

Information Technology Resource Management Council (ITRMC)

ENTERPRISE GUIDELINES – G500 SECURITY PROCEDURES

Category: G550 – CLEANSING DATA FROM SURPLUS COMPUTER EQUIPMENT

CONTENTS:

- I. [Definition](#)
- II. [Rationale](#)
- III. [Guideline](#)
- IV. [Resources](#)
- V. [Timeline](#)
- VI. [Revision History](#)

I. DEFINITION

1. Removal of State of Idaho Data – Removal of State of Idaho data from hard drives and electronic media is the process of removing sensitive and/or confidential programs or data files on computer hard drives or electronic media in a manner that gives assurance that the information cannot be recovered by keyboard or laboratory attack.
2. Physical Destruction – Hard drives should be physically destroyed when they are defective or cannot be economically repaired.
3. Degaussing – A process whereby the magnetic media are erased, (i.e., returned to a zero state).
4. Overwriting or Scrubbing – Replacing previously stored data on a drive or disk with a predetermined pattern of meaningless information.

II. RATIONALE

This guideline is applicable to all State agencies, their field operations, and institutions of higher education (collectively referred to as “agency”) that surplus, transfer, trade-in, otherwise dispose of, or replace the computer hard drives and electronic media resources in the State of Idaho. This guideline also applies to equipment owned or leased by the agency. The heads of State agencies, field offices, and institutions of higher education are responsible for ensuring electronic information is properly protected. This guideline may be of value to local government entities.

The guideline proposes:

1. To define the minimum requirements for the removal of State of Idaho data from an agency's computer hard drives and electronic media resources prior to its being surplus, transferred, traded-in, disposed of, or the hard drive is replaced;
2. To prevent unauthorized use or misuse of State information, and promote the privacy and security of sensitive and/or confidential information resources within the State of Idaho; and
3. To foster State agency compliance with federal regulations dealing with the confidentiality of personally identifiable information. Included are regulations such as the Health Insurance Portability and Accountability Act, the Gramm-Leach-Bliley Act (aka Financial Services Modernization Act), and the Family Educational Rights and Privacy Act.

III. GUIDELINE

1. Background

The surplus, transfer, trade-in, disposal of computers, or replacement of electronic storage media and computer software can create information security risks for the agency. This also includes equipment reassigned, released, or no longer in use in the agency. These risks are related to potential violation of software license agreements, unauthorized release of sensitive and/or confidential information, and unauthorized disclosure of trade secrets, copyrights, and other intellectual property that might be stored on the hard disks and other storage media. It should be noted that all agencies' computer hard drives, especially those containing sensitive and/or confidential data, shall have all State of Idaho data securely removed from their hard drives as suggested by this guideline before a computer system is surplus, transferred, traded-in, otherwise disposed of, or the hard drive is replaced.

Removal of confidential information in the past might have been accomplished by using the "FORMAT" command or the "DOS FDISK" command. Ordinarily, using these procedures gave users a sense of confidence that their data had been completely removed. When using the "FORMAT" command, Windows displays a message such as:

Important: Formatting a disk removes all information from the disk.

The "FORMAT" utility actually creates new "FAT" or "ROOTS" tables, leaving all previous data on the disk untouched. Moreover, an image of the replaced "FAT" and "ROOT" tables are stored, so that the "UNFORMAT" command can be used to restore them. "FDISK" merely cleans the "PARTITION TABLE" (located in the drive's first sector) and does not remove anything else.

In recent years, advances in data recovery have been made such that data can be reclaimed in many cases from hard drives that have been wiped or cleared. Free and commercial software exist that use techniques such as Partial Response

Maximum Likelihood (PRML), Magnetic Force Microscopy (MFM) and other recovery methods based on patterns in erased bands to recover cleared data.

Failure to expunge data that might be exposed under such risk situations could violate federal laws including, but not limited to, the Gramm-Leach-Bliley Act (GLBA), the Health Insurance Portability and Accountability Act of 1996 (HIPAA), and The Family Educational Rights and Privacy Act (FERPA), etc.

