

Data Destruction Policy 2011

This document provides specific guidance on the techniques and procedures involved in the data recovery, data destruction and product repair at Datastor. HMG Information Assurance Standard 5, (known as IA5) describes how to treat Protectively Marked information at various Impact Levels (IL). At Datastor, all media are treated as “Protect – IL2” as standard. Customers wishing drives to be treated as “Restricted – IL3” or “Confidential – IL4” will need to notify Datastor in advance. Data is not read in any of the activities undertaken at Datastor.

Datastor ensures that the highest appropriate security management arrangements are in place for the protection of client information during the provision of data destruction services in order to meet the requirements set out within IA5, further defined within EN15713:2009. Commercial clients can choose whether or not to follow these guidelines.

IA5 Level	Impact level	Business Impact Levels - examples	Magnetic Media			Optical
			Electrical sanitising by software overwrite	Electrical destruction by Degaussing	Physical destruction	Physical destruction
SSL2	Confidential IL4	Risk to a group of individual's safety and liberty. Undermine the financial viability of a major UK-based or UK-owned organisation.	CESG Higher Level	CESG Higher Level	Onsite Destruction Shred to 16mm particles Offsite Destruction Degauss at "CESG Lower Level" onsite then shred to 16mm offsite	Shred to 6mm particles
	Restricted IL3	Undermine the financial viability of a minor UK-based or UK-owned organisation.	CESG Lower Level			
SSL1	Protect IL2	Inconvenience an individual. Undermine the financial viability of a number of UK SMEs.	CESG Lower Level or Unassured software	CESG Lower Level	Shred to 16mm particles	
	Unclass'd IL1	Cause a loss to Public Sector of up to £1,000.				

Procedure

The following steps outline the policy of data destruction at Datastor.

1. Customer sends the drive to Datastor, identifying the media as a data destruction device and stating the Impact Level of the data. Datastor can also collect from customers' site.
2. Upon receipt, drives are logged and placed into a secure area until destruction begins.
3. Functioning drives can be electrically cleansed by software overwriting.
4. Faulty drives are electrically cleansed by degaussing.
5. If required, media will be physically destroyed and disposed of by Datastor.
6. All data destruction will be logged and certificated by serial number where possible.

Methods

The available methods of data destruction are listed below.

1. **Electrical Cleansing** by
 - a. **Software overwriting** is the process of completely filling a media with meaningless data so that all meaningful data is erased. Drive is reusable.
 - b. **Degaussing**, when properly applied by passing a massive magnetic field across any magnetic media, renders unreadable any previously stored data. Drive becomes permanently unusable.
2. **Physical destruction** is the process of physically destructing a media so that data cannot be retrieved.

Datastor retains a strict policy to ensure that all data on tapes, solid state media, optical disks and other removable media is destroyed on receipt. All jammed magnetic media inadvertently sent with a tape drive will be removed and held in a quarantine area. Any optical media such as CDs and DVDs will be physically destroyed. Any removable media that requires returning must be advised within 3 working days of shipping to Datastor.

Datastor operate a policy of integrity and honesty, should a client wish to observe the data destruction process, they may do so. Datastor works in partnership with our clients to ensure compliance with Environmental Legislation and the Datastor Environmental Policy.