13.4. Media and IT Equipment Sanitisation

Objective

13.4.1. Media and IT Equipment that is to be redeployed or is no longer required is sanitised.

Context

Scope

13.4.2. This section covers information relating to sanitising media and IT Equipment. Further information relating to sanitising IT equipment can be found in Section 12.6 - Product Sanitisation and Disposal.

Definition

13.4.3. Sanitisation is defined as the process of removal of data and information from the storage device such that data recovery using any known technique or analysis is prevented or made unfeasible. The process includes the removal of all useful data from the storage device, including metadata, as well as the removal of all labels, markings, classifications and activity logs. Methods vary depending upon the nature, technology used and construction of the storage device or equipment and may include degaussing, incineration, shredding, grinding, knurling or embossing and chemical immersion.

Sanitising media and IT Equipment

13.4.4. The process of sanitisation does not automatically change the classification of the media or IT Equipment, nor does sanitisation necessarily involve the destruction of media or IT Equipment.

Product selection

13.4.5. Agencies are permitted to use non-evaluated products to sanitise media and IT Equipment. However, the product will still need to meet the specifications and achieve the requirements for sanitising media and IT Equipment as outlined in this section.

Hybrid hard drives, Solid State Drives and Flash Memory Devices

13.4.6. Hybrid hard drives, solid state drives and flash memory devices are difficult or impossible to sanitise effectively. In most cases safe disposal will require destruction, this includes any equipment with integrated memory capability. The sanitisation and post sanitisation treatment requirements for redeployment of such devices should be carefully observed.

New Zealand Eyes Only (NZEO) Materials

13.4.7. NZEO endorsed material requires additional protection at every level of classification. In general terms, media and IT Equipment containing NZEO material should be sanitised and redeployed or sanitised and destroyed in accordance with the procedures in this section. Media and IT Equipment that has contained NZEO material must not be disposed of to e-recyclers or sold to any third party.

References

13.4.8.

Reference	Title	Publisher	Source
	Data Remanence in Semiconductor Devices	Peter Gutmann IBM T.J.Watson Research Center	http://www.cypherpunks.to/~peter/usenix01.pdf
	RAM testing tool memtest86+		https://www.memtest.org/
	MemtestG80 and MemtestCL: Memory Testers for CUDA- and OpenCL-enabled GPUs	Simbios project funded by the National Institutes of Health	https://simtk.org/home/memtest
	HDDerase **Capable of calling the ATA secure erase command for non-volatile magnetic hard disks. It is also capable of resetting host protected area and device configuration overlay table information on the media.**	A freeware tool developed by the Center for Magnetic Recording Research at the University of California San Diego.	https://cmrr.ucsd.edu/resources/secure-erase.html?_ga=2.231749531.545206853.1522881172-221519987.1522881172
	AISEP Evaluated Products List (EPL)	Australasian Information Security Evaluation Program	https://www.cyber.gov.au/acsc/view-all-content/epl-products
	ATA Secure Erase	ATA ANSI specifications	https://www.ansi.org/
	Secure sanitisation of storage media	NCSC, UK	https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media
	Reliably Erasing Data From Flash-Based Solid State Drives	Wei, Grupp, Spada and Swanson Department of Computer Science and Engineering, University of California, San Diego	https://www.usenix.org/legacy/event/fast11/tech/full_papers/Wei.pdf [PDF, 1.96 MB]
	The 2012 Analysis of Information Remaining on Computer Hard Disks Offered for Sale on the Second Hand Market in the UAE	Edith Cowan University Research Online. Australian Digital Forensics Conference	https://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1110&context=adf
	2010 Zombie Hard disks - Data from the Living Dead	Edith Cowan University Research Online. Australian Digital Forensics Conference	https://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1085&context=adf
	The 2009 Analysis of Information Remaining on Disks Offered for Sale on the Second Hand Market	Edith Cowan University Research Online. Australian Digital Forensics Conference	https://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1079&context=adf
	NSA/CSS Storage Device Declassification Manual December 2007	NSA	https://www.nsa.gov/portals/75/documents/resources/everyone/Media-destruction/storage-device-declassification-manual.pdf [PDF, 157 KB]

Rationale & Controls

Sanitisation procedures

13.4.9.R.01. **Rationale**

Sanitising media and IT Equipment prior to reuse or redeployment in a different environment ensures that classified information is not inadvertently accessed by an unauthorised individual or inadequately protected.

13.4.9.R.02. **Rationale**

Using approved sanitisation methods provides a high level of assurance that no remnant data is on the media and IT Equipment.

13.4.9.R.03. **Rationale**

The procedures used in the NZISM are designed not only to prevent common attacks that are currently feasible, but also to protect from threats that could emerge in the future.

13.4.9.R.04. **Rationale**

When sanitising media, it is necessary to read back the contents of the media to verify that the overwrite process completed successfully.

13.4.9.R.05. **Rationale**

If the sanitising process cannot be successfully completed, destruction will be necessary.

13.4.9.R.06. **Rationale**

It is important to note that "factory reset" or similar terms **do not** constitute sanitisation of media.

13.4.9.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4169]

Agencies MUST document conditions and procedures for the sanitisation of media and IT Equipment.

Media that cannot be sanitised

13.4.10.R.01. **Rationale**

Some types of media cannot be sanitised and therefore MUST be destroyed. It is not possible to use these types of media while maintaining a high level of assurance that no previous data can be recovered.

13.4.10.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4176]

Agencies MUST destroy the following media types **prior to disposal**, as they cannot be effectively sanitised:

- microfiche;
- microfilm;
- optical discs;
- printer ribbons and the impact surface facing the platen;
- programmable read-only memory (PROM, EPROM, EEPROM);
- flash memory and solid state or hybrid data storage devices;
- read-only memory; and
- faulty magnetic media that cannot be successfully sanitised.

Volatile media sanitisation

13.4.11.R.01. **Rationale**

The following guidance applies in cases where media is to be redeployed.

When sanitising volatile media, the specified time to wait following removal of power is based on applying a safety factor to research on recovering the contents of volatile media.

13.4.11.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4181]

Agencies MUST sanitise volatile media by:

- overwriting all locations of the media with an arbitrary pattern;
- followed by a read back for verification; and
- removing power from the media for at least 10 minutes.

Treatment of volatile media following sanitisation

13.4.12.R.01. **Rationale**

The following guidance applies in cases where media is to be redeployed.

There is published literature that supports the existence of short-term data remanence effects in volatile media. Data retention time is reported to range from minutes (at normal room temperatures) to hours (in extreme cold), depending on the temperature of the volatile media. Further, published literature has shown that some volatile media can suffer from long-term data remanence effects resulting from physical changes to the media due to continuous storage of static data for an extended period of time. It is for these reasons that TOP SECRET volatile media MUST always remain at this classification, even after sanitisation.

13.4.12.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4184]

Following sanitisation, volatile media MUST be treated as indicated in the table below.

Pre-sanitisation classification / Endorsement	Post-sanitisation classification / Endorsement
New Zealand Eyes Only (NZEO) Endorsement	NZEO
TOP SECRET	TOP SECRET
SECRET	SECRET
CONFIDENTIAL	UNCLASSIFIED
RESTRICTED and all lower classifications	UNCLASSIFIED

Non-volatile magnetic media sanitisation

13.4.13.R.01. **Rationale**

The following guidance applies in cases where media is to be redeployed.

Both the host protected area and device configuration overlay table of non-volatile magnetic hard disks are normally not visible to the operating system or the computer's BIOS. Hence any sanitisation of the readable sectors on the media will not overwrite these hidden sectors leaving any classified information contained in these locations untouched. Some sanitisation programs include the ability to reset devices to their default state removing any host protected areas or device configuration overlays. This allows the sanitisation program to see the entire contents of the media during the subsequent sanitisation process.

