Radford University | Information Technology Services

Policy Title: Data Storage and Media Protection	**Effective Date: 12/18/2008**
Policy ID: IT-PO-5102	**Approval Date: 5/14/2025**
Oversight Executive: Associate VP for IT & CIO	**Next Review Date: 5/14/2026**

1. Purpose

Radford University is committed to maintaining a reliable and secure technology infrastructure. Securing the storage of media where sensitive data is stored is critical to the security of University information. This policy provides guidelines for handling sensitive data and protecting data from compromise.

2. Policy

- Data owners are responsible for classifying the sensitivity of their data and for notifying system owners of that sensitivity and its data protection requirements.
- Data custodians are individuals or entities that are in physical or logical possession of data for owners. Custodians are responsible for protecting the data in their possession from unauthorized access, alteration, destruction, or usage.
- **Highly sensitive data** is prohibited from being stored on any mobile device or removable media, including laptops and non-network drives, and USB drives or removable hard drives, unless the data is encrypted and an exception identifying the business need, risks involved, mitigating security controls, and acceptance of any residual risk is approved by the CIO or CISO.
- Data storage media containing highly sensitive data must be physically and logically secured.
- Employees who have approval to store highly sensitive data on mobile devices must receive security awareness training specific to data media protection requirements.
- Only authorized personnel are permitted to pick up, accept, transfer, or deliver data storage media containing highly sensitive data including tape backups. Backup tapes must be secured in a locked enclosure during transport and moved directly from the data center to the offsite storage vault.
- All portable devices capable of storing information, such as tablets, mobile phones, portable hard drives, removable disks drives, jump drives, and other storage media are required to be purged of all data when they are reassigned, salvaged, or transferred to another agency.

3. Procedures

4. Definitions

Highly Sensitive - University data which, because of its potential risk in the event of disclosure, alteration, or destruction, is approved for use only on a very limited basis and with special security precautions. This includes personally identifiable information that can lead to identity theft exposure. The following data is defined as Highly Sensitive:

a. Social Security Number;
b. Driver's license number or state identification number issued in lieu of a driver's license number;
c. Passport or Visa information/number;
d. Financial bank/account numbers, credit card or debit card numbers; or

e. Health information, that if exposed, can reveal an individual's health condition and/or history of health services use.

Encrypted: The transformation of data through the use of an algorithmic process into a form in which there is a low probability of assigning meaning without the use of a confidential process or key, or the securing of the information by another method that renders the data elements unreadable or unusable.

5. Related Information

IT-5102s – Data and System Classification Standard

6. Policy Background

7. Approvals and Revisions

Reviewed: December 18, 2008 by Information Technology Advisory Committee
Approved: December 18, 2008 by Radford University Cabinet

Reviewed: May 7, 2022 by the Information Security Officer
Approved: May 11, 2022 by Associate VP for Information Technology & CIO

Reviewed: 8/3/2024
Replaced Highly Sensitive definition with the correct definition. Minor wording changes.

Reviewed: 5/12/2025
Updated wording about mobile devices and risk acceptance.
Approved: May 14, 2025 by Associate VP for Information Technology & CIO Ed Oakes.