Security Standard Secure Sanitisation and Destruction (SS-036)

Chief Security Office

Date: 26/10/2023

Department for Work & Pensions

This Secure Sanitisation and Destruction Security Standard is part of a suite of standards, designed to promote consistency across the Department for Work and Pensions (DWP), and supplier base with regards to the implementation and management of security controls. For the purposes of this standard, the term DWP and Authority are used interchangeably.

Technical security standards form part of the DWP Digital Blueprint, which is a living body of security principles, architectural patterns, code of practice, practices and radars, that aim to support Product Delivery Units (PDUs) and suppliers in delivering the DWP and HMG Digital Strategy. Security standards and policies considered appropriate for public viewing are published here:

https://www.gov.uk/government/publications/dwp-procurement-security-policies-and-standards.

Technical security standards cross-refer to each other where needed, so can be confidently used together. They contain both mandatory and advisory elements, described in consistent language (see table below).

Table 1 – Terms

Term	Intention
must	denotes a requirement: a mandatory element.
should	should denotes a recommendation: an advisory element.
may	denotes approval.
might	denotes a possibility.
can	denotes both capability and possibility.
is/are	is/are denotes a description.

1. Table of Contents

2. Revision history

Version	Author	Description	Date
1.0		First published version	11/10/2022
1.1		11.2.7 Replaced DoD 5220.22M with NIST 800-88 Revision 1 Standard for Media Sanitisation	26/10/2023

3. Approval history

Version	Approver title	Role	Date
1.0		Chief Security Officer	11/10/2022
1.1		Chief Security Officer	26/10/2023

This document will be reviewed for continued completeness, relevancy, and accuracy within 1 year of being granted “final” status, and at yearly intervals thereafter.

4. Compliance

Compliance with this standard will be verified through various methods, including but not limited to;

- controls tests performed by first-line teams and by 2nd line activities (e.g. security testing teams)
- security assurance activities to ensure that Architectural Design and delivery are appropriate and aligned to applicable Authority Security Standards. [See Security Assurance Strategy – Ref. I].
- independent external audit

Results of these will be fed back to the appropriate Authority Risk and System Owners.

5. Exceptions process

In this document the term **“must”** is used in bold letters to indicate a mandatory security measure. Any exceptions to the application of this standard, or where specific security measures cannot be adhered to, **must** be presented to the Authority. This **must** be carried out prior to deployment and managed through the design caveats or exception process.

Such exception requests will invoke the Risk Management process to clarify the potential impact of any deviation to the configuration detailed in this standard.

Exceptions to the standard **must** be maintained on a risk register for accountability, traceability, and security governance reporting to senior management.

6. Audience

This document is intended for, but not necessarily limited to, solution architects, security architects, domain architects, technical engineers, security teams, project teams, operations teams, including suppliers that are engaged in the design, development, implementation and operation of systems, services and applications that store Authority data.

7. Accessibility Requirements

Users of this standard **must** consider accessibility design requirements as appropriate. Further information on accessibility standards can be found in Appendix H.

8. Introduction

This standard defines the minimum technical security measures that **must** be implemented when required to securely sanitise and/or destroy media or devices originating within the Authority or used to store or process Authority data.

As the standard only provides minimum measures, they **should** be exceeded as appropriate depending on the threats and risks that need to be addressed, and in keeping with latest security enhancements.

The security measures are derived from industry best practice i.e. guidance published by NIST, CIS and OWASP (see Appendix E for full list external references) and support the implementation of appropriate security controls as selected by the Authority or our third party providers, such as the CIS Critical Security Controls v8 controls set. [see External References].

Every effort has been made to ensure the security measures are vendor and technology agnostic as far as possible; this is to ensure greater applicability of the standard regardless of the technologies used. The security measures **may** be implemented in different ways, depending on the technology choices and business requirements in question.

The aim of this standard is to:

- ensure security controls that are applicable to sanitisation and destruction activities are implemented consistently across the Authority and by third party providers.
- minimise risks from common threats associated with release of media and devices outside their normal operating environment.

Technical security standards ultimately support the achievement of security outcomes sought by the Authority. They set the expectations for what needs to be done and why, to achieve them. The outcomes are based on the official NIST Cyber Security Framework (CSF) sub-categories where possible to ensure close alignment with the NIST Cyber Security Framework, and they can be found in Appendix A of this standard.

