University of CINCINNATI	*Policy Title:* **Vulnerable Electronic Systems**	Policy Number: **9.1.2**
Category: Information Technology	**Effective Date:** 09/25/2019	**Policy Owner:** VP & CIO, UC Information Technologies
Policy applicable for: Data Custodians	**Prior Effective Date:** 09/26/2018	**Responsible Office(s):** Office of Information Security

Background

Vulnerability management is an essential component of any information security program and the process of vulnerability assessment is vital to effective management. 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 take measured and documentable steps to remediate these vulnerabilities. The University of Cincinnati strives to continually improve its security posture by protecting university data and improving the security of the university community.

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 anti-virus signature additions 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 systems, devices and supporting systems for organizational information systems must be maintained according to manufacturer recommendations or follow a university approved maintenance schedule. Critical security patches, as deemed by the vendor, must be installed on applicable systems within 14 days of release. Noncritical patches must be deployed as soon as possible, but no later than 30 days after release. All security patches must be installed unless testing against critical systems results in system instability or reduction in needed functionality. Exceptions must be documented and a plan of action to eliminate the exception must be implemented. The Office of Information Security (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 on the universities network, Data Custodians must perform a vulnerability scan using a university centrally managed vulnerability scanner. Data Custodian must also remediate any vulnerabilities discovered and maintain proof of remediation. If a Data Custodian is using a standard image that has been tested and deemed appropriate, no further scan is necessary in those instances. Data Custodians are also responsible for remediation of all vulnerabilities communicated by OIS.

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. Vulnerability assessments will be conducted in such a way as to cause minimal noticeable impact to university operations. 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 with Data Custodians as described in the Vulnerability Escalation Procedure (see Related Links section below). It is the responsibility of Data Custodians to cooperate fully with any vulnerability assessment being conducted on systems for which they are held accountable. Data Custodians shall be responsible for the remediation of any discovered vulnerabilities as described in the Vulnerability Escalation Procedure.

OIS 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.

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

History

Issued: 01/04/2008
Reviewed: 03/07/2016
Revised: 11/21/2016
Revised: 10/25/2017
Revised: 09/26/2018
Reviewed: 09/25/2019