



Data Capability Requirements v6.3

This document presents the minimum sanitisation requirements by media type or by product, for ADISA Asset Recovery Standard 8.0 and specifically criterion 3.4.1. The requirements set out below are subject to change following any new research or forensic assessment undertaken which indicates that the sanitisation techniques applied are no longer appropriate. Certified ITADs may provide a higher level of service than the DIAL rating of the ITAD's customer should they prefer to do so.

Data Storage Definitions

Volatile Storage.

Computer storage devices which requires power to maintain the ability to retain the data. The dissipation of the stored data is almost immediately from the point where power supply is ceased or after any battery backup has been exhausted. (e.g. CMOS RAM). This means that volatile storage will be free from data when an ITAD makes a collection.

Non-Volatile Storage.

Storage devices which do not require power to maintain the ability to retain stored data. All non-volatile storage devices or products using non-volatile storage, are subject to data sanitisation to ensure that the data which is present on the device is treated in a suitable way to maintain its confidentiality. The following are examples of non-volatile storage within scope of Standard 8.0.

- **Magnetic Hard Disk Drives (MHD)**

MHD are mechanical devices constructed as one or more rigid rotating platters, a motor drive spindle, actuator arm with head and casing. Data can be written to, or read from, the platter(s) which is coated in magnetic material, typically a ferromagnetic material. The platters(s) spin at high speed while the arm moves across the surface to read/write data to specific sectors.

The data is stored in the form of magnetic patterns with each pattern representing binary code (0 and 1) with the head able to magnetize each sector to write data or detect magnetic changes to read data.

Connection to these devices is via an interface such as ATA or SCSI.



Data Capability Requirements v6.3

- **Solid State Hard Drives (SSD)**

SSDs are non-mechanical devices constructed of integrated assemblies to store and retrieve data. Unlike MHD they do not rely on mechanical components but utilise memory chips (typically NAND flash memory) along with a controller chip. SSDs have a faster data retrieval rate than MHD which makes them attractive to use but typically have a shorter lifespan. To resolve this, SSDs are designed purposely with over provisioned storage areas to extend the lifespan of the device. This is achieved via the controller chip which shares the workload out between the different NAND cells using a mechanism known as wear levelling. In a physical sense, SSDs are smaller and lighter than MHDs and consume less power, and so were initially popular in user devices but thanks to improved reliability, higher capacities, and lower pricing they are now being used in most storage environments.

There are different interface types such as ATA, SCSI and NVMe.

- **Embedded Storage (eg eMMC)**

Historically storage media has been a removable component within a product enabling easy upgrade or replacement. As device design has changed, design pressures have resulted in a requirement for smaller user devices which has led the storage to become an embedded part of device itself. This is typically in user devices with flash storage being the preferred choice of storage.

- **Magnetic Tape**

A magnetic storage device which uses a long strip of plastic film coated with magnetic material to store data. Unlike other storage media, data is stored in a linear process so short lengths of tape can include readable information. For this reason, tape destruction is challenging as the surface area of the tape must be reduced significantly to ensure data recovery is infeasible.

- **Hybrid Disk Drives. (SSHD)**

Solid State Hybrid Drives are a storage solution which combines both solid state and mechanical storage technologies. The goal of this design was to provide quick access benefit of solid state but offering the longer life benefit of mechanical storage. At the time of launch it was believed that a market would exist for such a drive, but the decrease in pricing and increase in capacity of SSDs had led to SSHDs being a niche product for storage.



Data Capability Requirements v6.3

- **Network Devices such as routers, switches.**

There are a range of devices which play an important role in the management of data transfers within a computer network. These devices vary in their roles, but all have the capability to hold and store data either on magnetic hard drives or flash-based storage such as SSD. Examples are Routers, Switches, Hubs, Access Points, Modem, Firewall, Gateways and Bridges.

- **Smart Phones and Tablets.**

These are portable user devices which offer very similar architecture and features to each other, but with slightly different primary focus. Smart phones for communication and tablets for working on the move. Each run with an operating system and can be either directly attached to the internet or can be attached via wi-fi networks. Both have embedded flash-based storage media but due to the consistent nature of the operating systems (Android and iOS being the dominant global OS), there is confidence that the sanitisation features used operate consistently.

- **IoT (including flash-based technology such as watches and games consoles)**

IoT (Internet of Things) is a catch all term used to describe the growing list of electronic devices which are now “smart” and connected to either a local or cloud network to provide additional user features and benefits. An example of this being smart fridges and smart televisions. Almost every electronic household device which was standalone is now offering IoT options. Due to the nature of this rapid evolution, there are no universally agreed set of design protocols which means manufacturers can design devices with no constraints other than the ability to connect to each other. This means that sanitisation techniques must be assessed on a product-by-product basis.

- **Printers, Copiers and Multi-function devices**

These are devices which provide printing, scanning, copying and fax/email services. They are typically network devices although can be directly attached to a host, and as their breadth of functionality has become more complex, there are many which now include non-volatile storage for caching or job recall, as well as handling network and communication configurations. They must be viewed as a data storage device until otherwise confirmed as not.

