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 with timely updates.
- Where applicable, install antivirus software and ensure virus definitions are updated.
- Where applicable, install and maintain a firewall to limit network connections.
- Encrypt the storage and transmission of sensitive data in compliance with IT policy 5100.
- Configure and maintain logical access controls.
- Require complex rules for the formation of secure passwords.
- Maintain physical control of the asset.
- Where applicable, inventory of information technology resources.
- Adhere to the principle of least privilege.
- Ensure backups for recovery purposes.
- Alert the university 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 ISO.

4. Definitions

**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 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

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