



Protecting the integrity of data, for you and your customer

This document provides specific guidance on methods, processes and procedures to ensure no data remains on computer hard drives and removable media that's repaired and processed by NCE Computer Group. All drives are treated as "Sensitive Data" as standard. Customers wishing drives to be treated as "Secure Data" will need this to be made known to NCE and additional charges may occur.

No Data is ever read. The first activity is to format the drive or remove any removable media, followed by the erasing of any client data, this process occurs as soon as the unit enters the workshops.

<p>FORM 06-04-001</p> <p>TITLE: Data Security & Destruction of data</p> <p>1. OBJECTIVE</p> <p>To ensure the security of our customers' data whether we are performing repairs or replacements to data storage devices</p> <p>2. SCOPE</p> <p>This procedure covers how NCE ensures the destruction of all customers' data and to show how this is maintained and logged at all stages. Data is categorised into two areas as follows: -</p> <p>Sensitive Data: This is the least aggressive form of data destruction, the data is removed electronically and would normally be sufficient for most customers.</p> <p>Secure Data: This is where the data is physically destroyed and the media returned to customer or disposed of by NCE at an approved site.</p> <p>3. PROCEDURE</p> <p>3.1 NCE customer services issue an RMA and records the level of security required. This is determined by the customer and set out in section 2 above. Whether data is sensitive or secure. Customer is informed to print clearly on the exterior of the box ' FAO Department D'</p> <p>3.2 Customer ships drives to NCE clearly identifying box FAO Department D</p> <p>3.3 Upon receipt drives are unboxed entered onto the repairs database and the drives are passed immediately to a senior engineer or placed into allocated secure area until authorised staff can disposition drives.</p> <p>3.4 Apart from manufacturers, No third parties are involved in the repair operation.</p> <p>3.5 For sensitive data, functioning hard drives are tested on bespoke test software. This utility writes several predetermined data patterns covering the entire data surfaces destroying all previously recorded data. This is done on a block by block basis and covers all of the data areas on the disk.</p> <p>3.6 A drive deemed faulty and under manufacturers warranty is bulk erased destroying all data and servo information.</p> <p>3.7 Drives deemed faulty and are not covered by manufacturers warranty are bulk erased, The drives are then shipped to an Environment Agency approved site for precious metal reclamation.</p> <p>3.8 For secure data points 1 through to 5 are to be implemented except point 6.</p> <p>3.9 For all secure data drives the media will be removed. The media is scored and bulk erased, the drive serial number along with the data destruction number are written on the individual platters.</p> <p>3.10 The platters are placed in an allocated "Secure" area until shipping to customer via recorded post.</p> <p>3.11 All data destruction will be recorded in the log held in the QA department.</p> <p>3.12 NCE customer support will issue a data destruction certificate (03-04-004 iss. 002) as soon as data has been destroyed.</p> <p>3.13 The drive then follows the standard repair/replacement procedure.</p>	<p>ISSUE: 002</p> <p>PAGE: 1 OF 1</p> <p>DATE: 03/07/2009</p>
--	---

Methods and equipment for data destruction on removable media

NCE has a strict policy to ensure that all data on tapes, optical disks & other removable media is destroyed on receipt in the workshops. All magnetic media that jammed in drives will be removed from the drive, then degaussed* and finally physically destroyed. Any optical media such as CD's & DVD's will be physically destroyed. MO media will be treated as magnetic media.

Any removable media that is required to be returned to customers must be advised in writing prior to shipping to NCE and must be clearly marked on any incoming paperwork.

* Further information on degaussing methods can be found in text of the Hard Drive section found below.

Methods and equipment used for hard drive sanitisation and clearing

Overwriting is the process of replacing information (data) with meaningless data in such a way that meaningful information cannot be recovered from a hard drive. Overwriting Software will be used to overwrite hard drives.

NCE use a software product called Disk-Purge which is manufactured by Tabernus. Disk-Purge Declassification software is DES/DOD endorsed for completely and thoroughly sanitising any hard drive device to the following standards. DOD 5200.28, NCSC-TG-025, AFSSI 5020, OPNAV 5510 and AR-380-19.

Degaussing (i.e., demagnetizing) is a procedure that reduces the magnetic flux of a medium to virtual zero by applying a reverse magnetizing field. Properly applied, degaussing renders any previously stored data on magnetic media unreadable. This should be used as a last resort, as it renders the hard drive unusable.

NCE use the Verity Systems SV91M degausser which has been approved by the UK Government and meets the specified requirements of SEAP (Security Equipment Assessment Panel) for the secure erasure and destruction of information and data stored on magnetic media up to TOP SECRET level. Also meets German security approval DIN33858.

Destruction of a hard drive is the process of physically damaging a medium so that it is not usable in a computer and so that no known exploitation method can retrieve data from it.

Clearing data (deleting files) removes information from storage media in a manner that renders it unreadable unless special utility software or techniques are used to recover the cleared data. However, because the clearing process does not prevent data from being recovered by technical means, it is the least secure method of sanitising hard disk storage media.



ISO 9001 AND 14001 REGISTERED FIRM

NCE Services

Your Partnership for Data Storage

Repair

Supply

On-site

PEP

Adv Exchange