National Cyber
Security Centre
a part of GCHQ

NCSC ASSURED SERVICE
CAS SERVICE REQUIREMENT
SANITISATION

Version 2.1

Document History

Version	Date	Description
0.1	June 2012	Initial Draft Version (CAS Service Requirement – Destruction)
1.0	July 2012	Initial Release Version (CAS Service Requirement – Destruction)
2.0	November 2014	Updates to bring document in line with new Government security Classification Policy. Update in title from CAS Service Requirement – Destruction to CAS Service Requirement - Sanitisation
2.1	November 2018	Amended to reflect formation of NCSC

Soft copy location

NCSC-1844117881-495

This document is issued by NCSC

For queries about this document please contact:

CAS Administration Team
NCSC, A2i,
Hubble Road
Cheltenham
Gloucestershire
GL51 0EX
United Kingdom

Tel: +44 (0)1242 221 491
Email: cas@ncsc.gov.uk

The CAS Authority may review, amend, update, replace or issue new Scheme Documents as may be required from time to time.

CONTENTS

REFERENCES

[a] The Process for Performing CAS Assessments, Version 1.2 or later, NCSC

[b] HMG IA Standard No. 5 - Secure Sanitisation, Version 5.0 or later, NCSC

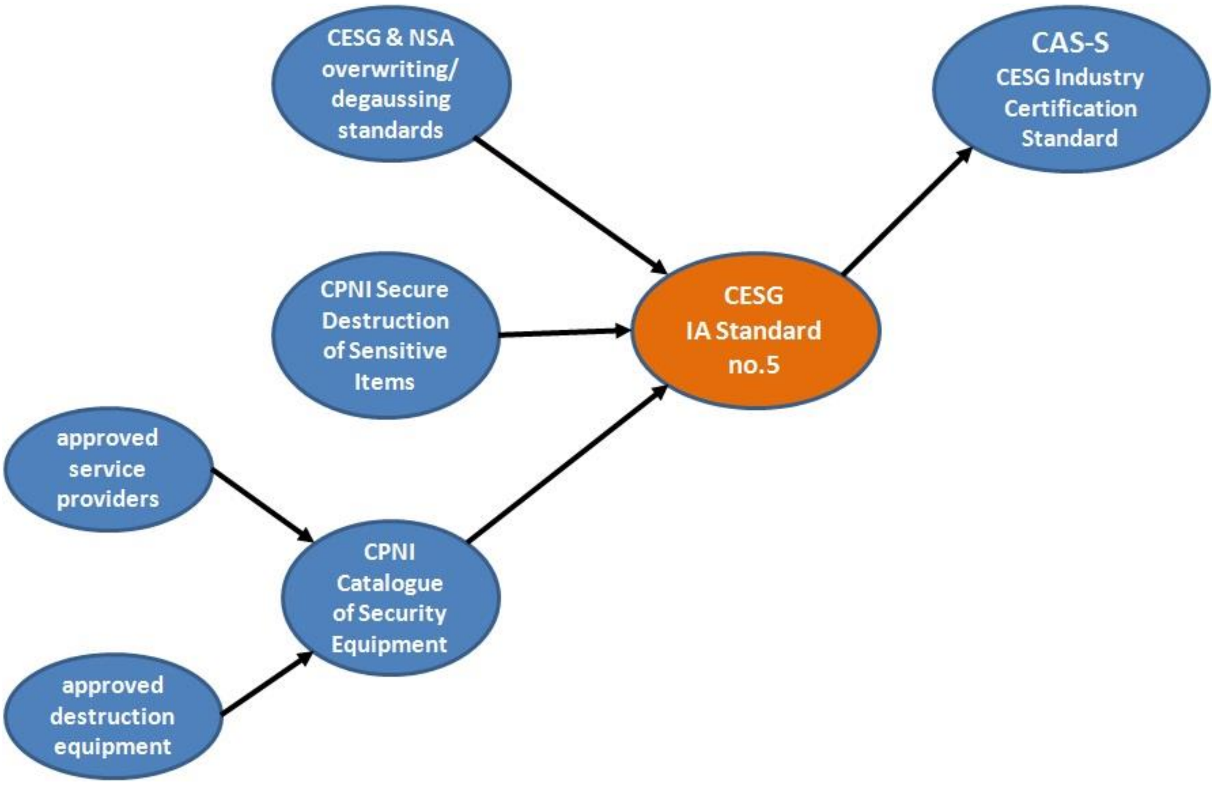
[c] HMG IA Standard No. 4 – Supplement No.9 - Destruction and Disposal of Cryptographic Items, Issue No 3 or later, NCSC