9. Purpose

The purpose of this standard is to ensure that Authority data stored on devices and media is not compromised when the device or media leaves its normal operating environment for repurposing, repair, disposal, or destruction.

10. Scope

This standard applies to all media and devices, (virtual and physical), that have stored or processed data both within the Authority and supplier base (contracted third party providers), for the purposes of delivering applications and services that handle Authority data.

Where data sanitisation is required in commodity cloud deployments, this standard must be used in conjunction with the SS-023 Cloud Computing Security Standard [Ref. A], noting that to achieve effective data sanitisation appropriate methods and arrangements should have been specified and agreed during the cloud service commissioning phase.

When considering media and devices that have held large amounts of Authority data, a risk-based decision **must** be made on the appropriate steps to take when considering repurposing or disposal, taking account of the amount and the classification of information stored or processed.

Any queries regarding the security measures laid out in this standard **should** be sent to the Authority.

11. Minimum Technical Security Measures

The following section defines the minimum-security measures that **must** be implemented to achieve the security outcomes described in Appendix A. For ease of reference, the official NIST CSF sub-category ID is provided against each security measure e.g., **PR.PT-3**, to indicate which outcome(s) it contributes towards.

11.1 General sanitisation and destruction considerations

Reference	Minimum technical security measures	NIST ID
11.1.1.	To establish whether it is appropriate to sanitise for reuse or destroy the media or devices, the following criteria **must** be considered: • residual value to the organisation • technological fit • technological currency • expected life • whether the device is repairable • whether the media or device is to be exchanged by the vendor • signs of equipment failure or damage • signs of tampering.	PR.IP-6, PR.DS-5
11.1.2.	Before being released for re-use, all devices/media that have stored Authority data **must** be sanitised on-site (wherever practical and possible) or on an assured site and always in accordance with this standard, see section 11.2. This includes re-use internally within the Authority and externally if being donated or sold.	PR.IP-6, PR.DS-5
11.1.3.	All devices/media **must** remain within a Authority approved, controlled environment until they have undergone appropriate sanitisation, and a robust chain of custody and approvals **must** be recorded and be able to be demonstrated.	PR.IP-6, PR.DS-5

Reference	Minimum technical security measures	NIST ID
11.1.4.	Wherever possible and appropriate an NCSC CPA certified erasure product **must** be used for sanitisation. An Authority approved third party may be used to undertake sanitisation where appropriate. [See External Refences].	PR.IP-6, PR.DS-5, ID.SC-2
11.1.5.	Release of all Authority devices/media **must** be formally signed-off by the respective Authority Risk Owner as remnants of data may persist depending on the technology type in question.	PR.IP-6, PR.DS-5
11.1.6.	If re-use of the device/media is not appropriate, it **must** be destroyed on-site wherever possible, unless it can be appropriately sanitised on-site before being taken off-site for destruction.	PR.IP-6, PR.DS-5, PR.PT-2
11.1.7.	An Authority approved third party contractor **must** be used for both on-site and off-site destruction.	PR.IP-6, PR.DS-5, ID.SC-2
11.1.8.	All off-site destruction **must** be approved via risk acceptance by the relevant Risk Owner which takes into consideration factors such as the media type, data sensitivity, data aggregation and association.	PR.IP-6, PR.DS-5
11.1.9.	A record of the sanitisation or destruction activity **must** be recorded, with appropriate evidence, in an asset management inventory/CMDB.	PR.DS-3, PR.IP-6, PR.DS-5
11.1.10.	If the media or device cannot be sanitised it **must** go through the approved destruction process, in compliance with the minimum requirements as set out in this standard – see 11.3 below.	PR.IP-6
11.1.11.	Media and device records **must** be updated in the asset management inventory/CMDB to indicate sanitisation or destruction status.	PR.IP-6

Reference	Minimum technical security measures	NIST ID
11.1.12.	Sanitisation or destruction records **must** be retained, along with appropriate certificates, in line with the Authority's Information Management Policy [Ref. B] requirements.	PR.IP-6, PR.DS-5
11.1.13.	Where applicable, a full manufacturer's reset to factory default settings, **must** be applied to devices prior to sanitisation or destruction.	PR.DS-5, PR.IP-6
11.1.14.	Where a necessity to sanitise data files on virtual machines arises, NIST SP 800-88 Rev1 [see External References] **must** be considered, applying Cryptographic Erasure (CE) where appropriate.	PR.DS-5, PR.IP-6

