

DEPARTMENT OF THE ARMY  
Corps of Engineers, Omaha District  
106 South 15<sup>th</sup> Street  
Omaha, Nebraska 68102-1618

OM 25-1-80

CENWO-IM

MEMORANDUM  
No. 25-1-80

1 August 2003

Information Management  
COMPUTER HARD DRIVE DISPOSAL

**History.** This document constitutes a new Omaha District office memorandum.

**Summary.** This memorandum prescribes the policy and procedures for the disposal of personal computer hard drives within the Omaha District.

1. Applicability. This memorandum applies to all Omaha District elements, NWD-Omaha personnel, and any other Corps offices that the Omaha District Information Management Office (IMO) services.

2. References.

a. Assistant Secretary of Defense Memorandum, "Disposition of unclassified DoD Computer Hard Drives," dated 4 June 2001.

b. Deputy Secretary of Defense Memorandum, "Destruction of DoD Computer Hard Drives Prior to Disposal," dated 8 January 2001.

c. Deputy Secretary of Defense Memorandum, "Disposition of Unclassified DoD Computer Hard Drives," dated 29 May 2001.

d. DoD 5220.22-M, National Industrial Security Program Operating Manual, 1 January 1995.

e. Joint DoDISS/Cryptologic SCI Information Systems Security Standards, Revision 2, 31 March 2001.

f. NWD Form 25-11, Computer Hard Drive Disposal Certificate.

3. Policy. Per the above references, the IMO must ensure that the hard drives in all excessed personal computing devices (desktop, laptop, server, etc.) are disposed of properly. Hard drives must either be erased using DataEraser software or destroyed, and a completed NWD Form 25-11, Certificate of Hard Drive Disposition (CHDD) must be completed for each hard drive prior to disposal. This form is available in FormFlow.

OM 25-1-80  
1 August 2003

4. Responsibilities.

a. The IMO will obtain and maintain software license(s) for the DataEraser software and provide the DataEraser software and necessary training to the appropriate personnel.

b. The Logistics Management Office (LMO) will notify the IMO when computers/hard drives are scheduled to be transferred out of Omaha District control and provide space for the IMO technician(s) to perform the necessary procedures.

c. The Information Assurance Manager (IAM) will maintain required records of disposal activities.

d. In remote locations, the local Information Assurance Security Officer (IASO) will ensure computers/hard drives are cleaned or destroyed as necessary in accordance with these instructions and forward necessary records to the IAM.

5. Procedures. The procedures below meet minimum security requirements for the disposal of hard drives. These procedures were extracted from the "Joint DODISS/Cryptologic SCI Information Systems Security Standards" which superseded Sup 1 to NSA CSS 130-1, the previous governing directive.

a. Record hard drive information on CHDD.

b. If the drive ever contained classified data, go to paragraph 6.f.

c. If the drive is under warranty, go to paragraph 6.j.

d. If the drive is not operational, go to paragraph 6.f.

e. Erase the drive with DataEraser software. See Appendix A for instructions. Go to paragraph 6.g.

f. Physically destroy the drive. Physical destruction must be accomplished to an extent that precludes any possible further use of the hard drive.

(1) Remove the hard drive from the chassis.

(2) In a suitable facility with individuals wearing appropriate safety

equipment, subject the hard drive to physical force (e.g. pounding with a sledgehammer or drilling a minimum of three 1/4-inch diameter holes completely through the case and all platters) that will mutilate the hard drive so that it cannot be re-used.

(3) Any electrical connectors must be damaged to the point that the hard drive cannot be re-connected without significant rework.

g. Sign and date the CHDD.

h. Attach a copy of the CHDD to the hard drive or PC case and send the original certificate to the IAM.

i. Release the hard drive or PC for disposal through the normal excess property process.

j. Contact the vendor for warranty procedures. The vendor must agree to one of the following:

(1) return the defective drive for disposal,

(2) erase the drive with a procedure at least as stringent as that used by the DataEraser software,

(3) physically destroy the drive,

(4) or accept a physically damaged drive.

k. If the vendor will not accept a physically damaged drive and will not return the drive, he must provide certification that it was destroyed or erased. Send the vendor certification to the IAM. If the vendor is willing to accept a physically destroyed drive, complete a CHDD, destroy the drive in accordance with the procedures in paragraph 6.f., and forward the signed certificate to the IAM.