[d] Secure Destruction of Sensitive Items – CPNI Standard, April 2014 or later, CPNI

I. OVERVIEW

1. This Service Requirement supersedes the previous CAS Service Requirement for Destruction.

2. CAS assessment against the Sanitisation Service requirement is a certification scheme to which commercial sanitisation services may subscribe; thus demonstrating compliance with IS5 when serving Government customers.


CESG & NSA overwriting/ degaussing standards
CAS-S
CESG Industry Certification Standard
CPNI Secure Destruction of Sensitive Items
CESG
IA Standard no.5
approved service providers
CPNI Catalogue of Security Equipment
approved destruction equipment

3. IS5 v5.0 onwards has been updated to reflect the new Government Classification Scheme, and abandons the use of Business Impact Levels. This Service Requirement therefore requires companies to sanitise storage media in line with the new Classification Scheme. Where legacy media is being processed, commercial services must come to an agreement with their customers on equivalency between old and new markings.

4. IS5 provides advice for the sanitisation of data at all classifications, recommending the use of good commercially available products for OFFICIAL. For storage media containing data at SECRET and above, IS5 invariably refers to the use of CPNI-approved products and services. The graphic above illustrates the relationship between IS5 and all related documentation.

5. The CAS scheme actively encourages the re-use of current and valid evidence gained through other routes where this evidence meets the requirements of the mitigations within this SR. For example, in the case of this Service Requirement, services which have been approved by CPNI against the ‘Secure Destruction of Sensitive Items’ CPNI Standard, will be able to leverage this as evidence against many of the mitigations listed within this SR.

A. Service Aims

6. In complying with this Service Requirement, Sanitisation Services aim to provide appropriately audited secure sanitisation of HMG Media and Assets (as listed in Annex A of HMG IA Standard No. 5) in line with relevant HMG IA policy and guidance (as detailed in section III.A of this document).

B. Variants

7. A number of different types of sanitisation service can be assessed via this assurance scheme – defined by the scope, the type and the location of the service. A service can be assessed against any or all of the options described below, and will be described accordingly in any NCSC literature regarding the service.

8. **Scope of Service offering** – Services can be assessed and certified against the re-use and/or destruction of any media type and government classification covered within Annex A of HMG IA Standard No. 5 (IS5), up to and including the full range of Media Types at all Classifications. Services covered can be those offering either or a combination of both destructive and non-destructive processes, as defined in point 5 below.

9. **Type of Sanitisation Service offering** –

   i. ***Non-destructive*** – An offering of the Service where the media is intended for re-use but which requires the secure erasure of existing data. The end state of the media will be that it is suitable for re-use in a higher risk or equivalent environment, depending on the requirements of the customer and as defined within IS5.

   ii. ***Destructive*** – An offering of the Service where the media is intended for full destruction and final disposal. The end state of the media will be that it is destroyed in such a way that it is unusable, and is releasable to any environment, as defined within IS5.

   iii. ***A combination* of destructive and non-destructive** – An offering where the Service Provider has the equipment and processes in place to offer either sanitisation for re-use, or full destruction, depending on the media type and requirements of the customer and in line with the requirements of IS5.

10. **Location of sanitisation activities** –

   i. ***Mobile Service*** – Services where the Service Provider has secure vehicles fitted with equipment that can perform sanitisation at the customer's own site or where items are transported using secure vehicles by the Service Provider for destruction at a CPNI approved facility.

   ii. ***Fixed Site Service*** – Services where sanitisation is carried out on the Service Provider's appropriately approved site.

