Secure Deletion

Secure deletion is a method of data deletion by which deleted information can not be recovered. It is usually used in deleting important or sensitive data.

Before disposing of or re-using storage media that contain sensitive information, such as hard disks, CDs or portable storage devices, the sensitive information should be erased completely. Meanwhile, computers or any electronic office equipment embedded with storage media, such as multi-function printers and photocopiers, may contain sensitive information. Those sensitive information must also be securely erased in order to avoid data leakage.

The Principle of Delete Command or Format Command

The common “Format” and “Delete” commands merely delete the pointer to a file, but the data will be kept in the same storage area until the area is occupied by other files or reused.

There are several data recovery software tools available in the market for recovering data deleted by the “Delete” or “Format” commands.

Secure Deletion Methods

There are generally three methods for secure deletion:

- Overwriting
- Degaussing
- Physical Destruction

Overwriting

Overwriting refers to using secure deletion software and services to repeatedly overwrite the data on the storage media with random characters or a series of 0 and 1 (or similar bit mode), in order to completely clear the original data.

Before executing overwriting, it is essential to configure the software properly and to complete the whole overwriting process without errors, so as to ensure complete clearance of the stored data.

Degaussing

Degaussing technique is to use a specialised degausser, with a strong magnetic field to completely destroy the stored data in the magnetic storage media. If used properly, degaussing can completely clear all the data stored on the magnetic storage media and data recovery is impossible even with the use of other recovery software or advanced laboratory instruments.

Apart from requiring less time to destroy data than overwriting, degaussing technique is especially suitable for use on damaged hard disks because overwriting may not be performed properly on these hard disks.

During the degaussing process, it is important to follow the operation manual provided by the manufacturer to avoid improper usage, which can lead to a large amount of information remaining on the magnetic storage media.

Physical Destruction

Physical destruction generally refers to the destruction of physical storage media by shredding or disintegration. This method is suitable for destroying data that cannot be securely deleted by overwriting or degaussing.

For storage media which have been used for storing sensitive information, physical destruction is recommended even after overwriting or degaussing method has been applied. This is to ensure complete and secure deletion.

As technology in storage media keeps advancing, the aforementioned methods are for reference only. On actual application, the most effective secure deletion method should be selected according to the technology used in the storage media.

To learn more about information security, please visit the InfoSec website at:

http://www.infosec.gov.hk