Cyber Security:

Erasing Information and Disposal of Electronic Media

(DELETING FILES DOES NOT ERASE INFORMATION)

A Non-Technical Guide

Essential for
Business Managers
Office Managers
Operations Managers

Multi-State Information Sharing and Analysis Center

NYS Office of Cyber Security

This appendix is a supplement to the *Cyber Security: Getting Started Guide,* a non-technical reference essential for business managers, office managers and operations managers. This appendix is one of many which is being produced in conjunction with the *Guide* to help those in small agencies and businesses to further their knowledge and awareness regarding cyber security. For more information, visit: http://www.dhses.ny.gov/ocs/.

INTRODUCTION

The intent of this policy is to describe how to dispose of computers and electronic storage media effectively and prevent the inadvertent disclosure of information that often occurs because of inadequate cleansing and disposal of computers and electronic storage media.

There are many laws that require information to be protected. Some examples of these laws are public health laws, privacy laws and the Health Insurance Portability and Accountability Act. Social Security numbers, credit card information, health-related information and trade secrets are examples of sensitive information requiring protection from disclosure. To the extent that electronic media is used to store official records, organizations must also adhere to records management rules, including records retention schedules.

Sensitive documents and data containing personally identifiable information can be stored electronically in multiple formats and locations. For example, the information might first exist on a CD then be copied to the computer's hard drive and subsequently backed up to a tape for disaster recovery purposes. In this example, there are three different storage media to consider: CD, hard drive and backup tape.

Remember: Simply viewing a file with a computer can create a copy of the file on the computer's hard drive.

Deleting files does not erase information. Information that is deleted from a computer may be retrieved by using forensics or other recovery tools. As new computers are purchased, older computers may be redeployed, discarded or surplused. It must be assumed that at some point in time sensitive information may have been stored and is still retrievable from all electronic storage media including computer and network hard drives, external hard drives, CDs, DVDs, floppy disks, tapes, thumb drives, memory sticks, PDAs, cell phones and other storage devices not enumerated here.

POLICY

When an organization determines that its computer or electronic storage media should be redeployed, discarded or surplused, the organization should use one or more of the following techniques.

TECHNIQUES FOR ERASING AND DISPOSING

Information in an organization carries both benefits and risks. The benefits are that it allows an organization to carry out its work making this information a valuable asset in the organization. The risks can include accidental or malicious destruction and unauthorized access to sensitive information. Organizations must carefully manage the risks of unauthorized access by knowing what information it must keep private and setting up protocols for securing that information. Most importantly, organizations need to develop and follow a set of policies and procedures that guide the process of destroying sensitive information on any media.

Ensuring Proper Erasure or Disposal Some tools may necessitate a knowledgeable and competent person to ensure the storage media is appropriately erased. If your organization cannot ensure erasure of the media, you must find trained personnel who can carry out that activity and

demonstrate that they have succeeded. Some commercial services may be available through IT consultants for small agencies and businesses. Your records office may be aware of additional tools and services. When in doubt, contact the device manufacturer.

Wiping Programs Wiping is a process of overwriting the space where files are located with random data. Read/writable media should be "wiped" using a utility that is compliant with the Department of Defense (DoD) 5015.2-STD RMA Design Criteria Standard.

Issues

- All appropriate options should be set to meet the DoD Standards.
- It may take a long time to rewrite the drive or media.
- A defective drive may not be able to be wiped.
- Additional procedures specified by the device manufacturer may need to be employed to ensure a complete wiping process.

Degaussing Degaussing is the erasure of information through the use of a very strong magnet. Degaussing is generally used for erasing of magnetic media examples include tapes and floppy disks. Magnetic media should be "degaussed" using a Department of Defense (DoD) rated unit.

Issues

- Since a very strong magnet is required to erase information, an organization needs to remember to keep ALL magnetic media a sufficient distance from the degaussing unit to prevent accidental erasure of essential information. Some examples include credit cards, cell phones and watches.
- Individuals with pacemakers need to maintain a safe distance from active degaussing.
- Degaussing any current generation hard disk will render the drive permanently unusable.

Physical Destruction Certain media can be read many times but can only be written once. These media cannot be overwritten. Sometimes the media are defective and can no longer be used for retrieval or storage. In each of these cases the media should be physically destroyed. Certain types of shredders are capable of shredding storage media such as CDs and DVDs.

Any storage media can be physically destroyed through burning, crushing or smashing.

Issues

- Environmental concerns may exist with incinerating media.
- Mechanisms need to be implemented to ensure the media is appropriately destroyed. Requiring a contractor to crush the media on site would be an appropriate control.
- Safety concerns include, but are not limited to, the use of safety goggles when using physical destruction techniques.

Recommended Techniques for Disposal of Electronic Storage Media

Once an organization has decided to dispose of electronic storage media then the following table can be used as a reference of recommended techniques to accomplish the job.

This is not an all inclusive list of devices but a sample of the most commonly used pieces of equipment. Any device used to process information electronically may store information.

Erasure and Disposal Technique Matrix			
Media Type	Wipe OR	Degauss OR	Physical Destruction
Computer Hard Drive Network Hard Drive External Drives	✓	✓	✓
Fax Machine Printer Copier	✓		✓
CDs DVDs			✓
USB Drives Thumb Drives Memory Sticks	✓		✓
Floppy Disks	✓	✓	✓
Tapes	✓	✓	✓
PDAs Cell Phones	✓		✓

OTHER CONSIDERATIONS

Returning Media Under Warranty Many hard drives are purchased with a warranty period. When devices fail during the warranty period, the vendor normally requires the return of the defective drive before a warranty replacement is provided. Warranty return of a defective drive includes all the data, documents and information stored on the drive prior to the fatal problems. Since sensitive data could potentially be exposed on a warranty returned defective drive, the organization should resort to physical destruction instead of returning the drive to the vendor. Your vendor may have an option to not return the hard drive.

Audit Trail A log should be maintained of all media that have been disposed. The log should include the date, type of device, manufacturer, serial number (if one exists), sanitation or destruction method used, disposal method such as sold or crushed.

Acknowledgement

Special thank you to Laura Iwan and the New York State Office of Cyber Security (OCS) for their contribution to this paper.

Portions of this article are taken directly from Monthly Cyber Security Tips NEWSLETTER Volume 1, Issue 3, August 2006 edition and reprinted with permission. The full article may be found on http://www.dhses.ny.gov/ocs/.

Any product-specific resources mentioned in this paper are provided as a general reference only. We do not endorse or promote the advertising of any resources.