



secure data destruction solutions

WHY ERASE DATA?

Tough regulations, the high cost of data breaches and the risk of data leaks means that it is imperative that the proper processes and procedures are implemented to ensure the complete and secure disposal of sensitive information.

CERTIFIED SOLUTIONS

ACT Logistics offers a number of secure data destruction and disposal solutions ensuring you meet regulatory compliance requirements. Full reporting and certification is provided to all customers detailing extensive information about each asset and the services performed.

WHAT IS DOD 5220-22.M STANDARD?

This program is run either from a CD or via the network to overwrite all addressable locations with a random character, overwrite with the characters compliment, and then verify. The Department of Defense (DOD) standard 5220-22.M requires 3 wipes. We recommend a 7 wipe process be used for servers or more sensitive sites.

COMPUTER HARD DRIVES

Data removal as required by Federal Government is a minimum 3 wipe process. ACT Logistics uses the widely accepted practice of deletion of data to Department of Defense DOD 5220-22.M (3 Wipe) standard unless otherwise specified. This process typically takes 2-3 hours (depending on the hardware specifications).

In the event of disk failure or corruption of the hard drive, ACT Logistics physically destroys the drive.

PRINTER HARD DRIVES

Modern multifunction printers and copiers have a similar hard drive to those found in PC's and laptops. These machines automatically store any document that has been printed or copied on the hard drive. This means that these units may contain sensitive data on the hard drive which must be destroyed. This is often overlooked in many organisations.

The same measures must therefore be practiced as with computer hard drives.



USB AND OTHER FLASH MEDIA

These devices present a significant challenge for many organisations. Their small size and ease of use allows unsupervised visitors or unscrupulous employees to smuggle data out with little chance of detection therefore proper data destruction is imperative.

Software is available to overwrite the data so the devices can be reused however from a cost perspective ACT Logistics recommend the physical destruction of these devices (via incineration).

Other methods of physical destruction that are available include: disintegration, pulverization, shredding, melting, sanding and chemical treatment. These methods do not actually destroy data but makes the media inoperable preventing data recovery.





secure data destruction solutions

ZIP, JAZ AND REV DISKS

There is a very limited second-hand market for these storage devices and as a result ACT Logistics would recommend physical destruction (as described above) for these products.

As per the USB devices software is available to overwrite data should a customer wish to reuse these disks.

MOBILE PHONES

Smart phones carry vast amounts of data in both internal / external memory and SIM cards. This generation of phones need to be treated as seriously as a laptop computer in order to avoid data breaches.

Where these phones are to be reused and redeployed within a corporate environment it is essential to use software to overwrite the data.

Alternatively these phones can be physically destroyed (as previously mentioned).

CONFIDENTIAL INFORMATION

Some staff leave personal items such as CD's, DVD's, Secure ID token's, USB keys etc in laptop carry bags or official and confidential information in printer trays or copiers. As part of our QA process we ensure there is no physical media, devices or printed information remaining in carry bags, printer trays, or photocopiers. Should there be any corporate information this is either returned to the organisation or physically destroyed.

