

## **Removal Of Commonwealth Data From Surplus Computer Hard Drives And Electronic Media Standard**

The policies and procedures outlined in this document will be observed in accordance with COV ITRM Standard SEC2003-02.1 of the Virginia Information Technologies Agency Guidelines for disposal of electronic storage devices.

### **Abstract:**

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, or 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, 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 must have all Commonwealth data securely removed from their hard drives as specified by this policy before a computer system is surplus, transferred, traded-in, otherwise disposed of, or the hard drive is replaced.

### **Standards and Procedure**

The following standards will be followed by VMI when a computer system is surplus, transferred, traded-in, or disposed of, or the hard drive is replaced.

#### **A.1 Standards**

A.1.a) Before a computer system is surplus, transferred, traded-in, disposed of, or the hard drive is replaced, all sensitive and/or confidential program or data files on any storage media will be completely erased or otherwise made unreadable in accordance with this procedure unless there is specific intent to transfer the particular software or data to the purchaser/recipient.

A.1.b) Hard drives of surplus computer equipment must be securely erased within 60 days after replacement.

A.1.c) Whenever licensed software is resident on any computer media being surplus, transferred, traded-in, disposed of, or the hard drive is replaced, the terms of the license agreement must be followed.

A.1.d) After the removal of Commonwealth data from the hard drive is complete, the process will be certified, as specified below, and a record maintained as specified by the agency's records retention schedule.

#### **B. Removal of Commonwealth Data from Hard Drives**

The following section outlines the acceptable methods to expunge data from storage media. Removal of Commonwealth data must 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 must be disconnected from any network to prevent accidental damage to the network operating system or other files on the network.

There are three acceptable methods to be used for the hard drives:

- Overwriting – Overwriting is an approved method for removal of Commonwealth 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 must be correctly understood and carefully implemented.
- 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.
- Physical Destruction – Hard drives should be physically destroyed when they are defective or cannot be economically repaired or Commonwealth 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 Commonwealth data, depends upon the operability of the hard drive:

- Operable hard drives that will be reused must be overwritten prior to disposition. If the operable hard drive is to be removed from service completely, it must be physically destroyed or degaussed.
- If the hard drive is inoperable or has reached the end of its useful life, it must 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 Commonwealth data from agency owned hard disk storage media.

## **Overwriting**

Overwriting is an approved method for the removal of Commonwealth 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 must meet the following standards:

### **B.1 Standards**

B.1.a) The data must be properly overwritten with a pattern. Department of Defense (DOD standard 5220.22-M) requires overwriting with a pattern, and then its complement, and finally with a random pattern of 1's and 0's.

B.1.b) Removal of Commonwealth data is not complete until three overwrite passes and a verification pass are completed.

B.1.c) 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.

B.1.d) The software must have the capability to overwrite using a minimum of three cycles of data patterns on all sectors, blocks, tracks, and any unused disk space on the entire hard disk medium.

B.1.e) The software must have a method to verify that all data has been removed.

B.1.f) Sectors not overwritten must be identified.

### **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 will be destroyed. Degaussing efforts will be audited periodically to detect equipment or procedure failures. The following standards must be followed when hard drives are degaussed:

### **B.2 Standards**

B.2.a) Follow the product manufacturer's directions carefully. It is essential to determine the appropriate rate of coercivity for degaussing.

B.2.b) Shielding materials (cabinets, mounting brackets), which may interfere with the degausser's magnetic field, must be removed from the hard drive before degaussing.

B.2.c) Hard disk platters must be in a horizontal direction during the degaussing process.

### **Physical Destruction**

### **B.3 Standards**

B.3.a) Hard drives must be destroyed when they are defective or cannot be repaired or Commonwealth data cannot be removed for reuse.

B.3.b) 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.

B.3.c) Multiple holes drilled into the hard disk platters is another method of destruction that will preclude use of the hard drive and provide reasonable protection of data written on the drive.