11.2 Sanitisation of storage media and devices

Reference	Minimum technical security measures	NIST ID
11.2.1	The types of media or device (physical or virtual) **must** be identified, and a decision made whether: a) the media or device should be put through a sanitisation process. b) the media or device goes straight into the destruction process e.g. Magnetic Tapes - destroy unless there's a legacy business imperative and replacement tapes are no longer available.	PR.DS-3
11.2.2	A record **must** be created, or the status updated, of the sanitisation activity in the asset management inventory/CMDB.	PR.DS-3

Reference	Minimum technical security measures	NIST ID
11.2.3	Any record produced **must** identify if sanitisation is to be carried out by: 1. internal staff 2. manufacturer 3. third-party (go to section on Third-party IT asset disposal (ITAD) suppliers).	ID.SC-3
11.2.4	Appropriate sanitisation software or method for the media or device sanitisation **must** be identified and utilised, in line with the security classification of the data which was stored on the media or device.	PR.DS-5
11.2.5	Media or devices **must** be entered back into the departmental reuse cycle after processing	PR.IP-6
11.2.6	Sanitisation certificates for media and devices **must** be obtained and retained, in line with the Authority's Information Management Policy [Ref B]. See Appendix C for certificate criteria.	PR.IP-6, PR.DS-5
11.2.7	The below sanitisation techniques **must** be followed, as a minimum. If a media or device type is not listed below, advice **must** be sought from the Authority, with an assigned Security Architect or Risk professional; **<u>Networking Devices</u>** – Routers, Switches, etc. Perform a full manufacturer's reset to reset the router or switch back to its factory default settings. **Note**. Refer to the manufacturer for additional information on the proper Sanitisation procedure. Network Devices may contain removable storage. The removable media **must** be removed and	PR.DS-5 PR.PT-2

Reference	Minimum technical security measures	NIST ID
	sanitised using media-specific techniques as set out in this standard. **<u>Mobile Devices</u>** - iPhones, Blackberrys, Devices running Google Android OS, Windows Phone OS, includes all other smart phones, PDAs, Tablets. Select the full sanitise option (typically Erase All Content or a Full Reset) and utilise MDM capability wherever possible and practical. Also, factor in any storage media installed i.e., expandable storage. **<u>Office Equipment</u>** - Printers, Fax, Multi-Function Devices Perform a full manufacturer's reset to reset the office equipment to its factory default settings. **Note.** Office equipment may contain removable storage media, and if so, media-dependent sanitisation techniques may be applied to the associated storage device. **<u>Magnetic Media</u>** - Reel and Cassette Format Magnetic Tapes Re-record (overwrite) all data on the tape using an approved pattern, using a system with similar characteristics to the one that originally recorded the data. For example, overwrite previously recorded sensitive VHS format video signals on a comparable VHS format recorder. All portions of the magnetic tape must be overwritten one time with known non-sensitive signals. Clearing a magnetic tape by re-recording (overwriting) may be impractical for most applications since the process occupies the tape transport for excessive time periods.	

Reference	Minimum technical security measures	NIST ID
	Note: Magnetic Tapes **-** destroy unless there's a legacy business imperative and replacement tapes are no longer available, in which case advice should be sought from the Authority. - ATA Hard Disk Drives This includes PATA, SATA, eSATA, etc. - SCSI Hard Disk Drives This includes Parallel SCSI, Serial Attached SCSI (SAS), Fibre Channel, USB Attached Storage (UAS), and SCSI Express Apply the NIST 800-88 Revision 1 Standard for Media Sanitization. In its guidelines, NIST uses the terms "Clear," "Purge," and "Destroy" to refer to various methods for erasing end-of-life data from storage devices (see Guidelines for Media Sanitization (nist.gov)). A risk assessment **must** be carried out to determine what level of sanitization is required. **<u>Peripherally Attached Storage</u>** - External Locally Attached Hard Drives. This includes USB, Firewire etc. Apply the NIST 800-88 Revision 1 Standard for Media Sanitization. In its guidelines, NIST uses the terms "Clear," "Purge," and "Destroy" to refer to various methods for erasing end-of-life data from storage devices (see Guidelines for Media Sanitization (nist.gov)). A risk assessment **must** be carried out to determine what level of sanitization is required. **<u>Optical Media</u>** - CD, DVD, BD N/A, **must** be destroyed, see section 11.3	