C. Typical Use Case(s)

11. Sanitisation of any Media Type listed within Annex A of IS5, in line with the requirements specified within section III.A of this document. For example:

i. Non-destructive procedures applied to SECRET Hard Disk Drives intended for re-use in an OFFICAL environment.

ii. Destructive procedures applied to TOP SECRET Flash media intended for release to any environment.

iii. A combination of non-destructive procedures, followed by destructive procedures, on TOP SECRET Hard Disk Drives intended for release into any environment.

D. Risks this Service will provide mitigations against

12. Possible attacks that this service should counter come under four categories:

- *Retrieval of data from sanitised media:*
  Attacker gains access to media which has been either incorrectly or incompletely sanitised and is able to retrieve some or all of the data from the media.
- *Insider attack:*
  A member of the Service Provider team (or a third party used as part of the destruction process) subverts the sanitisation process and removes, replaces, or transfers data from a piece of media in their care, which is intended for sanitisation.
- *Unauthorised access to the media prior to sanitisation:*
  An attacker gains access to an item of media while in the care of the Service Provider and is able to remove it, replace it, or transfer data from it.
- *Improper treatment of data:*
  The Service Provider sanitises the wrong media item.

E. Future Enhancements

13. NCSC welcomes feedback and suggestions on possible enhancements to this Service Requirement.

II. SERVICE REQUIREMENT FORMAT

15. All CAS Security Requirements contain a list of mitigations which the Service must meet.

16. Each mitigation includes informational text in italics, describing the threat that it is expected to mitigate. It also lists at least one specific mitigation which describes what must actually be done to achieve that requirement. In some cases there is additional explanatory text which expands upon these requirements.

17. In the requirements listed below, the following terminology can be used:

- ‘Must’, ‘Mandatory’ and ‘Required’ are used to express a mitigation that is essential. All mitigations and detailed mitigations are mandatory unless there is an explicit caveat, such as ‘not applicable to this Service offering’.

- ‘Should’ and ‘Strongly Recommended’ are used whenever a requirement is highly desirable, but is not essential. These are likely to become mandatory in future iterations of the Security Requirement.

- ‘Could’ and ‘Recommended’ are used to express a non-mandatory requirement that may enhance security or functionality.

18. For example:

MITXXX - [A mitigation]

*This mitigation is required to counter [**a threat**]*

For a CAS Service [**requirement**].

For example [**further explanatory comment**].

III. REQUIREMENTS

A. Mitigations

MIT001 – Keep items secure during transportation

This mitigation is required to ensure that processes are in place and understood by Servicer Provider staff in order to reduce the risk of compromise of data and media during transit.

Where the service is being offered as a mobile service (which involves the transportation of any items of media, regardless of whether these have been rendered unusable prior to transportation) then Security Procedures must be in place covering the transportation of media.

For services operating at Official only, these Security Procedures must include provision for the following:

i. ensuring the vehicle is never left unattended while it contains media in transit;
ii. ensuring that the vehicle is locked at all times between loading and unloading of media;
iii. vehicle tracking;
iv. ensuring that vehicle crew are able to communicate with, as a minimum, the vehicle owner and Emergency Services. The crew must be able to use the communications device safely and legally while the vehicle is in motion;
v. Business Continuity, including provision of crew replacement or vehicle replacement e.g in the event of illness, breakdown or traffic accident.

For services operating at Secret or above, these Security Procedures must be in line with the 'Transport of sensitive items' requirements, as defined in the Secure Destruction of Sensitive Items document provided by CPNI.

MIT002 – Secure Storage of Media

This mitigation is required to counter the threat from unauthorised access to the media prior to sanitisation

Where the service is being offered as a fixed site service and offers storage of media at Secret or above, as opposed to immediate sanitisation, the area where media is stored must be List X accredited to a level suitable for the classification of media being stored.

MIT003 - Staff are appropriately cleared

This mitigation is required to prevent uncleared personnel from gaining access to sensitive information.

