



# Australian Government Information Security Manual

JUNE 2021

## Guidelines for Media

### Media usage

#### Media management policy

Since media is capable of storing sensitive or classified data, it is important that a media management policy is developed and implemented to ensure that all types of media, and the data it stores, is protected in an appropriate manner. In many cases, an organisation's media management policy will be closely tied to their removable media usage policy.

**Security Control: 1549; Revision: 0; Updated: Aug-19; Applicability: O, P, S, TS**

*A media management policy is developed and implemented.*

#### Removable media usage policy

Establishing a removable media usage policy can decrease the likelihood and consequence of accidental data spills and data loss or theft. In doing so, a removable media usage policy will likely cover the following:

- permitted uses of removable media
- permitted types of removable media
- requirements for removable media registration
- requirements for removable media labelling
- requirements for the protection of removable media
- requirements for the reporting of lost or stolen removable media
- requirements for the sanitisation or destruction of removable media at the end of its life.

**Security Control: 1359; Revision: 3; Updated: Aug-19; Applicability: O, P, S, TS**

*A removable media usage policy is developed and implemented.*

#### Classifying media

Media that is not correctly classified could be stored and handled inappropriately or accessed by personnel who do not have appropriate security clearances.

**Security Control: 0323; Revision: 7; Updated: Jun-21; Applicability: O, P, S, TS**

*Media is classified to the highest sensitivity or classification of data stored on the media, unless the media has been classified to a higher sensitivity or classification.*

## Reclassifying media

Some activities will necessitate a change to the sensitivity or classification of media. For example, when rewritable media is connected to a system with a higher sensitivity or classification than the media and the system lacks a mechanism through which read-only access can be ensured, when rewritable media is sanitised, or when data stored on media is subject to a sensitivity or classification change.

**Security Control: 0325; Revision: 6; Updated: Apr-21; Applicability: O, P, S, TS**

*Any media connected to a system with a higher sensitivity or classification than the media is reclassified to the higher sensitivity or classification, unless the media is read-only or the system has a mechanism through which read-only access can be ensured.*

**Security Control: 0330; Revision: 5; Updated: Jun-21; Applicability: O, P, S, TS**

*In order to reclassify media to a lower sensitivity or classification, the media is sanitised (unless the media is read-only) and a formal administrative decision (in consultation with data owners) is made to reclassify the media.*

## Handling media

As media can be easily misplaced or stolen, measures should be put in place to protect data stored on it. Furthermore, applying encryption to media may reduce the requirements for storage and handling. Any reduction in requirements needs to be based on the original sensitivity or classification of the media and the level of assurance in the encryption software being used to encrypt the media.

**Security Control: 0831; Revision: 5; Updated: Sep-18; Applicability: O, P, S, TS**

*Media is handled in a manner suitable for its sensitivity or classification.*

**Security Control: 1059; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS**

*Media is encrypted with at least an Australian Signals Directorate Approved Cryptographic Algorithm.*

## Labelling media

Labelling media helps personnel to identify its sensitivity or classification and ensure that appropriate measures are applied to its storage, handling and usage.

While text-based protective markings are typically used for labelling media, there may be circumstances where colour-based protective markings or other marking schemes need to be used instead. In such cases, the marking scheme will need to be documented and personnel will need to be trained in its use.

**Security Control: 0332; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS**

*Media, with the exception of internally mounted fixed media within ICT equipment, is labelled with protective markings reflecting its sensitivity or classification.*

## Connecting media to systems

Some operating systems provide functionality to automatically execute software that resides on media. While this functionality was designed with a legitimate purpose in mind (e.g. automatically loading a graphical user interface to browse the contents of the media or to install software) it can also be used for malicious purposes. For example, an adversary can create a file on media that the operating system believes it should automatically execute. When the operating system executes the file, it can have the same effect as when a user explicitly executes malicious code; however, in this case the user is taken out of the equation as the operating system executes the file without explicitly asking for permission.

Device access control software allows control over media that can be connected to systems and how operating systems interact with it. For example, it can prevent data from being read from media, software being executed from media and/or data being written to media. Disabling connection ports in software can also assist in preventing operating systems from interacting with media.

Media can be prevented from connecting to systems by physical means such as using wafer seals or applying epoxy. If physical means are used to prevent media connecting to systems, processes and procedures covering detection and reporting are needed in order to respond to attempts to bypass these measures.