Reference	Minimum technical security measures	NIST ID
	Flash Memory-based Storage Devices - ATA Solid State Drives (SSDs), This includes PATA, SATA, eSATA, etc. - SCSI Solid State Drives (SSSDs) - NVM Express SSDs Apply the NIST 800-88 Revision 1 Standard for Media Sanitization. In its guidelines, NIST uses the terms “Clear,” “Purge,” and “Destroy” to refer to various methods for erasing end-of-life data from storage devices (see Guidelines for Media Sanitization (nist.gov)). A risk assessment **must** be carried out to determine what level of sanitization is required. **Note:** It is important to note that overwrite on flash-based media may significantly reduce the effective lifetime of the media. With flash-based media a minimum of “Purge” level **must** be used. Therefore, risk acceptance **must** be obtained from the Authority if the device is to be re-used or sold. - USB Removable Media, Memory Cards Overwrite with at least two passes, using a pattern in the first pass and its complement in the second pass. **Note:** Not approved for re-use external to the Authority therefore **must** be destroyed if no longer required. - Embedded Flash Memory on Boards and Devices If supported by the device, reset to the original factory settings otherwise destroy, see section 11.3. **Note:** Applying full factory reset does not guarantee complete data erasure therefore minimal data may persist. Risk acceptance **must** be obtained from the Authority if device is to be reused/sold. - RAM and ROM-based Storage Devices	

Reference	Minimum technical security measures	NIST ID
	- Dynamic Random Access Memory (DRAM) Power off the device, remove from the power source, and remove the battery (if battery backed). Alternatively, remove the DRAM from the device. The memory **must** be starved of power for a minimum of 24 hours. - Electronically Alterable PROM (EAPROM) - Electronically Erasable PROM (EEPROM) These types of memory cannot be effectively sanitised to Authority standards therefore **must** be destroyed when no longer required, see section 11.3.	

11.3 Destruction of storage media and devices

Reference	Minimum technical security measures	NIST ID
11.3.1	The types of media or device **must** be identified, and a decision made whether: a) if the media or device should be put through a sanitisation process prior to a destruction process. b) if the media or device goes straight into the destruction process.	PR.DS-3, PR.DS-5
11.3.2	A record **must** be created, or the status updated, of the destruction activity in the asset management inventory/CMDB.	PR.DS-3
11.3.3	Any record produced **must** identify if destruction is to be carried out by: a) internal staff. b) manufacturer. c) third-party (go to section on third-party IT asset disposal (ITAD) suppliers).	ID.SC-3

Reference	Minimum technical security measures	NIST ID
11.3.4	Appropriate methods for physical destruction **must** be identified in line with the security classification of the data which was stored on the media or device.	PR.DS-3, PR.DS-5
11.3.5	Sanitisation destruction records and certificates for media or devices **must** be obtained and retained in line with the Authority's Information Management Policy [Ref. B] if applicable. See Appendix C for certificate criteria.	PR.IP-6, PR.DS-5
11.3.6	The status of media or device **must** be updated in the asset management inventory/CMDB.	PR.IP-6
11.3.7	The below Destruction techniques **must** be followed, as a minimum. **Note.** Only Authority approved third parties **must** be used for destruction of Authority media. If the device is not listed below advice **must** be sought from the Authority, with an assigned Security Architect or Risk professional; **Networking Devices** - Routers, Switches etc. Shred, Disintegrate, Pulverize, or Incinerate by burning the device in an incinerator. **Mobile Devices** - iPhones, Blackberrys, Devices running Google Android OS, Windows Phone OS, includes all other smart phones, PDAs, Tablets. Shred, Disintegrate, Pulverize, or Incinerate by burning the device in an incinerator.	PR.DS-5 PR.PT-2