13.4.13.R.02. **Rationale**

Modern non-volatile magnetic hard disks automatically reallocate space for bad sectors at a hardware level. These bad sectors are maintained in what is known as the growth defects table or 'g-list'. If classified information was stored in a sector that is subsequently added to the g-list, sanitising the media will not overwrite these non-addressable bad sectors, and remnant data will exist in these locations. Whilst these sectors may be considered bad by the device quite often this is due to the sectors no longer meeting expected performance norms for the device and not due to an inability to read/write to the sector.

13.4.13.R.03. **Rationale**

The ATA secure erase command is built into the firmware of post-2001 devices and is able to access sectors that have been added to the g-list. Modern non-volatile magnetic hard disks also contain a primary defects table or 'p-list'. The p-list contains a list of bad sectors found during post-production processes. No information is ever stored in sectors on the p-list for a device as they are inaccessible before the media is used for the first time.

13.4.13.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4189]

Agencies MUST sanitise non-volatile magnetic media by:

- if pre-2001 or under 15GB: overwriting the media at least three times in its entirety with an arbitrary pattern followed by a read back for verification; or
- if post-2001 or over 15GB: overwriting the media at least once in its entirety with an arbitrary pattern followed by a read back for verification.

13.4.13.C.02. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4190]

Agencies MUST boot from separate media to the media being sanitised when undertaking sanitisation.

13.4.13.C.03. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:4191]

Agencies SHOULD reset the host protected area and drive configuration overlay table of non-volatile magnetic hard disks prior to overwriting the

media.

13.4.13.C.04. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:4192]

Agencies SHOULD attempt to overwrite the growth defects table (g-list) on non-volatile magnetic hard disks.

13.4.13.C.05. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:4193]

Agencies SHOULD use the ATA security erase command for sanitising non-volatile magnetic hard disks instead of using block overwriting software.

Treatment of non-volatile magnetic media following sanitisation

13.4.14.R.01. **Rationale**

The following guidance applies in cases where media is to be redeployed.

Highly classified non-volatile magnetic media cannot be sanitised below its original classification because of concerns with the sanitisation of the host protected area, device configuration overlay table and growth defects table.

13.4.14.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4200]

Following sanitisation, non-volatile magnetic media MUST be treated as indicated in the table below.

Pre-sanitisation classification	Post-sanitisation classification
New Zealand Eyes Only (NZEO) Endorsement	NZEO
TOP SECRET	TOP SECRET
SECRET	SECRET
CONFIDENTIAL	UNCLASSIFIED
RESTRICTED	UNCLASSIFIED

Non-volatile EPROM media sanitisation

13.4.15.R.01. **Rationale**

The following guidance applies in cases where media is to be redeployed.

When erasing non-volatile EPROM, the manufacturer's specified ultraviolet erasure time is multiplied by a factor of three to provide an additional level of certainty in the process. Verification is provided by read-back.

13.4.15.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4205]

Agencies MUST sanitise non-volatile EPROM media by erasing as per the manufacturer's specification, increasing the specified ultraviolet erasure time by a factor of three, then overwriting the media at least once in its entirety with a pseudo random pattern, followed by a read back for verification.

Non-volatile EEPROM media sanitisation

13.4.16.R.01. **Rationale**

The following guidance applies in cases where media is to be redeployed.

A single overwrite with a pseudo random pattern is considered good practice for sanitising non-volatile EEPROM media.

13.4.16.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4208]

Agencies MUST sanitise non-volatile EEPROM media by overwriting the media at least once in its entirety with a pseudo random pattern, followed by a read back for verification.

Treatment of non-volatile EPROM and EEPROM media following sanitisation

13.4.17.R.01. **Rationale**

The following guidance applies in cases where media is to be redeployed.

As little research has been conducted on the ability to recover data on non-volatile EPROM or EEPROM media after sanitisation, highly classified

media retains its original classification.

13.4.17.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4212]

Following sanitisation, non-volatile EPROM and EEPROM media MUST be treated as indicated in the table below.