**Security Control: 1600; Revision: 1; Updated: Apr-21; Applicability: O, P, S, TS**

*Media is sanitised before it is used for the first time.*

**Security Control: 1642; Revision: 0; Updated: Apr-21; Applicability: O, P, S, TS**

*Media is sanitised before it is reused in a different security domain.*

**Security Control: 0337; Revision: 5; Updated: Apr-21; Applicability: O, P, S, TS**

*Media is only used with systems that are authorised to process, store or communicate the sensitivity or classification of the media.*

**Security Control: 0341; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS**

*Any automatic execution features for media are disabled in the operating system of systems.*

**Security Control: 0342; Revision: 5; Updated: Sep-18; Applicability: O, P, S, TS**

*Unauthorised media is prevented from connecting to systems via the use of device access control software, disabling connection ports or by physical means.*

**Security Control: 0343; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS**

*Media is prevented from being written to via the use of device access control software if there is no business requirement for its use.*

## Using media for data transfers

Organisations transferring data between systems belonging to different security domains are strongly encouraged to use write-once media. When done properly (e.g. using non-rewritable compact discs that have been finalised) this will ensure that data from the destination system cannot be accidentally transferred, or maliciously exfiltrated, onto the media used for the data transfer and then onto another system, such as the original source system. Alternatively, if suitable write-once media is not used, the destination system should have a mechanism through which read-only access can be ensured (e.g. via a read-only device or hardware write-blocker). However, the use of read-only mechanisms is not immune to failure or compromise, therefore, rewritable media should still be sanitised following each data transfer.

It is important to note that for PROTECTED and below non-volatile flash memory media it will be possible to sanitise and reclassify the media after a data transfer to allow it to be connected to lower classified systems again. This is not possible for SECRET and above non-volatile flash memory media as the media cannot be reclassified to a lower classification following sanitisation.

**Security Control: 0347; Revision: 5; Updated: Apr-21; Applicability: O, P, S, TS**

*When transferring data manually between two systems belonging to different security domains, write-once media is used unless the destination system has a mechanism through which read-only access can be ensured.*

**Security Control: 0947; Revision: 6; Updated: Apr-21; Applicability: O, P, S, TS**

*When transferring data manually between two systems belonging to different security domains, rewritable media is sanitised after each data transfer.*

## Further information

Further information on accounting for and storing media can be found in the ICT equipment and media section of the ***Guidelines for Physical Security***.

Further information on labelling ICT equipment can be found in the ICT equipment usage section of the ***Guidelines for ICT Equipment***.

Further information on reducing storage and physical transfer requirements can be found in the cryptographic fundamentals section of the ***Guidelines for Cryptography***.

Further information on using media to transfer data between systems can be found in the ***Guidelines for Data Transfers***.

Further information on the use of protective markings can be found in the Attorney-General's Department (AGD)'s ***Protective Security Policy Framework (PSPF), Sensitive and classified information*** policy, at <https://www.protectivesecurity.gov.au/information/sensitive-classified-information/Pages/default.aspx>.

Further information on the storage and transfer of media can be found in AGD's PSPF, ***Physical security for entity resources*** policy, at <https://www.protectivesecurity.gov.au/physical/physical-security-entity-resources/Pages/default.aspx>.

## Media sanitisation

### Media in ICT equipment

ICT equipment will often contain devices that are quite small and may not be immediately recognisable as memory. Examples of these include M.2 or Mini-Serial Advanced Technology Attachment (mSATA) devices. When sanitising M.2 or mSATA devices, the method for non-volatile flash memory media sanitisation applies. Generally, if a device offers persistent storage of data, it is likely that the method for non-volatile flash memory media sanitisation will apply.

### Hybrid hard drives

When sanitising hybrid hard drives, separate the non-volatile magnetic media from the circuit board containing non-volatile flash memory media and sanitise each separately.

### Solid state drives

When sanitising solid state drives, the method for sanitising non-volatile flash memory media applies.

### Media that cannot be sanitised

When attempts to sanitise media are unsuccessful, the only way to provide assurance that all data has been erased is to destroy the media. Additionally, some types of media cannot be sanitised and therefore should be destroyed.

### Media sanitisation process and procedures

Sanitising media prior to reuse in a different environment ensures that data is not inadvertently accessed by unauthorised personnel or otherwise insufficiently protected.