Reference	Minimum technical security measures	NIST ID
	Office Equipment - Printers, Fax, Multi-Function Devices Shred, Disintegrate, Pulverize, or Incinerate by burning the device in an incinerator. **Magnetic Media** - Reel and Cassette Format Magnetic Tapes Incinerate by burning the tapes in a licensed incinerator or Shred. - ATA Hard Disk Drives This includes PATA, SATA, eSATA, etc. - SCSI Hard Disk Drives This includes Parallel SCSI, Serial Attached SCSI (SAS), Fibre Channel, USB Attached Storage (UAS), and SCSI Express Shred, Disintegrate, Pulverize, or Incinerate by burning the device in an incinerator. **Peripherally Attached Storage** - External Locally Attached Hard Drives. This includes USB, Firewire etc. Shred, Disintegrate, Pulverize, or Incinerate by burning the device in an incinerator. **Optical Media** - CD, DVD, BD Destroy in order of recommendations: 1. Removing the information-bearing layers of CD media using a commercial optical disk grinding device. Note that this applies only to CD and not to DVD or BD media 2. Incinerate optical disk media (reduce to ash). Use optical disk media shredders or disintegrator devices to reduce to particles that have a nominal	

Reference	Minimum technical security measures	NIST ID
	edge dimensions of 0.5 mm and surface area of 0.25 mm2 or smaller. **Flash Memory-based Storage Devices** - ATA Solid State Drives (SSDs), This includes PATA, SATA, eSATA, etc. - SCSI Solid State Drives (SSSDs) - NVM Express SSDs - USB Removable Media, Memory Cards - Embedded Flash Memory on Boards and Devices - Dynamic Random Access Memory (DRAM) - Electronically Alterable PROM (EAPROM) - Electronically Erasable PROM (EEPROM) Shred, Disintegrate, Pulverize, or Incinerate by burning the device in an incinerator.	

11.4 Storage of media or devices prior to sanitisation or destruction

Consideration of storage requirements before processing **must** be taken into account.

Reference	Minimum technical security measures	NIST ID
11.4.1	The media or device **must** be stored in a secure location in line with the security classification of data stored and in accordance with Authority's Security Classification Policy [Ref. C] and the Authority's Physical Security Policy [Ref. D].	ID.SC-2, ID.SC-3, PR.AC-2

Reference	Minimum technical security measures	NIST ID
11.4.2	If transport to a secondary or third-party site is required, a full record **must** be kept of: • the type of media or device ○ the manufacturer ○ it's serial number (or equivalent) ○ it's general characteristics • its original purpose and location • the data that was stored and its security classification • the encryption level implemented • the process to be carried out and expected outcomes • date and time the package was sent or collected	ID.SC-3, PR.AC-2
11.4.3	Any third-party engaged **must** be approved by the Authority.	PR.PT-2, ID.SC-2, ID.SC-3, ID.SC-4
11.4.4	Permission **must** be sought and documented, from the Authority when relocating media or devices.	PR.PT-2
11.4.5	Long term storage of media or devices with residual data **must** be avoided and a risk raised and approved by an appropriate SRO, should it be required. Suppliers **must** inform the Authority if this requirement arises.	PR.PT-2, PR.AC-2

11.5 Third party IT asset disposal (ITAD) suppliers

Reference	Minimum technical security measures	NIST ID
11.5.1	The level of sanitisation and destruction certification that the ITAD supplier holds, **must** be understood, and approved by the Authority, prior to use.	PR.IP-6, ID.SC-2, ID.SC-4, PR.AT-3, PR.DS-3, PR.DS-5
11.5.2	Assurance **must** be given that ITAD suppliers can: a) use secure transport [PR.PT-2] b) document evidence of safe and secure transportation c) provide pickup and drop off times [PR.DS-3] d) give asset tracking locations [PR.DS-3] e) provide personnel vetting status [ID.SC-3] f) provide certificates of sanitisation and or destruction for each asset. See Appendix C for example. [PR.DS-3] g) present a clear down process of ITAD equipment if brought onsite. [PR.DS-3] h) provide a secure physical storage environment, whilst the sanitisation and disposal process are on-going. [PR.AC-2] i) carry out quality assurance checks [ID.SC-4] j) provide third-party accreditations such as ISO27001 (information security management system).	ID.SC-4, ID.SC-3, PR.AT-3