This guideline applies to equipment owned or leased by the agency. All hard drives (this includes instances where equipment has multiple hard drives) and electronic storage media should have all State of Idaho data properly removed prior to disposal or release. Data removal procedures should be properly documented in accordance with the processes outlined below in section 1.B., section 1.C., and section 1.D., and in accordance with the software manufacturers' guidelines to prevent unauthorized release of sensitive and/or confidential information that may be stored on that equipment and other electronic media. This is to include all computer equipment that has memory, such as personal computers, Personal Digital Assistants (PDAs), routers, firewalls and switches. Examples of other media include, but are not limited to, tapes, diskettes, CDs, DVDs, write-once-read-many (worm) devices, and Universal Serial Bus (USB) data storage devices.

A. Removal of State of Idaho Data from Hard Drives

The following section outlines best practices to expunge data from storage media. Removal of State of Idaho data should be performed on hard drives to ensure that information is removed from the hard drive in a manner that gives assurance that the information cannot be recovered. Before the removal process begins, the computer shall be disconnected from any network to prevent accidental damage to the network operating system or other files on the network. Agencies are also urged to insure that all data being expunged has met the record retention requirements outlined in the *Records Management Guide* book. (http://www2.state.id.us/adm/purchasing/RecordsCenter/Record_Retention_2004_Book.pdf)

Three acceptable methods:

- (1) Overwriting – Overwriting is an approved method for removal of State of Idaho data from hard disk storage media. Overwriting of data means replacing previously stored data on a drive or disk with a predetermined pattern of meaningless information. This effectively renders the data unrecoverable, but the process should be correctly understood and carefully implemented. Overwriting is also known as “scrubbing;”
- (2) Degaussing – A process whereby the magnetic media are erased (i.e., returned to a zero state). Degaussing (demagnetizing) reduces the magnetic flux to virtual zero by applying a reverse magnetizing field. Properly applied,

degaussing renders any previously stored data on magnetic media unreadable by keyboard or laboratory attack; and

- (3) Physical Destruction – Hard drives should be physically destroyed when they are defective or cannot be economically repaired or State of Idaho data cannot be removed for reuse. Physical destruction must be accomplished to an extent that precludes any possible further use of the hard drive.

The method used for removal of State of Idaho data, depends upon the operability of the hard drive:

- (1) Operable hard drives that will be reused should be overwritten prior to disposition. If the operable hard drive is to be removed from service completely, it shall be physically destroyed or degaussed; or
- (2) If the hard drive is inoperable or has reached the end of its useful life, it should be physically destroyed or degaussed.

Clearing data (deleting files) removes information from storage media in a manner that renders it unreadable unless special utility software or techniques are used to recover the cleared data. However, because the clearing process does not prevent data from being recovered by technical means, it is **not** an acceptable method of removing State of Idaho data from agency-owned hard disk or storage media.

(1) Overwriting

Overwriting is an approved method for the removal of State data from hard disk drives. Overwriting of data means replacing previously stored data on a drive or disk with a predetermined pattern of meaningless information. This effectively renders the data unrecoverable. All software products and applications used for the overwriting process should meet the following Guidance:

(a) Guidance

- (i) The data must be properly overwritten with a pattern by means of, at a minimum, one (1) pass of the entire disk;
- (ii) The software must have the capability to overwrite the entire hard disk drive, independent of any BIOS or firmware capacity limitation that the system may have, making it impossible to recover any meaningful data;
- (iii) The software must have the capability to overwrite using a minimum of one (1) pass of data patterns on all sectors, blocks, tracks, and any unused disk space on the entire hard disk medium;

- (iv) The software must have a method to verify that all data has been removed. It is the responsibility of the agency to verify that a drive overwritten is, in fact, clean of any intelligible or prior data. This verification can be either as a separate process or included as part of the software used for overwriting; and
- (v) Sectors not overwritten must be identified.

