Access Intelligence Secure Data Erasure & Asset Disposal Guide

1.0 *Overview*

When IT infrastructure reaches the end of its useful life, there are two primary considerations relating to how it should be disposed of:

- The first relates to the secure erasure of all data that may be stored on the disposed assets: in the UK, Directors have responsibility to ensure their organisation's full compliance with GDPR 2018, as well as any other applicable legislative or contractual requirements which may apply.
- The second relates to the environmental perspective: with an increasing amount of UK and European legislation requiring Company Directors to ensure that assets are disposed of in an environmentally responsible manner, in accordance with, amongst others, WEEE Regulations (Waste Electrical and Electronic Equipment) and RoHS Regulations (Restriction of Hazardous Substances).

2.0 *Asset Disposal Considerations*

2.1 Accountability and Traceability

Disposal of assets needs to be conducted in enough detail to provide complete traceability of which assets have been disposed of, when, in what way, by whom and how. This task starts with initial identification of those assets that are due to be disposed of, which should be sufficiently identified by serial numbers and appropriately updated within the Company's asset register, which in the case of Access Intelligence is Snipe-IT.

The tracking of assets through transportation, processing and data destruction (see Sections 2.2 to 2.4 below) should also be recorded, providing full accountability of how assets have been disposed of.

2.2 Outsourcing Disposal Activities

Very few organisations have their own effective on-site asset disposal function, so inevitably when the time arises for disposal of equipment with sensitive data, they will need to engage with a specialist company to undertake the task on their behalf. When assessing the suitability of a potential disposal/recycling supplier, there are a number of important things to take into consideration:

- How long has the company been established, and what is its existing client base?
- Can they provide client references, and can these be verified with the clients?

- Do they operate full quality, environmental and security processes? Are these accredited and certified?
- Are their premises and facilities properly secured against all conceivable risks?
- Are their employees' security screened?
- Are their data destruction tools and methods the latest available? Do they produce logs?
- What waste recycling/recovery activities are used for assets which are to be disposed of?
- Are they registered as a waste processor under the WEEE Directive (see Section 3.0)?
- Are you able to visit their site and fully observe and audit their operations?
- If so, how strict were the security arrangements for your visit? Were they adequate?

2.3 Transportation

Secure methods of collection and transportation are required to ensure that redundant IT assets are properly and securely transported between locations without risk of theft or data exposure. To achieve this, the following transportation controls should be implemented:

- All asset transportation should be undertaken on a point-to-point basis, with no distribution hubs or multiple collections en route. Assets should be secured into the vehicle at the point of collection, and only be unsealed and unloaded when it arrives within the secure compound at the disposal facility location.
- GPS and real-time vehicle tracking should be employed to ensure total visibility of the route of the assets, including time-stamping the collection and delivery points.
- Collection and delivery drivers should ideally be vetted and properly trained, and familiar with emergency procedures to be followed in case of any incidents.

2.4 Processing

Any facility utilised for asset disposal, whether owned and operated by the originating organisation or an external supplier, should have the following security controls in place:

- A secure perimeter to prevent unauthorised access or interference with the facility.

- Comprehensive internal and external CCTV recording all asset disposal activities, with recordings maintained and securely stored for a minimum of 30 days.

- Effective access control measures (including ID cards, access control doors, biometric scanners and other similar devices), including the means of logging personnel access activity, and processes for granting and revoking access.

- A processing audit trail, capable of providing information on the location and status of every asset progressing through the facility.

2.5 Data Destruction

Contrary to some perceptions, it is not necessary to destroy each asset that is no longer required. What is important is to identify those elements of an asset that either do or can hold data and isolate these to undergo a specific data destruction process. These items normally include hard disk drives and removable optical or magnetic media, where the originating organisation should satisfy itself that it has the skills to identify these components, or if not that its external disposal partner has.

2.5.1 Hard Drive Data Wiping

With modern computer operating systems, data is never actually fully deleted from the hard disks when a file or folder is deleted. Instead, the area on the hard disk that the data occupies is simply marked as free for future use and is therefore available for overwriting. The use of the "undelete" command and the ability to restore from the recycling bin demonstrate that this "deleted" data can be quickly and easily recovered. Formatting a hard drive may appear to permanently remove data from a previously used hard drive, but here again this data can be easily recovered by running one of several readily available software utilities.

Organisations need to be aware that hard drives can now be found in equipment other than computer systems: modern photocopiers have one to store and process scanned images, security systems use them for the digital recording of CCTV systems, and they also exist as standalone backup storage devices with simple USB connections.