OM 25-1-80  
1 August 2003

## **Appendix A**

### DataEraser Procedure

1. Insert the DataEraser diskette in your A: drive and reboot or power on your computer. The ONTRACK Operating System starts up. If your system fails to boot from the diskette, see the troubleshooting section in the README.TXT file on the diskette.
2. If your system contains SCSI hard drives, in order to access the drives the ASPI drivers need to be loaded. During boot up, a LoadASPI program will give you three options:
  - a. Skip loading an Aspi driver
  - b. Use a known Aspi device driver. This allows you to enter the location (path) and name of an Aspi driver on the system to use.
  - c. Autodetect for a host adapter. The program will detect what type of Aspi driver is required and automatically load it. If you do not have a SCSI device on your system, you can either skip loading an Aspi driver or let the program default to auto-detect.
3. The *Welcome* dialog provides an overview of DataEraser.

Press ENTER to continue to the DataEraser menu.

[Menu]

The menu provides you with the following options:

- \* Run DataEraser
- \* View Drives
- \* View README File
- \* View License Agreement
- \* Exit DataEraser

To select from this list, highlight the option desired and press ENTER. To scroll to the option, use the Page-Up, Page-Down, Up-Arrow, and Down-Arrow keys. NOTE: The same keys may be used throughout DataEraser to scroll when there is more text than will display on the screen.

[Run DataEraser]

4. To overwrite your drive, select "Run DataEraser" from the menu.
5. DataEraser displays the hard disk drives detected. If the information is correct, select the drive you would like to overwrite or all drives to overwrite every drive on your system, and press ENTER. If not correct, press F1 and a screen will explain possible reasons why your drives were not detected. Select EXIT to return to the main menu.
6. Select the specific partition you would like to overwrite or the Entire Drive and press ENTER. If you choose to overwrite a partition, DataEraser will return to this menu until all the partitions or the entire drive has been overwritten. You must select an entire drive to have a validation certificate created. Select EXIT to return to the main menu.
7. Select the type of overwrite you wish to run:
  - a. Single pass.
  - b. Triple pass meeting U.S. Department of Defense specifications. This is the selection you should choose.
  - c. Seven pass meeting German standards.
  - d. Multiple pass (configurable up to ninety-nine passes).
  - e. Select Exit to return to the main menu.
8. If you selected Multiple pass, you would need to edit the number of overwrite passes you wish to perform and then press ENTER. Or just press ENTER to use the default of 99 passes.
9. Enter the hex pattern you would like used to overwrite the drive or partition or press ENTER to use the default '00'. If you chose a multiple pass overwrite type, this pattern will be used on the final pass. Use the default of "00".
10. If you chose to overwrite the entire drive, now select the type of verification to use. Choose from:

Appendix A  
OM 25-1-80  
1 August 2003

- a. Full Verification which reads and verifies the entire drive, (choose this selection)
- b. Quick Verification which verifies approximately 1% of the drive, or
- c. Choose not to validate at all.
- d. Select Exit to return to the main menu.

11. If you chose Full Verification, you may enter any comments you would like printed on the Validation Certificate. A database file, 'DE\_Data.txt,' is created or appended containing all the validation certificate information in order to download to a database.

12. Before the overwrite and verification are completed, a review screen is presented for you to verify the options you chose. Tab or arrow to [Y]es to continue or [N]o to return to the main menu.

13. The overwrite and verification are performed without interruption. If you wish to cancel the overwrite at any time, press ESC and you will return to the main menu.

14. When the overwrite and verification are completed, a dialog box will display the results. If the verification was successful, a validation certificate, 'DE\_Cert.txt,' will be created on the diskette. If any read/write errors were detected on the drive, they are reported in the 'Report.txt' file on the diskette. See the troubleshooting section on how to view this file.

15. If the validation certificate was created, it will be displayed.

16. Press ENTER to return to the main menu.