Using approved methods provides a level of assurance that no data will be left on media. The methods described in these guidelines are designed not only to prevent common data recovery practices but also to protect from those that could emerge in the future.

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

**Security Control: 0348; Revision: 3; Updated: Aug-19; Applicability: O, P, S, TS**

*A media sanitisation process, and supporting media sanitisation procedures, is developed and implemented.*

## **Volatile media sanitisation**

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

If read back cannot be achieved following the overwriting of media contents, or data persists on the media, destroying the media is the only way to provide complete assurance data no longer persists.

**Security Control: 0351; Revision: 5; Updated: Sep-18; Applicability: O, P**

*Volatile media is sanitised by removing power from the media for at least 10 minutes or by overwriting all locations on the media with a random pattern followed by a read back for verification.*

**Security Control: 0352; Revision: 3; Updated: Sep-18; Applicability: S, TS**

*Volatile media is sanitised by overwriting the media at least once in its entirety with a random pattern, followed by a read back for verification, and then followed by removing power from the media for at least 10 minutes.*

## **Treatment of volatile media following sanitisation**

Published literature suggests that short-term remanence effects are likely in volatile media. Data retention times have been reported to be measured in minutes at normal room temperatures and up to hours in extreme cold. Furthermore, some volatile media can suffer from long-term 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 under certain circumstances TOP SECRET volatile media retains its classification following sanitisation.

Typical circumstances preventing the reclassification of TOP SECRET volatile media include a static cryptographic key being stored in the same memory location during every boot of a device and a static image being displayed on a device and stored in volatile media for a period of months.

**Security Control: 0835; Revision: 3; Updated: Sep-18; Applicability: TS**

*Following sanitisation, highly classified volatile media retains its classification if it stored static data for an extended period of time, or had data repeatedly stored on or written to the same memory location for an extended period of time.*

## **Non-volatile magnetic media sanitisation**

Both the host-protected area and device configuration overlay table of non-volatile magnetic media are normally not visible to an operating system or a computer's basic input/output system. Therefore, any sanitisation of the readable sectors of media will not overwrite these hidden sectors leaving any data contained in these locations untouched. Some sanitisation programs include the ability to reset media to their default state removing any host-protected areas or device configuration overlays. This allows the sanitisation program to see the entire contents of media during the subsequent sanitisation process.

Modern non-volatile magnetic media automatically reallocates 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 data was stored in a sector that was subsequently added to the g-list, sanitising the media will not overwrite these non-addressable bad sectors. While these sectors may be considered bad by the media, quite often this is due to the sectors no longer meeting expected performance norms and not due to an inability to read/write to them. The Advanced Technology Attachment (ATA) secure erase command was built into the firmware of post-2001 media and is able to access sectors that have been added to the g-list.

Modern non-volatile magnetic media also contain a primary defects table or 'p-list'. The p-list contains a list of bad sectors found during post-production processes. No data is ever stored in sectors on the p-list as they are inaccessible before the media is used for the first time.

**Security Control: 1065; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS**

*The host-protected area and device configuration overlay table of non-volatile magnetic media is reset prior to sanitisation.*

**Security Control: 0354; Revision: 5; Updated: Sep-18; Applicability: O, P, S, TS**

*Non-volatile magnetic media is sanitised by booting from separate media to the media being sanitised and then overwriting the media at least once (or three times if pre-2001 or under 15 Gigabytes) in its entirety with a random pattern followed by a read back for verification.*

**Security Control: 1067; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS**

*The ATA secure erase command is used where available, in addition to using block overwriting software, to ensure the growth defects table (g-list) is overwritten.*

## **Treatment of non-volatile magnetic media following sanitisation**

Due to concerns with the sanitisation of the host-protected area, device configuration overlay table and growth defects table, highly classified non-volatile magnetic media retains its classification following sanitisation.

**Security Control: 0356; Revision: 5; Updated: Sep-18; Applicability: S, TS**

*Following sanitisation, highly classified non-volatile magnetic media retains its classification.*

## **Non-volatile erasable programmable read-only memory media sanitisation**

When sanitising non-volatile erasable programmable read-only memory (EPROM), the manufacturer's specification for ultraviolet erasure time should be multiplied by a factor of three to provide an additional level of certainty in the process.

