— UNIVERSITY POLICY —

Vulnerability Management Policy

Accommodations for individuals with disabilities in accessing these policies are available upon request by emailing accessiblepolicy@wcupa.edu

Purpose and Scope

The Vulnerability Management Policy for West Chester University Information Services & Technology computing facilities, systems and resources applies to all members of the University community, including faculty, students, staff, contractors, and affiliates, and to authorized visitors, guests, and others for whom University technology resources and network access are made available by the University. This policy also applies to campus visitors who avail themselves of the University's temporary visitor wireless network access service or eduroam access, and to those who register their computers and other devices through Conference Services programs or through other offices, for use of the campus network.

Policy Statement

The purpose of this policy is to ensure that the confidentiality, integrity, and availability of all West Chester University servers remains at the highest levels by installing vendor updates in a timely fashion and adhering to configuration/system hardening best practices. Alerts and notifications of system vulnerabilities, whether discovered internally or brought to the attention of IS&T (Information Services & Technology) from a third party, will be cataloged and responded to according to the criticality of each notification.

This policy applies to all university owned or supported servers, regardless of host operating system or whether the server is a physical device or virtual machine. Exceptions may be made, at the discretion of IS&T and the Information Security Office, based on legitimate need to support legacy software and/or hardware or facilitate the continuation of critical business processes.

All Microsoft Windows servers will have Windows Security Patches installed during the monthly maintenance cycle. These updates may also include patches which affect the operation of servers and services. Linux-based servers must also be patched in a timely manner to ensure operating systems are as secure as currently possible. The timeline and frequency of patches issued for various Linux distributions will vary by both vendor and version of the operating system in use.

In addition to requiring operating system updates to be consistently installed, IS&T insists that the software running on university-owned servers also be installed with haste. While numerous avenues to alert IS&T system administrators of vulnerable software exist, the primary source of this information will be from the Cybersecurity and Infrastructure Security Agency (CISA).

Procedures

CISA conducts weekly scans of WCU's registered server environment and provides updated reports of newly discovered security flaws or vulnerabilities in the software running on the systems within the scope of the weekly scans. Based on the potential danger posed by the vulnerability discovered, as well as the potential ease with which an attacker could target the flaw, CISA assigns

vulnerability a numeric score from 1.0-10.0. These scores are also compiled into four severity levels:

- Critical
- High
- Medium
- Low

Severity is also impacted if it is a Known Exploited Vulnerability (KEV), as opposed to a vulnerability that is only theoretically able to be leveraged by attackers. Recommended timelines for remediations of discovered vulnerabilities are also determined by their severity score and if it is a KEV. Targeted remediation schedules will be:

- Critical – within 15 calendar days
- High – within 30 calendar days
- Medium – within 60 calendar days (If in scope)
- Low – within 90 calendar days (If in scope)

Definitions

BOD – Binding Operational Directive – a compulsory direction to federal, state departments or associated agencies and contractors.

CISA – The Cybersecurity and Infrastructure Security Agency – Government agency that leads the national effort to understand, manage, and reduce risk in our cyber and physical infrastructure.

KEV – Known Exploited Vulnerability – A discovered vulnerability that has been proven or viewed to be effectively exploited on systems in production environments.

References

CISA BOD 19-02: https://www.cisa.gov/sites/default/files/bod-19-02.pdf

Executive Order 14028 "Improving the Nation's Cybersecurity"
https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

End of Life Software Support and Access Policy
https://wcupa.sharepoint.com/:b:/s/President/EWWSrY9ipxRBmQJ-35DZC5wB_Fz7MlupwRzb3Pw5ya5vPg?e=diKF7B

Reviewed by: **Information Services & Technology**

Policy Owner: **Stephen Safranek**

Chief Information Security Officer
Information Services & Technology

Office of Labor Relations Review: Review completed December 27, 2022

Approved by:

JT Singh
Senior Associate VP & CIO
Information Services & Technology
Date: October 13, 2023

Effective Date: **October 13, 2023**

Next Review Date: October 13, 2027

History:

Initial Draft: 9/23/2022

Initial Approval: 12/27/2022

Review Dates: 9/14/2022, 12/27/2022, 10/13/2023, 11/14/2023

Amended: