Data Destruction

# Data Destruction

'Data destruction' is the process of erasing or otherwise destroying data stored on virtual/electronic or physical mediums such as, but not limited to, printed copies, tapes and hard disks in order to completely render data irretrievable and inaccessible and otherwise void.

## The base principle

For legislative, regulative, privacy and security purposes, it **must** be possible to decommission and delete (irreversibly 'erase' or 'destroy') data and confirm to a degree of relative confidence it has been completed.

Data should be erased from all related systems, such as disaster recovery, backup and archival, subject to reasonable data lifecycle caveats.

## Destruction standards

The following standards and guidelines are the *minimum* basis for data decommissioning or destruction. Follow and apply them as appropriate. There might also be extra steps specific to a data set or system.

* National Cyber Security Centre (NCSC) guidance on end-user device reset procedures: <https://www.ncsc.gov.uk/guidance/end-user-device-guidance-factory-reset-and-reprovisioning>
* NCSC guidance on secure sanitisation of storage media: <https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media>
* NCSC Cloud Security Principle 2: Asset Protection and Resilience (Data Destruction): <https://www.ncsc.gov.uk/guidance/cloud-security-principle-2-asset-protection-and-resilience#sanitisation>
* Payment Card Industry Data Security Standard (PCI-DSS) (Data Destruction): <https://www.pcisecuritystandards.org>
* DIN: <http://www.din-66399.com/index.php/en/securitylevels>

Data Destruction for electronic/magnetic storage **must** include, unless otherwise superseded by NCSC, PCI-DSS or specific Ministry of Justice (MoJ) guidance:

* the revocation or otherwise destruction of decryption keys and/or mechanisms to render data inaccessible or otherwise void through the use of modern cryptography; AND/OR
* data overwriting methods consisting of at least 3 (three) complete overwrite passes of random data.

Data Destruction for printed materials **must** include, unless otherwise superseded by NCSC or specific MoJ guidance:

* paper cross-shredding methods to satisfy at least the DIN 66399 Level 4 standard with a maximum cross cut particle surface area 160 (one hundred and sixty) millimeters squared with a maximum strip width of 6 (six) millimeters

## Data lifecycle caveats

Automated systems involved in data management and associated lifecycles may not be capable of immediate destroying data on demand.

Examples of such systems are data backup and disaster recovery solutions that have a defined and automated data cycle and retention system.

There is generally no need to attempt to manually delete such data prior to the automated retention lapse as long as it is ensured that if the data is restored prior to data destruction it is not processed.

It is important that the final expected data where all data lifecycles will have completed to be readily identifiable with high confidence.