11.6 Third-party (ITAD) responsibilities

Reference	Minimum technical security measures	NIST ID
11.6.1	Third-party ITAD suppliers **must** provide secure collection and transportation services, in line with the Authority's Security Classification Policy [Ref. C] and the Authority's Physical Security Policy [Ref. D].	PR.AC-2, ID.SC-2, ID.SC-3, PR.AC-2, PR.AT-3, PR.DS-3
11.6.2	Third-party ITAD suppliers **must** safely store media or devices prior to sanitisation and or destruction processes, in line with the Authority's Security Classification Policy [Ref, C] and the Authority's Physical Security Policy [Ref. D].	PR.AC-2, ID.SC-2, ID.SC-3, PR.AC-2, PR.AT-3
11.6.3	Third-party ITAD suppliers **must** ensure a register of media or devices processed is maintained.	PR.DS-3, ID.SC-3, PR.AT-3, PR.DS-3
11.6.4	Third-party ITAD suppliers **must** ensure certification of sanitisation and or destruction is made available to the Authority.	PR.DS-3, ID.SC-2, ID.SC-3, PR.AT-3
11.6.5	Third-party ITAD suppliers **must** use accredited auditors to audit the sanitisation and or destruction process and make records available to the Authority when required.	ID.SC-4, ID.SC-2, ID.SC-3, PR.DS-3
11.6.6	Third-party ITAD suppliers **must** assure the Authority that the sanitisation and or destruction equipment is regularly reviewed and maintained.	ID.SC-4, ID.SC-2, ID.SC-3, ID.SC-4

Reference	Minimum technical security measures	NIST ID
11.6.7	Third-party ITAD suppliers **must** ensure that appropriately vetted personnel are utilised in line with the Authority’s Security Vetting Policy [Ref. E], in the transportation, handling, and sanitisation and or destruction process.	ID.SC-3, ID.SC-2, PR.AT-3

12 Appendices

Appendix A – Security Outcomes

The minimum security measures defined in this standard contribute to the achievement of security outcomes described in the table below. For consistency, the official NIST Sub-category IDs have been carried through to the standards.

Table 2 – List of security outcomes mapping

Ref	Security outcome (sub-category)	Related security measure
ID.SC-2	Suppliers and third-party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process.	11.4.1, 11.4.3, 11.5.1, 11.6.1, 11.6.2, 11.6.4, 11.6.5, 11.6.6, 11.6.7
ID.SC-3	Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization’s cybersecurity program and Cyber Supply Chain Risk Management Plan.	11.2.3, 11.3.3, 11.4.1, 11.4.2, 11.4.3, 11.5.2, 11.6.1, 11.6.2, 11.6.3, 11.6.4, 11.6.5, 11.6.6, 11.6.7
ID.SC-4	Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.	11.4.3, 11.5.1, 11.5.2, 11.6.5, 11.6.6
PR.AC-2	Physical access to assets is managed and protected.	11.4.1, 11.4.2, 11.4.5, 11.5.2, 11.6.1, 11.6.2
PR.AT-3	Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities.	11.5.1, 11.5.2, 11.6.1, 11.6.2, 11.6.3, 11.6.4, 11.6.7
PR.DS-3	Assets are formally managed throughout removal, transfers, and disposition.	11.1.1, 11.2.1, 11.2.2, 11.3.1, 11.3.2, 11.3.4, 11.5.1, 11.5.2, 11.6.1, 11.6.3, 11.6.4, 11.6.5

Ref	Security outcome (sub-category)	Related security measure
PR.DS-5	Protections against data leaks are implemented.	11.1.1, 11.1.4, 11.1.5, 11.2.4, 11.2.6, 11.2.7, 11.3.1, 11.3.4, 11.3.5, 11.3.7, 11.5.1,
PR.IP-6	Data is destroyed according to policy.	11.1.1, 11.1.2, 11.1.3, 11.1.4, 11.1.5, 11.2.5, 11.2.6, 11.3.5, 11.3.6, 11.5.1
PR.PT-2	Removable media is protected, and its use restricted according to policy.	11.4.3, 11.4.4, 11.4.5, 11.5.2

Appendix B. Media and devices in scope

If a media or device type is not listed below, advice **must** be sought from the Authority.

Media

- flash memory
- (S)SSD
- magnetic disk drives
- optical
- USB storage
- all forms of SD cards (including all non-volatile memory cards)
- soldered storage attached to circuit boards
- tape

Devices

- desktop computers
- laptops
- servers
- mobile phones
- tablets
- portable storage devices
- networking devices
- network storage systems
- network-attached storage (NAS)
- storage area network (SAN)
- virtual disk drives / devices / machines

Appendix C. Criteria for sanitisation and destruction certificates

Certificates of sanitisation should include:

- Manufacturer of hardware/media
- Model of hardware/media
- Serial number
- Media/device type
- Media/device source
- Sanitisation type – clear purge or destroy
- Sanitisation method – degauss, overwrite, block erase, cryptographic erase etc.
- Sanitisation tool used (including version)
- Verification method

For sanitisation and validation:

- Activity performed by: <<name>>
- Job role
- Date and time (completion)
- Location
- Contact information
- Field for signature of person who performed activity:
    - establish if electronic signature is used, ensure appropriate electronic signature process has been established
    - establish if a wet signature is to be used
- If a remote wipe is undertaken, consider:
    - location of device
    - location of erasure software
    - location of erasure operator.