2.5.1.1 Zero Fill

The only secure way to ensure that a hard drive does not contain recoverable data, without physically destroying it, is to ensure that every track, sector and cylinder of the drive has been overwritten with a predefined pattern or random data. Hence, all the existing data on the hard disk including the operating system is destroyed, making data recovery impossible. The zero character (0) is usually used for this, giving rise to the term "zero fill". The benefit of the zero-fill method is that the hard drive can then immediately be re-used rather than having to be destroyed.

2.5.1.2 Degaussing

Data is stored on hard drives in small magnetic domains. A different method of permanently removing the data from a hard drive is to subject it to "degaussing", or the application of a strong electromagnetic field which randomly changes the alignment of the domains making the previously held information permanently unrecoverable. Hard drives subject to degaussing are, however, normally unable to be reused, as the degaussing activity also damages the sensitive circuitry which controls how the hard drive operates.

Devices used to perform degaussing should be compliant with the CESG Degaussing Standard which has two levels. "Lower Level", for information classified as Restricted and below, and "Higher Level for information classified as Confidential and above.

2.5.1.3 Shredding

Hard drives can also have their data destroyed by being physically destroyed. This normally takes the form of the drive being shredded by specifically designed heavy machinery, which should conform to "HMG Infosec Standard 5" which specifies that all shredding should produce the smallest possible pieces. In order to ensure maximum compliance with the WEEE Directive, the shredded materials should be segregated into constituent parts (metals, plastics, circuit boards) before recycling.

2.5.2 Removable Magnetic/Optical Media Data Destruction

Removable tape media (backup tapes, floppy drives etc.) can have their data wiped using the same three options for hard drives in Section 2.5.1. Many organisations consider the time and costs associated with "zero fill" data overwriting excessive for the low unit cost price of the removable media. Degaussing is sometimes used for removable magnetic media which, dependent on the method and strength of the degaussing may leave the media suitable for subsequent re-use (optical media cannot be degaussed). The quickest, cheapest and safest method of removing data from all types of removable media is destruction by shredding, as noted earlier.

3.0 ***Recycling and Residual Value***

Having securely removed data using one of the options explained in Section 2.5, the residual assets (chassis, circuit board, monitors etc.) need to be addressed under the UK WEEE (Waste Electrical and Electronic Equipment) Directive. This requires for one of four options to be taken in order to present evidence of compliant waste disposal:

- Equipment is refurbished or remanufactured and available on the market for re-sale
- WEEE has been treated, and the component materials received at a re-processing facility
- WEEE has been treated, and the component materials passed through customs for export
- WEEE has been treated overseas, and passed to a reprocessor for recovery or recycling

Dependent on the age, functionality and residual value of the assets, the first option may be the most appropriate. Otherwise, the assets will need to be broken down and passed for recovery or recycling in order to comply with WEEE Directive.

4.0 *In-Life Equipment Failure*

An additional consideration relates to IT infrastructure that for whatever reason fails prior to its scheduled end of life retirement. Many organisations fail to identify that equipment or components being returned to vendors or resellers under warranty is often shipped still loaded with organisational information or records. Detailed discussions should take place with vendors and resellers before this happens to understand the actions to be taken when such equipment or component failures occur

- Does the vendor/reseller provide a facility to securely wipe the organisation's residual data?
- How secure is this process? And the transportation back to the vendor/reseller?
- Otherwise, is there a requirement to securely wipe the residual data before returning?
- Are there any data wiping methodologies which may invalidate warranty returns?

5.0 *Document Version Control*

This guide needs to be reviewed annually as an absolute minimum, or if required changes are identified to address one or more of the following:

- An identified shortcoming in the effectiveness of this guide, for example because of a reported information security incident, formal review or audit finding.
- A change in business activities (e.g. mergers and acquisitions) which will or could possibly affect the current operation of the Access Intelligence Information Security Management System, and the relevance of this document.
- A change in the way in which Access Intelligence manages or operates its information assets and/or their supporting assets, which may affect the validity of this document.

The current version of this policy, together with its previous versions, shall be recorded below.

Version History

Revision	Author	Date	Reason for issue
1.0	David Roud	31/10/2018	First version, to enable Access Intelligence to achieve ISO 27001 accreditation
2.0	Ato Abraham	26/11/2019	Amendments made in preparation for ISO 27001 accreditation audit
3.0	Adam Palmer	13/12/2021	Annual approval
4.0	Adam Palmer	09/01/2023	Annual policy review

Approver(s)

Name	Role	Signature	Date
Mark Fautley	Chief Financial Officer		20/01/2022
Mark Fautley	**Chief Financial Officer**		**19/01/2023**