**Security Control: 0357; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS**

*Non-volatile EPROM media is sanitised by erasing the media in accordance with 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 random pattern followed by a read back for verification.*

## **Non-volatile electrically erasable programmable read-only memory media sanitisation**

A single overwrite with a random pattern is considered best practice for sanitising non-volatile electrically erasable programmable read-only memory (EEPROM) media.

**Security Control: 0836; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS**

*Non-volatile EEPROM media is sanitised by overwriting the media at least once in its entirety with a random pattern followed by a read back for verification.*

## **Treatment of non-volatile erasable and electrically erasable programmable read-only memory media following sanitisation**

As little research has been conducted into the ability to recover data from non-volatile EPROM and EEPROM media following sanitisation, highly classified EPROM and EEPROM media retains its classification following sanitisation.

**Security Control: 0358; Revision: 5; Updated: Sep-18; Applicability: S, TS**

*Following sanitisation, highly classified non-volatile EPROM and EEPROM media retains its classification.*

## **Non-volatile flash memory media sanitisation**

In non-volatile flash memory media, a technique known as wear levelling ensures that writes are distributed evenly across each memory block. This feature necessitates non-volatile flash memory media being overwritten with a random pattern twice as this helps ensure that all memory blocks are overwritten.



**Security Control: 0359; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS**

*Non-volatile flash memory media is sanitised by overwriting the media at least twice in its entirety with a random pattern followed by a read back for verification.*

## **Treatment of non-volatile flash memory media following sanitisation**

Due to the use of wear levelling in non-volatile flash memory media, and potentially bad memory blocks, it is possible that not all memory blocks were written to when attempting to overwrite the non-volatile flash memory media. For this reason, highly classified non-volatile flash memory media retains its classification following sanitisation.

**Security Control: 0360; Revision: 5; Updated: Sep-18; Applicability: S, TS**

*Following sanitisation, highly classified non-volatile flash memory media retains its classification.*

## **Encrypted media sanitisation**

When applied appropriately, the use of encryption can provide additional assurance during media sanitisation, reuse and disposal. However, unless otherwise stated in consumer guides for evaluated encryption software, the use of encryption does not reduce the post-sanitisation classification of media.

**Security Control: 1464; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS**

*Where a consumer guide for evaluated encryption software exists, the sanitisation and post-sanitisation requirements stated in the consumer guide are followed.*

## **Further information**

Further information on sanitising ICT equipment can be found in the ICT equipment sanitisation and disposal section of the **Guidelines for ICT Equipment**.

Further information on recoverability of data from volatile media can be found in the paper **Data Remanence in Semiconductor Devices** at [https://www.usenix.org/legacy/events/sec01/full\\_papers/gutmann/gutmann.pdf](https://www.usenix.org/legacy/events/sec01/full_papers/gutmann/gutmann.pdf).

Further information on the random-access memory (RAM) testing tool MemTest86 can be obtained from <https://www.memtest86.com/>.

Further information on the graphics card RAM testing tool MemtestG80 and MemtestCL can be obtained from <https://simtk.org/projects/memtest>.

Further information on HDDerase, a freeware tool developed by the Center for Memory and Recording Research at the University of California San Diego, can be obtained from <https://cmrr.ucsd.edu/resources/secure-erase.html>. HDDerase is capable of calling the ATA secure erase command as well as resetting the host-protected area and device configuration overlay table on non-volatile magnetic media.

Further information on reliably erasing data from solid state drives can be found in the paper **Reliably Erasing Data From Flash-Based Solid State Drives** at [https://www.usenix.org/legacy/event/fast11/tech/full\\_papers/Wei.pdf](https://www.usenix.org/legacy/event/fast11/tech/full_papers/Wei.pdf).

## **Media destruction**

### **Media destruction process and procedures**

Documenting a process and supporting procedures for media destruction will ensure that organisations carry out media destruction in an appropriate and consistent manner.

**Security Control: 0363; Revision: 2; Updated: Aug-19; Applicability: O, P, S, TS**

*A media destruction process, and supporting media destruction procedures, is developed and implemented.*

## Media that cannot be sanitised

It is not possible to sanitise some types of media while maintaining a level of assurance that no data can be recovered.

**Security Control: 0350; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS**

*The following media types are destroyed prior to disposal as they cannot be sanitised:*

- microfiche and microfilm
- optical discs
- programmable read-only memory
- read-only memory
- other types of media that cannot be sanitised
- faulty media that cannot be successfully sanitised.

