Computer and Electronic Solid Waste Management Security and Privacy of Data Held in Electronic Devices December 22, 2004

This guidance has been developed to comply with the provisions of Act 1410 of 2001 which states in Section 4. (a)(2) "the policy shall mandate that all hard drives of surplus computer equipment be degaussed, cleared of all data, software and be otherwise prepared for sale within ninety (90) days after replacement."

Computers and other electronic devices may hold sensitive data. When these items are no longer used by their original owners, the data must be removed before passing the equipment to others for use or disposal. This document addresses the need for data security and privacy in light of the disposal and recycling options addressed in Act 1410.

Introduction

Many electronic devices retain data even after normal file deletion steps have been taken. Readily available utilities can recover deleted files. Besides business documents, electronic devices may retain information for efficiency of operation, such as user identification, software settings, Internet access, and financial information. Appropriate measures must be taken to insure that privacy and security violations do not occur when computers and other electronic devices are removed from service. The type of device, the sensitivity of the data, and the safety of the person destroying devices have to be considered when complying with the requirement that the equipment be degaussed and cleared of all data.

Devices

The need to remove data before equipment disposal applies to all electronic devices that retain information after the power is turned off (nonvolatile storage.) This includes computer hard drives, removable media, personal digital assistants (PDAs), Blackberries, USB memory sticks, some printers and copiers, and any other device that has nonvolatile storage. Since the disposal methods listed here are general in nature, the manufacturer of a device may need to be contacted to determine the best method of cleansing a particular piece of equipment.

Data

According to the Data and System Classification Grid Guidelines within the Arkansas Shared Technical Architecture, four sensitivity levels are assigned to data: unrestricted, sensitive, very sensitive, and extremely sensitive. When preparing an electronic device for disposal or reuse outside the current work area, the sensitivity of the data that has been held on those devices serves as a guide to

choosing the method of data removal. Individual state entities are responsible for the classification of their data.

Unrestricted data should be removed from a device in a way that assures that the data cannot be retrieved with commercially available software or other simple means. Sensitive and very sensitive data should be removed such that no means of recovering the data is possible with current technology. Usually devices that held extremely sensitive data should be destroyed.

Cleansing Methods

The appropriate cleansing method depends on the particular device and the sensitivity of the data. It is acceptable to use a more secure method of data removal than those listed in this guidance. All cleaning methods must be documented. One copy goes with the device if it is reassigned, sent to Marketing and Redistribution, sold, or donated, and the other stays with the agency.

Fixed Disks

Preparation of fixed disk storage for disposal is to be accomplished by single pass overwriting, triple pass overwriting, or destruction, depending on the sensitivity of the data. If an overwrite process is used all data on the device must be overwritten, including the operating system. Even if a device is going to be destroyed, the device should be overwritten first. RAID systems may have to be reconfigured before the drives can be cleaned with an overwrite process. A number of free and low cost products are available. No one particular product is specified in this guidance.

The overwrite process can only be performed on a functioning drive. A non-working drive or one that has contained extremely sensitive data should be destroyed. Destruction should include the cutting of all cables and disassembly of the drive. The platters should be severely damaged by drilling holes, pounding with a hammer, or cutting with snips.

Removable Media

Because most removable media is inexpensive, destruction may be considered for all items, although overwriting alone is acceptable if no extremely sensitive data was ever stored on the media. Diskettes should be disassembled and the recorded media mutilated by puncturing, cutting, and/or sanding. Rewritable CDs not containing extremely sensitive data may be overwritten. Other CDs, DVDs and other optical media should be punctured, sanded and cut.

Magnetic Tape

The process of overwriting magnetic tape is only suitable for removal of unrestricted data. Degaussing is acceptable except for extremely sensitive data as long as the degaussing device is matched with the type of tape and the process is performed properly. Deviations from an approved method or rate of coercivity could leave significant portions of data remaining on a hard drive. Destruction can be accomplished by disintegration, incineration, pulverization, or shredding.

- **Nonvolatile Memory Storage** – Some devices such as memory sticks and

USB memory devices can be overwritten with the same utilities used for overwriting hard drives. In cases where other memory devices such as erasable programmable read-only memory (EPROM) may contain sensitive data, the manufacturer's instructions for full chip erasure should be followed. If extremely sensitive data is involved the device should be destroyed.

- **Personal Digital Assistants** – Any PDA, Blackberry, or similar device should be wiped of all data according to the manufacturer's instructions and reset to factory defaults. Batteries should be removed for several hours. If the device contained extremely sensitive data it should be destroyed. The device can be adequately wrapped in material to prevent injury, and then hammered until the internal parts are mangled.

Third Parties

If a third party is used for the cleaning or destruction of storage media containing sensitive data there should be a signed agreement stating that the data removal and device disposal practices will be at least as stringent as those in this guidance document.

Maintenance

When devices containing sensitive data are sent out for maintenance either the sensitive data must be overwritten before sending the device out, or an agreement should be signed stating the data will be held securely and protected from disclosure. Security of the device during transport is the responsibility of the owning agency.

Leases

Lease agreements should be reviewed to assure that components of leased devices can be cleaned or destroyed according to the sensitivity of the data they've held.

Summary

Before devices are reassigned or disposed of, measures must be taken to assure that data is properly removed. The Data and System Classification Grid Guidelines type data as unrestricted, sensitive, very sensitive, or extremely sensitive. Device components with extremely sensitive data should be destroyed. Data can be removed from most disks with an overwrite process. Magnetic tape can be reasonably cleaned by proper degaussing methods. The responsibility for data security extends through transport for maintenance and through third party disposal.

References

- Data Classification Standard: **http://www.cio.arkansas.gov/techarch**
- Arkansas Act 1410 of 2001 **http://www.arkleg.state.ar.us/ftproot/acts/2001/htm/act1410.pdf**
- National Industrial Security Program Operating Manual (NISPOM), Chapter

8, 1995
http://www.dss.mil/isec/nispom.htm

- Memorandum – Disposition of Computer Hard Drives, Arkansas Office of the State Executive C I O, January 3, 2002
http://www.oit.state.ar.us/Announce/Disp_HD.htm

Glossary

- Coercivity – Defines the magnetic field necessary to reduce a magnetically saturated material's magnetization to zero. The coercivity strength of an applied magnetic field determines which type of degausser may be applied to a particular type of magnetic material.
- Degaussing – Degaussing (i.e., demagnetizing) is a procedure that reduces the magnetic flux to virtually zero by applying a reverse magnetizing field. Properly applied, degaussing renders any previously stored data on magnetic media unreadable.
- Overwriting – A process of writing patterns of data on top of the data stored on a magnetic medium in order to obscure the previously written data.