

Disposal of Computer Equipment Containing Sensitive Information

1. Is it possible to retrieve data deleted with the "delete" command?

A typical "delete" command merely deletes the pointer to a file. The data will not be overwritten until the storage area is reallocated and re-used. By using commonly available utilities, it is possible to retrieve the deleted data in a computer.

2. How about the "format" command?

The "format" command in many cases merely creates an empty root directory and a new blank indexing scheme for all allocation units on the storage media making it available for the storage of new files. There are commercially available utilities to recover lost data from storage media caused by accidental execution of the "format" command.

3. Are there tools or software available for the complete data deletion purpose and are they reliable?

Commercial software and services are available in the market to perform secure data deletion by means of writing over the storage media a number of times and with different patterns. Those software packages which overwrite the data space with a character, the complement of that character, then a random character can be considered as reliable and follow current industry best practice for secure data deletion. However, you may need to evaluate the capability and features of such

products and consult their respective product vendors for details to see if they fulfill your specific requirements. Also, besides technical solution, necessary checks and balances should be in place to ensure that the secure deletion process is performed and is successful. Some of the possible measures which you may consider include proper approval/logging of the whole process, sample check/verification of erase hard disks, etc.

4. We understand that there are tools that claim to be capable of retrieving data even from a hard disk that was burnt by fire. Is it true?

Yes, commercial tools are available for data recovery. However, the prime objective of those tools is to address the disaster recovery need, e.g. when the data or its media is deleted or damaged by accident or natural disaster such as fire rather than after the application of the secure deletion procedures.

5. Is it possible to recover data from a computer after being overwritten by those secure deletion tools?

To recover or reconstruct data that has been deliberately overwritten usually requires specialised devices and/or environment. Data recovery and/or guessing would likely be uneconomical and hence impractical after the secure deletion procedures that follow the industry best practices are adopted.

In fact, Secure data deletion is one form of security risk management, similar to other information security topics. The security risk level associated with data deletion and recovery would be related to the value of the data being protected, the resources required to delete/undelete the data, and the cost of the equipment to be reused.

6. Is degaussing an acceptable method for secure data deletion for magnetic media such as hard disks, floppy disks and magnetic tapes?

According to international/industry practices, degaussing is considered an acceptable technical solution for secure data deletion for magnetic media such as hard disks, floppy disks and magnetic tapes if properly employed. During the degaussing process, the magnetic flux of the media is reduced to virtually zero by applying a reversing magnetizing field. Properly applied, degaussing renders any previously stored data on the media unrecoverable by keyboard or laboratory attack.

7. Are there any considerations regarding the use of degaussers for secure data deletion ?

With reference to current international/industry best practices, the following are some major considerations/practices when using degaussers for secure data deletion:

- The resistance of a magnetic media to demagnetization is the coercivity of the magnetic media and is measured in Oersteds. In order to completely erase the content on the magnetic media (e.g. hard disk), the degausser should produce a sufficiently strong magnetic field. It is recommended that the magnetic field should be at least 1.5 times higher than the coercivity of the media. Typical figures for various types of magnetic media are given below:

Typical Media Coercivity Figures

Medium	Coercivity
5.25" 360K floppy disk	300 Oe

5.25" 1.2M floppy disk	675 Oe
3.5" 720K floppy disk	300 Oe
3.5" 1.44M floppy disk	700 Oe
3.5" 2.88M floppy disk	750 Oe
3.5" 21M floptical disk	750 Oe
1/2" magnetic tape	300 Oe
1/4" QIC tape	550 Oe
8 mm metallic particle tape	1500 Oe
DAT metallic particle tape	1500 Oe
4mm DDS-1 tape	1550 Oe
4mm DDS-2 tape	1650 Oe
4mm DDS-3 tape	2300 Oe
4mm DDS-4 tape	2350 Oe
Older (1980's) hard disks	900-1400 Oe
Newer (1990's) hard disks	1400-2200 Oe
Newer (2000) hard disks	2000-3400 Oe

- During the degaussing process, the degaussers have to be operated at their full magnetic field strength. The product manufacturer's directions must be followed carefully since deviations from an approved method could leave significant portions of data remaining on the magnetic media.
- For degaussing hard drives, all shielding materials (e.g. castings, cabinets, and mounting brackets), which may interfere with the degausser's magnetic field, must be removed from the hard drive before degaussing. Hard disk platters must be in a horizontal direction during the degaussing process. For degaussing hard drives with very high coercivity ratings, it may be necessary to remove the magnetic platters from the hard drive's housing.
- Sufficient checks and balances mechanisms should be in place for the degaussing process such as requiring the individual who performs the degaussing to certify the completion of the degaussing by affixing a signed

verification label to the hard drive or the computer housing the hard drive indicating the date and degaussing product used for the procedure. Sample check of the degaussed media should also be performed by another party to ensure that the degaussing is done properly. Besides, the degausser should also be periodically tested accordingly to manufacturer's directions to ensure that they function properly.