

MEDIA SANITISATION



**Deleting data does not necessarily delete the files from the media. Instead, most file systems only remove the link to the data. ACEHOBA offers socially responsible and regulatory compliant companies, a secure and ethical way of disposing of data.**

.....  
**Contact ACEHOBA to discuss your requirements:**

T: (+350) 200 40157  
 E: helpdesk@acehoba.com  
 W: www.acehoba.com  
 A: Suite 23, Watergardens 6, Gibraltar

**How does file deletion work?**

When a file is deleted, the data contained is not necessarily deleted. Typically, just the file name or some other link identifying the file, is deleted. This way, the space on the media associated with the deleted files can be re-allocated for re-use. However, until the data is overwritten, the residual physical representation of the data, e.g. data remanence, may still remain on the media and the data may be recoverable.

**The actual data has been overwritten. Does this make it unrecoverable?**

The simple answer is – no. Data which has been deleted, e.g. overwritten once or even twice, can still be recovered through the use of commercially available software. A hard drive for example, contains an image of everything ever written to it; however, the older the data the less visible it is. Also, as a hard drive ages some of its sectors used for storage fail to meet working parameters (as seen by the drive electronics), and as a result are marked as not suitable for re-use. During a normal overwrite process they are ignored, leaving the data stored there open to retrieval.

**What are the recommended guidelines for secure deletion of data so that it is not recoverable?**

The number of times data is overwritten depends on the sensitivity of the data and the potential impact if it is recovered. It can vary widely from 3 to 35. Typically, for data of a confidential nature, it is sufficient to overwrite it in the region of 8 times.

**Does media which is to be re-used internally still need to be deleted securely?**

In most companies, different users have different access privileges. To maintain data confidentiality, it is advisable to at least clear data (see below).

**Data classifications and sanitisation techniques**

The following are best practice guidelines based on data classification offered by ACEHOBA:

<u>Data</u>	<u>Technique</u>
<b>Public</b>	Disposal – the act of discarding media without any sanitisation considerations.
<b>Proprietary</b>	Clearing – the act of erasing data so that it cannot be recovered by using keyboard commands.
<b>Confidential</b>	Purging – the act of erasing data so that it is unlikely that a laboratory attack would recover the data.
<b>Highly Confidential</b>	Destroying – after media is destroyed it cannot be reused as originally intended.

Media is disposed of in compliance with WEEE regulations and certificates can be produced.

**ACEHOBA's fees for data deletion**

The fees for secure data deletion depend on the media type, the security level required and the size of the media. For example, the fee for securely deleting (using eight pass scrambling) an 80GB hard drive is £25.