PROCEDURES FOR ELECTRONIC MEDIA DISPOSITIONS

Who Should Know This

This standard applies to all FSU staff that provide IT support services. IT Staff must read and understand this document before removing any computers, devices, or media from service, re-purposing, or disposing of them.

Definitions	
Devices	Any electronic device capable of storing data, typically items such as mobile phones, PDAs, digital audio players, hard drives (both portable and installed in another device, such as a computer or server), etc.
Media	Removable and portable data storage, including floppy disks, CDs and DVDs, portable hard drives, portable memory devices (USB 'thumb disks'), camera, phone, and other memory devices ('compact flash', 'SDA', 'Memory Stick', etc.), etc.
Media Reuse	Media that will be repurposed for less secure use than its current use or will be transferred to a different authorization environment.

Purpose

Unauthorized persons could access data left on media and devices containing restricted data compromising the privacy of that data and exposing the university to liability. Even when deleted by conventional means (simply using a 'delete' or 'format' function), the data is often easily recoverable. This document outlines standards for securely destroying data and sanitizing storage media and devices in ways that the data cannot be recovered.

Standards

1. Reasonable steps must be taken to ensure all Restricted Data is rendered unrecoverable prior to reuse or disposal of the media on which it was stored [3].

2. Data destruction should be done according to the guidelines in this standard. The FSU Chief Information Officer or their designee must approve any other destruction methods. Check the FSU Purchasing web site for vendors that have contracted with FSU for data destruction.

3. Units must create and follow procedures to ensure that all devices and media are

processed in accordance with these standards.

4. Between the times that media containing Restricted Data is removed from service, and the time it is sanitized or destroyed, it must be safeguarded. Evaluate possible storage spaces with the same security used for locating production systems used with Restricted Data.

5. Compliance with this standard does not obviate the need to comply with public records law. Before data destruction, Units must verify compliance with records disposition requirements.

6. Media and devices containing Restricted Data that will be stored or transported prior to destruction should be inventoried in case of loss before data is destroyed. Inventory documentation should include a unique identifier where appropriate (such as a hard disk model and serial number, an item or lot description, or description of data records). Inventory documentation should be retained at least until the media or device is destroyed.

Guidelines

1. The following table lists recommended methods of Restricted Data destruction for various devices and media types. Other methods may suffice for other data. For property being transferred to Asset Management Services, see http://fa.ufl.edu/am/destroy-data.asp for their data destruction requirements. Data Principals may also have different requirements.

Media Type	Data Destruction Method
Functioning hard disks that may be re-used	Minimum 3-pass overwrite, or utilization of ATA Secure Erase feature
Hard disks that are damaged or will not be re-used	Degauss
Tapes (video and data backup)	Degauss or 3-pass overwrite
Flash media based devices (thumb drives, memory cards)	Minimum 3-pass overwrite in a way that ensures all storage space is overwritten
CD, DVD, floppy disks	Cross-cut shredding
Devices such as PDAs, phones, digital audio/video players	Cell Phone Data Eraser, http://wirelessrecycling.com/home/data_eraser/default.asp or http://www.recellular.com/recycling/data_eraser/default.asp. Also see brand/model specific guidance.
Media and devices	Incineration, pulverization, disintegration (These methods should be reserved for media and devices that are non-functional, obsolete, or have no other practical method of destruction.)

2. Vendors contracted for data disposal should be certified by the National Association for Information Destruction (NAID). For a current list of certified members, see http://www.naidonline.org/certified_members.html.

3. Brand/Model specific guidance
    - When in doubt about the proper procedures for device, contact the manufacturer.

PalmOS devices	Perform Factory Reset as documented in Solution ID 15574, 'Performing a Factory Reset before your Palm device changes ownership or is sent away for repair' at http://kb.palm.com/. Older Palm devices that do not have the Factory Reset option may have Zero Out Reset or Secure Erase functions as documented in Solution ID 887. If the device supports none of these methods, a Hard Reset can be used.
Blackberry devices	See http://www.blackberry.com knowledgebase article number KB-02318, “How to delete all data, or all data and applications on the BlackBerry device.”

4. Suggested tools
    - UCSD ATA Secure Erase utility, http://cmrr.ucsd.edu/hughes/subpgset.htm
    - Darik's Boot and Nuke, http://dban.sourceforge.net/