## Media destruction equipment

When physically destroying media, using approved equipment can provide a level of assurance that that data residing on the media is actually destroyed.

Approved equipment includes destruction equipment listed in the Security Construction and Equipment Committee (SCEC)'s **Security Equipment Evaluated Products List**, the Australian Security Intelligence Organisation (ASIO)'s Security Equipment Guide (SEG)-009, **Optical Media Shredders**, and ASIO's SEG-018, **Destructors**. ASIO's SEG-009 and SEG-018 are available from the Protective Security Policy GovTEAMS community or ASIO by email.

If using degaussers to destroy media, the United States' National Security Agency maintains an **Evaluated Products List for Magnetic Degaussers**.

**Security Control: 1361; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS**

*SCEC or ASIO approved equipment is used when destroying media.*

**Security Control: 1160; Revision: 2; Updated: Aug-20; Applicability: O, P, S, TS**

*If using degaussers to destroy media, degaussers evaluated by the United States' National Security Agency are used.*

## Media destruction methods

The destruction methods given below are designed to ensure that recovery of data is impossible or impractical.

**Security Control: 1517; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS**

*Equipment that is capable of reducing microform to a fine powder, with resultant particles not showing more than five consecutive characters per particle upon microscopic inspection, is used to destroy microfiche and microfilm.*

**Security Control: 0366; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS**

*One of the methods in the following table is used to destroy media.*

Item	Destruction Methods					
	Furnace/ Incinerator	Hammer Mill	Disintegrator	Grinder/ Sander	Cutting	Degausser
Electrostatic memory devices	Yes	Yes	Yes	Yes	No	No



<i>Magnetic floppy disks</i>	<i>Yes</i>	<i>Yes</i>	<i>Yes</i>	<i>No</i>	<i>Yes</i>	<i>Yes</i>
<i>Magnetic hard disks</i>	<i>Yes</i>	<i>Yes</i>	<i>Yes</i>	<i>Yes</i>	<i>No</i>	<i>Yes</i>
<i>Magnetic tapes</i>	<i>Yes</i>	<i>Yes</i>	<i>Yes</i>	<i>No</i>	<i>Yes</i>	<i>Yes</i>
<i>Optical disks</i>	<i>Yes</i>	<i>Yes</i>	<i>Yes</i>	<i>Yes</i>	<i>Yes</i>	<i>No</i>
<i>Semiconductor memory</i>	<i>Yes</i>	<i>Yes</i>	<i>Yes</i>	<i>No</i>	<i>No</i>	<i>No</i>

## Treatment of media waste particles

Following destruction, normal accounting and auditing procedures for media do not apply. However, depending on the destruction method used and the resulting particle size, it may still need to be stored and handled as classified waste.

**Security Control: 0368; Revision: 6; Updated: Sep-18; Applicability: O, P, S, TS**

*The resulting waste for all destruction methods, except for furnace/incinerator and degausser, is stored and handled as per the following table.*

<i>Initial Media Handling</i>	<i>Screen Aperture Size Particles Can Pass Through</i>		
	<i>Less Than or Equal to 3 mm</i>	<i>Less Than or Equal to 6 mm</i>	<i>Less Than or Equal to 9 mm</i>
<i>TOP SECRET</i>	<i>OFFICIAL</i>	<i>SECRET</i>	<i>SECRET</i>
<i>SECRET</i>	<i>OFFICIAL</i>	<i>PROTECTED</i>	<i>SECRET</i>
<i>PROTECTED</i>	<i>OFFICIAL</i>	<i>OFFICIAL</i>	<i>OFFICIAL</i>
<i>OFFICIAL: Sensitive</i>	<i>OFFICIAL</i>	<i>OFFICIAL</i>	<i>OFFICIAL</i>
<i>OFFICIAL</i>	<i>OFFICIAL</i>	<i>OFFICIAL</i>	<i>OFFICIAL</i>

## Degaussing magnetic media

Degaussing magnetic media changes the alignment of magnetic domains resulting in data being permanently corrupted.

Coercivity (the resistance of magnetic material to change) varies between magnetic media types and between brands and models of the same type of media. Care is needed when degaussing magnetic media since a degausser of insufficient strength will not be effective. The United States' National Security Agency provides further information on the common types of magnetic media and their associated coercivity ratings within their list of evaluated degaussers.

