Standard Title: Minimum System Configuration
Standard

Associate VP for IT & CIO	Next Review Date: 2/3/2024

1. Purpose

Radford University is committed to maintaining a reliable and secure information technology environment. In order to accomplish this, it is important to ensure that all interaction with the university information technology environment meet or exceed this standard. This standard is intended to aid in reducing vulnerabilities in systems that interact with the university information technology environment; sometimes referred to as ‘hardening a system’.

2. Standard

Information technology x Is connected to a university network; or

x Interacts with university sensitive systems, or

x Stores, accesses or transmits university data.

This standard applies whether the information technology resource is local to the university or remotely located.

The owner of a personal information technology device may use it at his or her discretion; however, once that device interacts with the university information technology environment, connects to the university network, or is granted access to university data, it is then subject to applicable laws and regulations, and to university policies, procedures and standards.

2.2 Responsibilities

Responsible parties must ensure that information technology resources under their control meet the procedures set forth in section 3.0 of this standard. They must also ensure that users of those resources conform to all university policies, procedures and standards.

3. Procedures

Responsible parties must adhere to these minimum information technology security standards, including but not limited to:

- Apply system patches and maintain the operating system and application software per the following requirements:

  Cadence:

Table 1: Regular Patching Schedule Cadence

Item	Frequency
Windows Servers: Monthly	Monthly
Linux Servers: Monthly	Monthly
Other Windows Devices: At least Monthly	At Least Monthly
Classroom Devices, Load Balancers, DHCP and Internal DNS appliances	Quarterly
Software Update Review: review for appliances and network devices	Quarterly

Security appliances

For clarification or questions about enforcement, contact the CISO.

4. Definitions

CVE – refers to the “Common Vulnerabilities and Exposures” system, which is maintained by the United States' National Cybersecurity FFRDC, operated by The MITRE Corporation, provides a tracking mechanism for vulnerabilities and a standardized rating system that is used to communicate the severity of a vulnerability.

Responsible Party – Individuals, groups, departments or organizations responsible for ensuring the ongoing security of the information technology resource(s) that have been granted permission to interact with the university information technology environment or store, access or transmit university data.

Information Technology Resource – Any entity such as a computer and associated peripherals owned by Radford University or used to store, access or transmit university data, including

Reviewed: 11/21/2022
Revised for updated template.
Approved: November 21, 2022 by Associate Vice President for Information Technology & CIO, Ed Oakes

Reviewed: 2/3/2023
Revised to include to
& to by