Appendix D. Internal references

Below, is a list of internal that **should** be read in conjunction with this standard.

Table 3 – Internal references

Ref	Document	Publicly available
A.	SS-023 Cloud Computing Security Standard	Y
B.	Information Management Policy	Y
C.	Security Classification Policy	Y
D.	Physical Security Policy	Y
E.	Security Vetting Policy	N
F.	Digital Blueprint	N
G.	Acceptable Use Policy	Y
H.	Hardware Lifecycle Management Security Policy	N
I.	Security Assurance Strategy	No

Appendix E. External references

The following publications and guidance were used in the development of this standard and **should** be referred to for further guidance.

Table 4 – External References

	External Documents List
1.	HMG Security Classification Policy
2.	DWP Acceptable Use Policy
3.	NIST – Cyber security Framework – 2018-04-16
4.	NIST – Special publication 800-88r1 – Guidelines for Sanitisation https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-88r1.pdf
5.	ISO/IEC 27001:2013
6.	Cloud Security Alliance Cloud Controls Matrix Version 4
7.	Verify suppliers - NCSC.GOV.UK - https://www.ncsc.gov.uk/section/products-services/verify-suppliers?scheme=Commercial+Product+Assurance+%28CPA%29
8.	secure sanitisation of storage media - NCSC.GOV.UK - https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media
9.	erasing devices - NCSC.GOV.UK - https://www.ncsc.gov.uk/collection/device-security-guidance/managing-deployed-devices/erasing-devices
10.	NPSA Standard 'Secure Destruction of Sensitive Items' April 2014 - https://www.npsa.gov.uk/secure-destruction-0
11.	NCSC Commodity Information Assurance Services - NCSC.GOV.UK - https://www.ncsc.gov.uk/information/commodity-information-assurance-services

Appendix F. Abbreviations

Table 5 – Abbreviations

Abbreviation	Definition	Owner
CIS	Centre for Internet Security	Industry term
CMDB	Configuration Management Database	Industry term
DWP	Department of Work and Pensions.	UK Government
GSCP	HMG Government Security Classification Policy	UK Government
ICO	Information Commissioners Office	UK regulator
IPR	Intellectual Property Rights	Industry term
ISO	International Organization for Standardization	Industry term
ITAD	IT asset disposal	Industry term
NCSC CAS	National Cyber Security Centre CAS	UK Special Interest Group
NIST	National Institute of Standards and Technology	US Government
NIST – CSF	National Institute of Standards and Technology – Cyber Security Framework	US Government
OWASP	Open Web Application Security Project	Industry term
SRO	Senior Risk Owner	UK Government

Appendix G. Glossary

Table 6 – Glossary

Term	Definition
Destruction	Where media or devices should be destroyed - it cannot be put to reuse and may require sanitisation prior to destruction.
Device	Any physical hardware (in scope) used by the Authority staff members to access departmental systems or hardware used as part of the Authority ICT infrastructure to underpin the connectivity of and storage of departmental systems' and their data.
Media	Physical devices or writing surfaces including, but not limited to, magnetic tapes, optical disks, magnetic disks, Large-scale integration memory chips (LSI), printouts *but not including display media) onto which information is recorded, stored, or printed within an information system. (NIST Glossary)
OFFICIAL	Information classification mark, identified in the HMG Government Security Classification Policy.
Sanitisation	The process of irreversibly removing data from media or devices

Appendix H. Accessibility artefacts

A variety of accessibility guidance is available from the below URL, that includes:

DWP Digital Accessibility Policy | DWP Intranet

https://accessibility-manual.dwp.gov.uk/

https://www.gov.uk/guidance/guidance-and-tools-for-digital-accessibility

https://www.gov.uk/guidance/accessibility-requirements-for-public-sector-websites-and-apps