Pre-sanitisation classification	Post-sanitisation classification
New Zealand Eyes Only (NZEO) Endorsement	NZEO
TOP SECRET	TOP SECRET
SECRET	SECRET
CONFIDENTIAL	UNCLASSIFIED
RESTRICTED	UNCLASSIFIED

Non-volatile flash memory & FPGA media sanitisation

13.4.18.R.01. **Rationale**

The following guidance applies in cases where media is to be redeployed.

Wear levelling ensures that writes are distributed evenly across each memory block in flash memory. Where possible flash memory SHOULD be overwritten with a pseudo random pattern twice, rather than once, as this helps to ensure that all memory blocks are overwritten during sanitisation. Verification is provided by read-back.

13.4.18.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4215]

Agencies MUST sanitise non-volatile flash memory media by overwriting the media at least twice in its entirety with a pseudo random pattern, followed by a read back for verification.

Treatment of non-volatile flash memory & FPCA media following sanitisation

13.4.19.R.01. **Rationale**

The following guidance applies in cases where media is to be redeployed.

Owing to the use of wear levelling in flash memory, it is possible that not all physical memory locations are written to when attempting to overwrite the media. Classified information can therefore remain on the media. It is for these reasons that TOP SECRET, SECRET and CONFIDENTIAL flash memory media MUST always remain at their respective classification, even after sanitisation.

13.4.19.R.02. **Rationale**

Non-volatile flash memory may be redeployed within systems of the same classification only after **all** manufacturer's sanitation procedures have been followed. Destruction and Disposal are covered in sections 13.5 - Media and IT equipment destruction and 13.6 - Media and IT equipment Disposal respectively.

13.4.19.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4218]

Following sanitisation, non-volatile flash memory media MUST be treated as indicated in the table below.

Pre-sanitisation classification	Post-sanitisation classification
New Zealand Eyes Only (NZEO) Endorsement	NZEO
TOP SECRET	TOP SECRET
SECRET	SECRET
CONFIDENTIAL	CONFIDENTIAL
RESTRICTED	UNCLASSIFIED

13.4.19.C.02. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:5426]

Where manufacturer sanitation procedures cannot be determined, items MUST be destroyed.

Sanitising solid state drives

13.4.20.R.01. **Rationale**

Solid state drives operate a Flash Translation Layer (FTL) to interface with the storage devices – usually NAND chips. Current sanitation techniques address the FTL, rather than destroying the underlying data. It is possible to bypass the FTL, thus accessing the underlying data. With current technology, there is no effective means of sanitising solid state drives.

13.4.20.R.02. **Rationale**

Solid state drives also use wear equalisation or levelling techniques which can leave data remnants.

13.4.20.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4222]

Solid state drives MUST be destroyed before disposal.

13.4.20.C.02. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4223]

Solid state drives MUST be sanitised using ATA Secure Erase sanitation software before redeployment.

13.4.20.C.03. **Control System Classifications(s): Secret, Confidential, Top Secret; Compliance: Must Not** [CID:4224]

Solid state drives MUST NOT be redeployed in a lower classification environment.

Hybrid Drives

13.4.21.R.01. **Rationale**

Hybrid drives combine solid state memory devices with magnetic disk technologies. As such they are subject to the same difficulties in effective sanitisation as solid state devices.

13.4.21.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4227]

Hybrid drives MUST be treated as solid state drives for sanitisation purposes.

Sanitising media and IT Equipment prior to reuse

13.4.22.R.01. **Rationale**

Sanitising media and IT Equipment prior to reuse at the same or higher classification assists with enforcing the need-to-know principle within the agency. This includes any material with an NZEO endorsement.

13.4.22.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:4230]

Agencies SHOULD sanitise all media and IT Equipment prior to reuse at the same or higher classification.

Verifying sanitised media and IT Equipment

13.4.23.R.01. **Rationale**

Verifying the sanitisation of media and IT Equipment with a different product to the one conducting the sanitisation process provides an independent level of assurance that the sanitisation process was conducted correctly.

13.4.23.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:4234]

Agencies SHOULD verify the sanitisation of media and IT Equipment using a different product from the one used to perform the initial sanitisation.