Information Security Standard

Media Handling and Disposal Standard

Initially Approved: September 25, 2015
Revised: March 30, 2020 (as the Media Handling and Disposal Standard)
Administering Office: Office of the CIO

I. STANDARD STATEMENT

This standard, operating under University Policy 117 Information Security, establishes controls that prevent unauthorized disclosure, modification, removal, or destruction of information stored on media.

II. SCOPE AND APPLICATION OF THE STANDARD

This standard applies to all employees, vendors and agents operating on behalf of Western Carolina University.

III. DEFINITIONS

Media for the purpose of this standard is defined as physical storage that contains data such as removable and non-removable hard disk drives, magnetic tapes, DVD and CD discs, USB flash drives, and all other types of removable storage.

IV. MEDIA HANDLING AND DISPOSAL STANDARD

- **Management of removable media**
  - WCU's Data Handling Procedures classify removable media in the "Low Security Zone." This means that no sensitive data will be stored on removable media. The only exception is for course-related student data on removable storage if it is encrypted and removed after one year. Refer to the Use of Cryptographic Controls Standard for information regarding data encryption.
  - Removable media can degrade and become unusable over time. Important data should be transferred to fresh media after three years. Additionally, important data must also be stored in another location to mitigate the risk of degraded or lost removable media.
  - All removable media will be stored in a safe and secure environment to prevent damage, loss, or theft.

- **Disposal of media**
  - Media that has been used will be disposed of securely when no longer required or needed. Where removable media on which PII is stored is disposed of, secure disposal procedures should be used to ensure that previously stored PII will not be accessible.
  - All media, as defined in this standard, must be disposed of according to the IT Surplus Hard Drive and Data Disposal Process with the exception of CD, DVD and floppy discs, which may be rendered unusable by breaking or shredding the disc without utilizing the IT disposal process.
- **Physical media transfer**
  - Media containing data will be protected against unauthorized access, misuse, or corruption during transportation.
  - Any media containing sensitive data must be shipped by a tracked carrier with a recipient signature required. For encrypted data, the encryption key should only be released after the package has arrived and been signed for.
  - Legal advice should be sought to ensure compliance before media containing encrypted information or cryptographic controls are moved across jurisdictional borders.

V. ENFORCEMENT

Failure to comply with this standard will increase the chance of a data breach which may result in the imposition of fines, or other significant penalties against WCU, and disciplinary action against employees.

VI. REFERENCES

International Standards Organization (ISO/IEC 27002:2022, Clause 7 Physical Controls)

45 CFR Part 164, Subpart C, Security and Privacy

University Policy 117 Information Security

Data Handling Procedures Related to the Information Security and Privacy Governance Policy

Use of Cryptographic Controls Standard
IT Surplus Hard Drive and Data Disposal Process