UF UNIVERSITY of FLORIDA Health Science Center

Security Program for the Information and Computing Environment

Standard

Standard: PS0003.02	Category: Physical Security	Version Date: 02/22/2010
Title: **Device and Media Destruction Standard**		Effective Date: 04/01/2008
Originating Unit: Security Program for the Information and Computing Environment Project		Last Review: 12/04/2009
Review Resp: HSC Chief, Information Security		Next Review: 12/04/2012

Purpose:

To establish standard requirements and responsibility for the receipt, removal, re-use, and disposal of any Information Asset containing Restricted or Sensitive information or the movement of Restricted or Sensitive information itself into or out of the UF HSC or throughout the UF HSC.

References:

1. UF Policies and Procedure: Finance and Accounting: University Property Services: http://fa.ufl.edu/uco/handbook/handbook.asp?doc=1.4.4.1
2. Policy PS0003: Device and Media Controls
3. NIST Special Publication 800-88 Guidelines for Media Sanitization http://csrc.nist.gov/publications/PubsSPs.html
4. NIST Special Publication 800-36 Guide for Selecting IT Security Products – 5.9 Media Sanitizing http://csrc.nist.gov/publications/PubsSPs.html
5. SPICE Approved Media Sanitizing Tools https://security.health.ufl.edu/isa_ism/recommended_technologies.shtml#disposal
6. UF HSC Electronic media disposal service: https://security.health.ufl.edu/disposal
7. National Association for Information Destruction, Inc.: http://www.naidonline.org/

Standard:

1. All covered Information Assets when re-used, removed, donated, sold, or disposed of shall have all information removed and/or destroyed in such manner that the information cannot be retrieved, even partially, by conventional means or commercially available processes.
2. Removal and destruction of any (or potential) Restricted and/or Sensitive information shall be based on common standards and practices while considering the safety of the individual charged with executing the process.
3. A record shall be maintained detailing the property decal number, time and date, a description of the Information Asset, the disposition of the Information Asset, the procedure employed to remove and/or destroy the information, and the individual executing the procedure.

4. Acceptable methods of data destruction are as follows:
    a. Overwriting – Unlike other data destruction methods, overwriting preserves the media for re-use after the data destruction process. This process includes overwriting not only the logical storage location of a file(s) (*e.g.*, file allocation table) but also all addressable locations. The overwriting process will replace written data with random data. A minimum of 3 over writing passes are required. Overwriting can generally be applied to optical, magnetic or flash media. Overwriting cannot be used for media that are damaged or not rewriteable. Acceptable overwriting tools can be found at the link in reference 5.
    b. Degaussing - Degaussing is exposing magnetic media to a strong magnetic field in order to disrupt the recorded magnetic domains. A degausser is a device that generates a magnetic field used to sanitize magnetic media. Degaussing can be an effective method for purging damaged or inoperative media, for purging media with exceptionally large storage capacities, or for quickly purging diskettes. Degaussing is useful for purging data on hard disk drives in disrepair that need to be returned to manufacturers under warranty. Degaussed media should not be expected to be re-used. The HSC Security Office has a degausser for use on HSC media. See the link in reference 5.
    c. Destruction - The HSC Security Office has contracted with an outside facility for media destruction services available for use by all HSC Units. See the link in reference 6. Should HSC staff chose to securely destroy their own media, the following methods must be used.
        i. Disintegration, Pulverization, Melting, and Incineration are designed to completely destroy the media and therefore any data it contains. They are typically carried out at an outsourced metal destruction or licensed incineration facility with the specific capabilities to perform these activities effectively, securely, and safely.
        ii. Shredding can be used to destroy flexible media such as diskettes, CDs or DVDs once the media are physically removed from their outer containers. The shred size of the refuse should be small enough that there is reasonable assurance in proportion to the data confidentiality that the data cannot be reconstructed.
        iii. Optical mass storage media, including compact disks (CD, CD-RW, CD-R, CD-ROM), optical disks (DVD), and MO disks, must be destroyed by pulverizing, crosscut shredding or burning. When material is disintegrated or shredded all residues must be reduced to nominal edge dimensions of five millimeters (5 mm) and surface area of twenty-five square millimeters (25 mm2).
        iv. Electronic media disposal service companies contracted by HSC Units should be certified by the National Association for Information

Destruction (NAID certified.) Contact UF Purchasing for media disposal service companies under contract.

5. Any time a new type of media is encountered, Unit ISMs should verify that the chosen method of data destruction is effective on the new media.
6. Almost all computers and mobile devices, including cell phones, implement some form of storage media and should be handled accordingly. Care must be taken at the time of disposal or recycle to discover the storage within and destroy the data it stores according to these standards. If the existence of internal storage cannot be definitively ruled out, then the device must be destroyed.