(2) Degaussing

Degaussing is a process whereby the magnetic media is erased. Hard drives seldom can be used after degaussing. **The degaussing method will only be used when the hard drive is inoperable and will not be used for further service.**

Please note that extreme care should be used when using degaussers since this equipment can cause extreme damage to nearby telephones, monitors, and other electronic equipment. Also, the use of a degausser does not guarantee that all data on the hard drive has been destroyed. Degaussing efforts should be audited periodically to detect equipment or procedure failures. The following guidance should be followed when hard drives are degaussed:

(a) Guidance

- (i) Follow the product manufacturer's directions carefully. It is essential to determine the appropriate rate of coercivity for degaussing;
- (ii) Shielding materials (cabinets, mounting brackets), which may interfere with the degausser's magnetic field, must be removed from the hard drive before degaussing; and
- (iii) Hard disk platters must be in a horizontal direction during the degaussing process.

(3) Physical Destruction

(a) Guidance

- (i) Hard drives should be destroyed when they are defective or cannot be repaired or State data cannot be removed for reuse;
- (ii) Physical destruction must be accomplished to an extent that precludes any possible further use of the hard drive. This can be attained by removing the hard drive from the cabinet and removing any steel shielding materials and/or mounting brackets and cutting the electrical connection to the hard drive unit. The hard drive should then be subjected to physical force (pounding with a sledge hammer) or

extreme temperatures (incineration) that will disfigure, bend, mangle or otherwise mutilate the hard drive so it cannot be reinserted into a functioning computer; and

(iii) Multiple holes drilled into the hard disk platters is an optional method of destruction that will preclude use of the hard drive and provide reasonable protection of data written on the drive.

B. Removal of State Data from Other Electronic Devices

(1) Guidance

Electronic devices that hold user data or configurations in non-volatile memory should have all State data removed by either the removal of the battery or electricity supporting the non-volatile memory or by such other method recommended by the manufacturer for devices where the battery is not removable. This is to include all computer equipment that has memory such as personal computers, PDAs, routers, firewalls and switches.

C. Removal of State Data from Other Computer Media

(1) Guidance

If there is any risk of disclosure of sensitive data on media other than computer hard drives, that media should be destroyed. Disintegration, incineration, pulverization, shredding or melting are acceptable means of destruction. Examples of other media include, but are not limited to, tapes, diskettes, CDs, DVDs, worm devices, and USB data storage devices.

D. Certification of the Removal of State Data from Surplus Computer Hard Drives and Electronic Media

Each agency is responsible to audit the removal of State data when any computer hard drives or electronic media are surplus, transferred, traded-in, disposed of, or the hard drive is being replaced, as well as to ensure the audit process occurs in a timely manner and the audit controls are effective.

(1) Guidance

Prior to submitting surplus forms to the agency's appropriate organizational unit, the process for removal of State data should be documented on a form that explicitly outlines:

(a) The method(s) used to expunge the data from the storage media;

(b) The type of equipment/media from which State data is being removed;

- (c) The name of the person responsible for the removal of State data; and
- (d) The name and signature of their supervisor.

IV. RESOURCES

1. The National Industrial Security Program Operating Manual of the US DOD:
<http://www.dss.mil/isec/nispom.htm>
2. Information (precautions when selling, trading, or sending a PC to salvage or to a repair shop): <http://ftp.aset.psu.edu/pub/ger/documents/SecureFixedDiskWiping.html>
3. DOD 5220.22-M disk overwriting Standard:
<http://www.usaid.gov/policy/ads/500/d522022m.doc>
4. Secure Deletion of Data from Magnetic and Solid-State Memory:
http://wipe.sourceforge.net/secure_del.html
5. Programs:
 - A. Darik's boot and nuke: <http://dban.sourceforge.net/>
 - B. Heidi Eraser: <http://www.heidi.ie/eraser/>

V. TIME LINE

Last Revised: September 13, 2006
Effective Date: October 24, 2005

VI. REVISION HISTORY

9/13/06 – Moved recommended best practices to ITRMC IT Policy 4530; updated numbering.