- **Removable flash such as SD Card and USB or rigid magnetic disks**

This includes the now largely obsolete floppy disk drive but also includes any removable direct attach storage such as pen drives and USB drives.



Data Capability Requirements v6.3

- **Optical Media**

This storage format uses optical technology to read and write data. A laser is used to interact with the surface of a disk allowing for storage and retrieval of data. Examples are CD, DVD and Blue Ray.

- **Specialist Devices**

There are industry specific devices, such as Medical Equipment and AV, which may use standard technology, but their operating systems have specific characteristics. These vary device to device and there is a requirement for experts who understand this technology to process them. The requirements reflect this and have been written to allow any non-standard device to fall into this category.



Data Capability Requirements v6.3

Sanitisation Requirements by Media Type

Storage Type	Re-Use			Destroy
	Dial 1	Dial 2	Dial 3	All
Magnetic Hard Disk Drives, Solid State and Hybrid Drives. ¹¹	The software being used by the ITAD shall meet the CLEAR requirements as laid out in a recognised international¹ standard for this media type. With verification of 5%⁴ of user addressable space. Sanitisation activity must prevent data recovery by a threat level 1 attack⁹. (See Exceptions² permissions.)	The software being used by the ITAD shall meet the PURGE requirements as laid out in a recognised international¹ standard for this media type. If PURGE commands are not supported by the firmware the software shall fall back to CLEAR. With verification of 5%⁴ of user addressable space. Sanitisation activity must prevent data recovery by a threat level 2 attack⁹. (See Exceptions² permissions.)	The software being used by the ITAD shall meet the PURGE requirements as laid out in a recognised international¹ standard for this media type. If PURGE commands are not supported by the firmware the software shall FAIL the sanitisation process. With verification of 100%⁴ of user addressable space. Sanitisation activity must prevent data recovery by a threat level 2 attack⁹. (See Exceptions² permissions.)	Platter(s) and every NAND cell(s) shall be physically impaired⁵ to stop its operation and then mixed for aggregation⁶. The use of degaussers on magnetic hard drives shall be governed by 3.4.9 within Standard 8.0 Part 2. NB: Degaussers are not permitted on Hybrid or SSD.
Magnetic Tape	The sanitisation solution which is used by the ITAD shall hold a valid certification ⁷ for tape reuse issued by a recognised	The sanitisation solution which is used by the ITAD shall hold a valid certification ⁷ for tape reuse issued by a recognised independent laboratory	Not permitted	Tape must be treated by two out of three of the following sanitisation techniques: • Shredding • Degaussing



Data Capability Requirements v6.3

	independent laboratory following a written scientific method.	following a written scientific method.		• Incineration⁸
Optical and Paper	Not permitted			Destroy by destruction technique approved in writing by the customer. Material to be mixed for aggregation ⁶ .



Data Capability Requirements v6.3

Sanitisation Requirements by Product Type

Product Type	Re-Use	Destroy
Laptops with embedded storage. ¹¹	Software being used by the ITAD shall hold a certification⁷ for embedded storage which is issued by a recognised independent laboratory following a written scientific method. Sanitisation activity must prevent data recovery by a threat level 2 attack⁹. (See Exceptions² permissions.)	Each storage area, for example NAND cell, shall be physically impaired ⁵ to stop its operation and then mixed for aggregation ⁶ .
Network Devices such as routers, switches.	Software being used by the ITAD shall hold a certification⁷ for networking devices issued by a recognised independent laboratory following a written scientific method with a supported product list in the public domain. Any manual process being used shall be controlled by a written methodology carried out by suitably competent¹⁰ personnel and approved by the customer in writing. Use of the Factory Reset alone cannot be accepted without written evidence being available for each model of device being sanitised. In such cases, this must be approved by the customer in writing.	Platter and / or NAND cell shall be physically impaired ⁵ to stop its operation and then mixed for aggregation ⁶ .
Smart Phone and Tablets. ¹¹	Software being used by the ITAD shall hold a certification ⁷ for the operating system of the phones and / or tablets you are processing. This must be issued by a recognised independent laboratory following a written scientific method.	Each NAND cell shall be physically impaired ⁵ to stop its operation and then mixed for aggregation ⁶ .



Data Capability Requirements v6.3

Internet of Things (IOT) (including Smart Watches and games consoles)	Each device shall be investigated such that the architecture is understood. All areas of non-volatile storage shall be identified. Where data storage media is removable, it shall be removed and treated as per this table. Where the storage is not removable, or the normal sanitisation process renders the device inoperable, ITAD shall either: • follow manufacturer's instructions for data sanitisation and then verify and document the effectiveness. OR • use a software / hardware solution which holds a certification⁷ for the device you are processing. This must be issued by a recognised independent laboratory following a written scientific method. In all cases sanitisation for reuse shall only be done after written approval of this process by the customer.	Each device shall be investigated such that the architecture is understood. All areas of non-volatile storage shall be identified. If storage is removable, it shall be removed and treated as per this table. If the storage is not removable the type of storage shall be identified and then whole device destruction undertaken following a documented risk assessment and after written approval of this process by the customer.
Printers, Copiers and Multi-function devices	All areas of non-volatile storage shall be identified. Where data storage media is removable, it shall be removed and treated as per this table. Where storage is embedded the factory reset may be used but only after written approval of this process by the customer.	All areas of non-volatile storage shall be identified. Where data storage media is removable, it shall be removed and treated as per this table. If the storage is not removable the type of storage shall be identified and then whole device destruction undertaken following a documented risk assessment and after written approval of this process by the customer.
Removable flash such as SD Card and USB or rigid magnetic disks	Not permitted	Destroy by degauss (magnetic disk only) or shred to render the device physically inoperable ensuring that



