FERRIS STATE UNIVERSITY

Media Sanitization Standard

Effective Date: 10/10/2017
Owner: CTO/IT Security

INTRODUCTION

This document provides standard mode of sanitization operation for the assets defined in the "scope" section. The standard is in alignment with Ferris' data classification policy and data handling standards for all data users:

SCOPE

The standard is designed to provide a uniform process for proper handling of electronic media

- All University owned/leased equipment in any area including but not limited to scope of HIPAA, PCI DSS, FERPA
- All electronic media storage (hard drives, memory cards, USB drives, etc.). "Electronic media" is defined as any electronic medium capable of storing data
- Electronic media storage leaving the University, being disposed or otherwise dispositioned for repair, resale, donation, etc.

PROCEDURE

The procedure is based on NIST SP800-88r1, "Guidelines for Media Sanitization". All service requests or incidents need to be submitted to the Technology Assistance Center. For specific directions and recommended methods for sanitization refer to *Section 5* "Summary of Sanitization Methods" and *Appendix A* "Minimum Sanitization Recommendations". At minimum for FSU, the electronic media must be sanitized using method 1 AND 2 OR method 3.

1. Cleared first using a vendor supplied method or University approved and licensed tool to overwrite the data on the electronic media with at least 1 DoD approved pass (if applicable)
   AND
2. Purged using cryptographic erasure (CE) or another FSU IT Security approved and licensed tool to overwrite the data on the electronic media with at least 1 DoD approved pass
   OR
3. Destroy using University provided media shredder (where technically feasible and without endangering the asset specialist health) or other applicable method as outlined in the "Minimum Sanitization Recommendations" and approved by IT Security

VERIFICATION

Provide documented evidence of the performed procedure and create searchable records for an extended period of time of at least six years.

- Obtain record/report of the sanitization (clear, purge, destroy)
    - Who completed the procedure? Who was present to witness it? Who obtained the drive? Who verified it was erased?
    - Where it was sanitized? For example, IT controlled area with the attestation of a colleague
    - When was the sanitization performed? Date/time
    - What was sanitized? Record the hard drive serial number, any other unique identifiers, and include photograph to show evidence of the sanitization (clearing, purging, or destruction)
    - How was it sanitized? Include the pass and any evidence it was completed
    - Why was it sanitized? Reason for the procedure. For example, resale, internal redistribution, vendor repair, resale, recycling, etc.
- Upload the report with the who, what, when, where, and how to a ticket in Cherwell to keep historical record

REFERENCES

- Data Classification Policy
    - https://ferris.edu/HTMLS/administration/buspolletter/information/data-classification-policy.pdf
- Data Handling Standards for All Data Users
    - https://ferris.edu/HTMLS/administration/buspolletter/information/Data-Handling-Standards.pdf
- FSU Technology Assistance Center
    - https://ferris.edu/TAC/
- NIST-SP800-88r1 Guidelines for Media Sanitization".
    - http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf