
Category: Information Technology	**Effective Date:** 06/24/2021	**Policy Owner:** VP & CIO, UC Information Technologies
Policy applicable for: Data Custodians	**Prior Effective Date:** 09/25/2019	**Responsible Office(s):** 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 by identifying and remediating vulnerabilities.

Policy

All university owned or operated computer systems and devices must be protected through the deployment and installation of software updates, patches, service packs, hot fixes and signatures in a timely manner. Data Custodians are responsible for monitoring the latest update releases, applying them on a regular schedule and checking to ensure the completeness and effectiveness of their patching processes. All university information systems and devices and applications must be maintained according to manufacturer recommendations or follow a university approved maintenance schedule. This 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.

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 system will be utilized and administered by OIS.

The university classifies vulnerabilities as follows:

- **Catastrophic**
  Out-of-band catastrophic vulnerabilities as deemed by OIS or university leadership must be remediated as soon as possible, but no later than 7 days. Due to the extremely critical nature these vulnerabilities exemptions are not available without executive leadership approval and documentation.

- **High (Level 4-5)**
  High level vulnerabilities must be remediated as soon as reasonably possible, but no later than 30 days after release.

- **Moderate (Level 3)**
  Moderate level vulnerabilities must be remediated as soon as reasonably possible, but no later than 60 days after release.

- **Low (Level 2)**
  Low level vulnerabilities must be remediated as soon as reasonably possible, but no later than 90 days after release.

- **Informational (Level 1)**
  Informational vulnerabilities are often deviations from industry best practice and when possible, should be remediated within 180 days.

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 reduction in essential functionality. Exceptions must be documented and a plan of action to eliminate the exception must be implemented. The Office of Information Security 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 on the university's network, Data Custodians must perform a vulnerability scan using a university centrally managed vulnerability scanner. Data Custodians must remediate any vulnerabilities discovered and maintain proof of remediation.

Data Custodian and/or System Owners must allow access to the university vulnerability management agent or allow for the ability to run authenticated 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 to Data Custodians as described in the Vulnerability Escalation Procedure. It is the responsibility of Data Custodians to cooperate fully with any vulnerability assessment being conducted 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 Data Custodians to seek a resolution.

Any exceptions to this policy for end-of-life operating systems/applications, catastrophic or high-level vulnerabilities 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

Data Custodian: computer system administrators 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 Escalation Procedure
Data Governance & Classification Policy
Risk Acceptance Policy