RADFORD UNIVERSITY

Information Technology Policy and Procedures

Standard: Minimum System Configuration

Standard Title: Minimum System Configuration Standard	**Effective Date: 2/6/2023**
Standard ID: IT-5214s	**Approval Date: 10/8/2012**
Oversight Executive: 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 resources that interact with the university information technology environment must be securely maintained, and must be associated with a responsible party.

2.1 Scope

This standard applies to any information technology resource that:

- Is owned or managed by the university; or
- Is connected to a university network; or
- Interacts with university sensitive systems; or
- 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 - (Firewalls, IPS, VPN)	Semi-Annually
Network devices – (network switches, and VoIP)	Annually

  - Vulnerability Management:
    The normal patching cadence is superseded when significant vulnerabilities are discovered or disclosed. The following criteria defines when the normal patching cadence is overridden.

Table 2: Vulnerability Remediation Timeframes

Severity	Time
Critical Vulnerabilities (Internet Facing Systems)	48 hours
Critical Vulnerabilities (Internal Systems Only):	2 weeks
High Vulnerabilities	30 days
Medium or Low	System Cadence as per Table 1

    - **Critical Vulnerabilities (Internet Facing Systems)**: Common Vulnerabilities and Exposures (CVE) of "Critical", the affected Radford system is exposed to the Internet, and the vulnerability is actively being exploited in the wild. Patch or address as soon as possible, within 48 hours or sooner. This work takes precedence over all other work, and may also involve the activation of the Cyber Security Incident Response Team (CSIRT).

- **Critical Vulnerabilities (Internal Systems Only)**: CVE of "Critical", affects Radford systems that are not exposed to the internet, and the vulnerability is actively being exploited in the wild. Patch or mitigate within 2 weeks.
- **High Vulnerabilities**: CVE of "High" and affects Radford systems. Patch or mitigate within 30 days.
- **Medium or Low Vulnerabilities**: All other vulnerabilities to be tracked and addressed within the normal patching cadence.

- Change Window: the change window is Monday through Thursday between 4 and 7 a.m. All changes should be scheduled to occur within these timeframes. Changes outside this schedule require out-of-band approval by IT management.
  - NOTE: Holiday schedules may diverge from this schedule.

- Reboot: all updates of all devices must include a reboot. If a reboot during the change window is not feasible, then an out-of-band reboot must be scheduled and approved by IT management.

- Install antivirus software and ensure virus definitions are updated at least daily. The justification for exceptions should be documented.
- Install and maintain a firewall to limit network connections. The justification for exceptions should be documented.
- Encrypt the storage and transmission of sensitive data in compliance with IT policy 5100 – Encryption Policy.
- Configure and maintain logical access controls in accordance with Information Technology Security Standard 5003s-01.
- Require complex rules for the formation of secure passwords in accordance with Information Technology Security Standard 5003s-01.
- Maintain physical control of the asset.
- Maintain an inventory of information technology resources. The justification for exceptions should be documented.
- Adhere to the principle of least privilege.
- Ensure backups for recovery purposes.
- Alert the CISO or IT Security Office should an information security incident occur.

3.1 Enforcement

The university reserves the right to assess whether information technology resources meet this standard. Non-compliance with this standard is considered a serious offense. Response to noncompliance may include, but is not limited to, the following:

- The university reserves the right to refuse connections to any information technology resource that does not meet this standard.
- The university reserves the right to disconnect or disengage from any information technology resource that is suspected to be non-compliant with this standard.
- In cases where the university information environment is threatened by improperly maintained resources (university owned or privately owned) the Information Security Officer (ISO) will act to eliminate the threat.

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, and 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 those in contracts or private activities associated with the university, and privately owned technology devices that interact with the university information technology environment or store, access or transmit university data.

ISO: Information Security Officer. The agency manager responsible for information security at Radford University.

5. Related Information

IT 5003s-01 – Information Technology Security Standard

IT 5100 – Encryption Policy

6. Policy Background

7. Approvals and Revisions

Approved: October 8, 2009 by Vice President for Information Technology & CIO, Danny Kemp

Reviewed: 10/8/2012
No changes.
Approved: October 8, 2012 by Vice President for Information Technology & CIO, Danny Kemp

Reviewed: 5/18/2018
No changes
Approved: May 18, 2018 by Vice President for Information Technology & CIO, Danny Kemp

Reviewed: 5/3/2021
Reviewed with minor wording changes for clarification.
Approved: May 3, 2021 by Associate Vice President for Information Technology & CIO, Ed Oakes

RADFORD UNIVERSITY

Information Technology Policy and Procedures

Standard: Minimum System Configuration

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 defined patching cadence, vulnerability management, change windows, and reboot requirements.
Approved: February 3, 2023 by Associate Vice President for Information Technology & CIO, Ed Oakes