Since 2006, perpendicular magnetic media has been available. As some degaussers are only capable of sanitising longitudinal magnetic media, care needs to be taken to ensure that a suitable degausser is used.

Finally, to ensure that degaussers are being used in the correct manner to achieve an effective destruction outcome, product-specific directions provided by degausser manufacturers should be followed.

**Security Control: 0361; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS**

*A degausser of sufficient field strength for the coercivity of the magnetic media is used, with the field strength being checked at regular intervals.*

**Security Control: 0838; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS**

*A degausser capable of the magnetic orientation (longitudinal or perpendicular) of the magnetic media is used.*

**Security Control: 0362; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS**

*Any product-specific directions provided by degausser manufacturers are followed.*

**Security Control: 1641; Revision: 0; Updated: Mar-21; Applicability: O, P, S, TS**

*Following destruction of magnetic media using a degausser, the magnetic media is physically damaged by deforming the internal platters by any means prior to disposal.*

## Supervision of destruction

To verify that media is appropriately destroyed, the process needs to be supervised by at least one person cleared to the sensitivity or classification of the media being destroyed.

**Security Control: 0370; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS**

*The destruction of media is performed under the supervision of at least one person cleared to the sensitivity or classification of the media being destroyed.*

**Security Control: 0371; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS**

*Personnel supervising the destruction of media supervise the handling of the media to the point of destruction and ensure that the destruction is completed successfully.*

## Supervision of accountable material destruction

Accountable material is more important than standard media. As such, its destruction should be supervised by at least two personnel who sign a destruction certificate afterwards.

**Security Control: 0372; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS**

*The destruction of accountable material is performed under the supervision of at least two personnel cleared to the sensitivity or classification of the media being destroyed.*

**Security Control: 0373; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS**

*Personnel supervising the destruction of accountable media supervise the handling of the material to the point of destruction, ensure that the destruction is completed successfully and sign a destruction certificate afterwards.*

## Outsourcing media destruction

ASIO has approved National Association for Information Destruction AAA certified destruction services with endorsements, as specified in ASIO's Protective Security Circular (PSC)-167, **External destruction of security classified information**, for the outsourced destruction of media. ASIO's PSC-167 is available from the Protective Security Policy GovTEAMS community or ASIO by email.

**Security Control: 0840; Revision: 3; Updated: Sep-18; Applicability: O, P, S**

*When outsourcing the destruction of media to an external destruction service, a National Association for Information Destruction AAA certified destruction service with endorsements, as specified in ASIO's PSC-167, is used.*

**Security Control: 0839; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS**

*The destruction of TOP SECRET media or accountable material is not outsourced.*

## Further information

Further information on the destruction of ICT equipment can be found in the ICT equipment sanitisation and disposal section of the ***Guidelines for ICT Equipment***.

Further information on the United States' National Security Agency's ***Evaluated Products List for Magnetic Degaussers*** is available at <https://www.nsa.gov/Resources/Media-Destruction-Guidance/>.

Further information on the SCEC's ***Security Equipment Evaluated Products List*** is available at <https://www.scec.gov.au/catalogue>.

## Media disposal

### Media disposal process and procedures

Before media, or its waste, can be released into the public domain it needs to be sanitised, destroyed or declassified. As the compromise of official data still presents a security risk, albeit minor, an appropriate authority needs to formally authorise its release into the public domain.

In addition, removing labels and markings indicating the classification, codewords, caveats, owner, system or network details will ensure media does not display indications of its prior use and draw undue attention following its disposal.

***Security Control: 0374; Revision: 2; Updated: Aug-19; Applicability: O, P, S, TS***

*A media disposal process, and supporting media disposal procedures, is developed and implemented.*

***Security Control: 0375; Revision: 5; Updated: Jun-21; Applicability: O, P, S, TS***

*Following sanitisation, destruction or declassification, a formal administrative decision (in consultation with data owners) is made to handle media, or its waste, as 'publicly releasable' before it is released into the public domain.*

***Security Control: 0378; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS***

*Labels and markings indicating the classification, codewords, caveats, owner, system, network, or any other marking that can associate media with its original use, are removed prior to disposal.*

## Further information

Further information on the disposal of ICT equipment can be found in the ICT equipment sanitisation and disposal section of the ***Guidelines for ICT Equipment***.