Data Capability Requirements v6.3

		all NAND cells have been impacted, and then mixed for aggregation ⁶ .
Specialist Devices (e.g Medical Equipment and AV Equipment)	Applicant shall have a written method for the type of specialist device to achieve the following: - Storage Identification - Identify whether each the device contains volatile storage or not. - Reset Functionality - Identify what capability the native device user interface provides and whether a reset or other sanitisation function is available. - Post-reset Accessibility - If a reset or other sanitisation function is available – perform a test to verify reset effectiveness to ensure that subsequent users of the device cannot access original data/information stored in the device. - Repeatability - Create a written sanitisation methodology for each type of specialist device for future use and build up a knowledge bank. - Audit Validation - Following each sanitisation process a unique certificate or other form of evidence shall be created. - Audit Verification - Quality control shall be carried out by a member of the team who is not involved in the sanitisation process. NB: The use of software can be added to the method but is not required.	All areas of non-volatile storage shall be identified. Where data storage media is removable, it shall be removed and treated as per this table. If the storage is not removable the type of storage shall be identified and then whole device destruction undertaken following a documented risk assessment and after written approval of this process by the customer.



Data Capability Requirements v6.3

Footnotes

¹ Current recognised Standards / guidelines are NIST 800-88 rev 1 and IEEE 2883:2022. To submit a different guideline / standard for review by the Advisory Council please email info@adisa.global

² An Exception is defined as a non-standard offering as determined by a specific written customer requirement³. Whilst there may be situations where there are multiple customer exceptions from one ITAD, the ITAD itself cannot deem part of certification to be an exception for the entire ITAD operation.

³ Examples of a non-standard offering could be where a customer requires a specific sanitisation algorithm to be used such as HMG Enhanced or DOD 5220.22-M

⁴ IEEE 2883:2022 only requires 5% of user addressable area to be verified. For DIAL 3 100% verification is required. This verification is typically a configurable feature of the sanitisation software being used which takes place immediately after the sanitisation algorithm/commands complete, rather than being a separate process for the ITAD to undertake.

⁵ Examples of “Physical Impaired” techniques permitted by ADISA are Degaussing of MHD (not permitted on SSD or other flash-based media), Shredding, Disintegration, Pulverization, or Incineration such that data cannot be recovered using a data recovery technique equivalent to ADISA Threat Level 2. This will protect the impaired particles of media from laboratory attacks other than using spin stand, magnetic force microscopy, and decapsulation. The use of aggregation (mixing), anonymization (the original owner of the data of the particles would be unknown) and physical barriers (the material is within a secure ITAD certified by ADISA) will render these types of a laboratory attack unlikely as an adversary within such capabilities will target other areas within the process where “success” will be more assured than attempting a data recovery technique from these particles.

⁶ Aggregation is the process for mixing shredded or deformed material into a mass of other material. This must be achieved immediately after the physical destruction activity has taken place. For example, in the particle bin under the appropriate device.

⁷ To be classified as a valid certification, the certificate held by software shall be issued no more than three years prior to the date of the sanitisation. The certificate shall be issued to the Software version being used. (Note: Newer revisions are permitted to be included under the certificate issued).

⁸ This approach allows data processors to undertake the first of two methods in order to render the media sanitised and aggregated to threat level 1, rather than requiring a data processing agreement with the incinerator company as a sub-processor for the ITAD. The second method of destruction adds robustness to the sanitisation state of the media ensuring it is adequate for threat level 2.



Data Capability Requirements v6.3

⁹ Threat levels of attack, or ADISA Threat Capability numbers as outlined in the ADISA Threat Matrix:

THREAT LEVEL	THREAT ACTOR AND COMPROMISE METHODS	ATTACK EXAMPLES
1	Casual or opportunistic threat actor only able to mount unsophisticated attacks.	Keyboard attacks using the standard device interface using commercial off the shelf (COTS) or open-source forensic tools.
2	Motivated, targeted threat actor such as organised crime or journalists or hackers applying laboratory methods.	Advanced attacks using specialist hardware and software to interrogate the device / storage media using the device interface and component attacks.
3	State-sponsored organisations using sophisticated techniques with unlimited time and resources.	Typical attack may involve proprietary hardware and software techniques not available on the general commercial market.

¹⁰ Competency would be evidenced via suitable training records and / or qualifications.

¹¹The product completion certificate or log will show a minimum of the following:

- Make / Model of device sanitised
- Serial number of device sanitised
- The sanitisation method applied in the process.
- The result of the sanitisation method applied