The Sanitisation Service Provider staff must be suitably cleared as appropriate to the level of media being handled (as detailed in the explanatory comment below). This includes any staff that have potential access to Media prior to destruction, or records regarding customer data.

DV clearance is required for providers offering destruction of media up to and including Top Secret, SC for destruction of media up to and including Secret, and BPSS for destruction of Official media.

MIT004 – Items for Sanitisation are subject to Auditing and Asset management

This mitigation is required to ensure that media is fully accounted for throughout the sanitisation process and that any discrepancies can be investigated at an early stage.

All Sanitisation Service Providers must produce a full audit trail covering the entire service, from receipt of any media through to its final disposal.

Audit documentation must be provided to the customer to show that data has been handled and sanitised appropriately. The Service Provider must have a documented process for raising and investigating any discrepancies, and informing the relevant data owner of such occurrences.

The audit trail becomes vitally important where storage media is re-used in a different environment. It is crucial that the audit log is maintained correctly to track the highest classification of data ever held on the media, and therefore, it can be destroyed appropriately at end-of-life.

MIT005 - Assured equipment and facilities are used

This mitigation is required to ensure that equipment or facilities used as part of the Service meet the requirements of IS5 and so confidence can be gained that media is being successfully sanitised/destroyed.

This mitigation is required to counter exploitation of a failed or partial sanitisation.

The destruction process must use approved products/devices appropriate to the media type and Government Classification of the data being sanitised, as defined in Annex A of IS5. In addition, if part of the sanitisation methodology relies on the use of external facilities (e.g 3rd party incineration facilities) then these facilities must also be approved, as per the requirements of Annex A of IS5.

For example, destruction equipment used by the Service Provider should follow guidelines as outlined in IS5 standard, as appropriate, depending on media type and Government Classifications and corresponding requirements of IS5.

MIT006 – Sanitisation and Destruction equipment is used correctly

This mitigation is required to ensure that Service Providers are using Sanitisation/Destruction Products as they were intended to be used.

This mitigation is required to counter exploitation of a failed or partial sanitisation.

All Sanitisation/Destruction products must be used in line with Manufacturer’s operating procedures, user guides and any published Security Procedures. Sanitisation Service Provider staff must be trained in the correct usage of such equipment and processes must be in place to verify that equipment is being used correctly.

MIT007 – Equipment is maintained

This mitigation is required to ensure that Service Providers undertake regular maintenance of Equipment and secure transportation used as part of the Service, so that confidence can be gained that Equipment is working in accordance with their certifications and reducing the risk of unexpected disruption to the Service.

This mitigation is required to counter exploitation of a failed or partial Sanitisation.

All equipment used as part of the Sanitisation Service (Including but not limited to Sanitisation equipment and secure transportation where the service is being offered as a mobile service) must be subject to regular maintenance, and maintenance records must be kept.

MIT008 - HMG IA Standard No. 5 Sanitisation Methodology is followed

This mitigation is required to ensure that confidence can be gained that media has been appropriately sanitised.

This mitigation is required to counter exploitation of failed or partial sanitisation.

The Service Provider must have documented sanitisation procedures.

These procedures must follow the appropriate processes relevant to the media type and Government Classification of the data being sanitised, as defined in the requirements listed in Annex A of HMG IS5.

The Service Provider must demonstrate that these procedures are followed in practice.

MIT009 – Continuous Audit and Improvement

This mitigation is required to ensure that the service is consistently working as expected and that any security flaws are identified and fixed.

Processes must be in place for providing regular internal audits of the service being delivered, in order to ensure that all processes are being correctly followed and that media is being destroyed as expected. Audits must be conducted by a separate member of staff from the team providing the instance of the service being audited. Processes must be in place to identify and fix any issues identified where the service is not being delivered as expected.

IV. GLOSSARY

19. The following definitions are used in this document:

Term	**Meaning**
CAS	NCSC Assured Service
CPNI	Centre for the Protection of National Infrastructure
Media	In this context Media refers to any item of Media described within Annex A of IS5