— UNIVERSITY POLICY —

End of Life Software Support and Access Policy

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

Purpose and Scope

The End of Life Software Support and Access 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 data and systems remains at the highest levels by not utilizing or deploying hardware and software that is no longer supported by the manufacturer.

This policy applies to all members of the West Chester University community, such as faculty, staff, students, vendors, volunteers, and guests ("Users") who

utilize West Chester University computing resources or access the campus network, whether locally or remotely. Exceptions may be made, at the discretion of Information Services & Technology (IS&T), for a small number of machines based on legitimate need to support legacy software and/or hardware.

West Chester University IS&T requires Users and University partners to adhere to information security best practices by only utilizing devices and software that can receive critical system and security updates. Vendors typically announce the release of new products and software versions of existing offerings and may eventually declare end of life and end of support on specific products. End of Life (EOL) software is no longer eligible to receive critical security updates that are integral to the ongoing defense against new threats and vulnerabilities. Operating systems and applications that are End of Life (EOL) and do not receive security updates, may not be used on general computing devices.

In general, best practices for keeping systems secure through vendor updates are as follows:

- Patch the system if updates are available
- Replace the system with a new device that is able to perform the business function if patching the original system is not viable
- Remove the system from network if it cannot be replaced
- If the system performs a vital function, and cannot feasibly be replaced, the device may stay on the network with CISO (Chief Information Security Officer) approval. The system owner also must work with IS&T to develop a security plan detailing how the system will be secured to compensate for lack of critical updates.

Policy Framework

Devices procured by IS&T running End of Life (EOL) software will be upgraded or replaced in order to access the University network or sensitive/confidential data. Likewise, servers must not host or utilize software that is deemed End of Life (EOL), and servers must be eligible for all security updates in accordance with IS&T's Vulnerability Management Policy (formerly Server Patch Management Policy).

Systems purchased and owned by departments or individual users must also comply with this End of Life (EOL) software policy to comply with security best practices and avoid compromise or unintentional data exposure. Users may contact IS&T for advice and recommendations in the event a device in their possession is using an application or operating system that the vendor has announced will be retired and nearing End of Life. Users should be on alert for notifications or communications from vendors informing them of critical updates or impending End of Life (EOL) status of software. Owners of devices using End of Life (EOL) software discovered hosting sensitive/confidential University data or connected to the University network will be notified so that corrective action may be taken. Access may be revoked to mitigate exposure as/ if needed, and continued use after notification could face further action.

Policy Exceptions

Exceptions to this policy may be considered for systems that host applications or operating systems that are End of Life (EOL) but are critical to specific University or research-related functions. IS&T will evaluate exception requests on a case-by-case basis to determine the level of risk presented by each request, as well as investigate any other options for meeting the needs of the requestor. Non-

compliant systems that do not obtain exception approval may face removal from the WCU network and/or other take-down action. All approved exceptions are temporary and must be replaced with compliant solutions when available.

Definitions

End of Life (EOL) – the useful life of an operating system, application, hardware, firmware, or service. After this period, the vendor will stop updating, supporting, marketing, or selling that item.

References

Information Technology Procurement Policy
http://www.wcupa.edu/policies/documents/Information%20Technology%20Procurement%20Policy.pdf

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: 11/1/2022

Initial Approval: 12/27/2022

Review Dates: 11/1/2022. 10/23/2023, 11/15/2023

Amended: 11/15/2023