Information security manual

Last updated: March 2025

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, implemented and maintained 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.

Control: ISM-1549; Revision: 1; Updated: Dec-22; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
A media management policy is developed, implemented and maintained.

Removable media usage policy

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

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

Control: ISM-1359; Revision: 4; Updated: Dec-22; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
A removable media usage policy is developed, implemented and maintained.

Removable media register

Developing, implementing, maintaining and regularly verifying a register of removable media can assist an organisation in tracking and accounting for authorised removable media as well as identifying any non-authorised removal media in use within their organisation.

Control: ISM-1713; Revision: 2; Updated: Dec-22; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
A removable media register is developed, implemented, maintained and verified on a regular basis.

Labelling media

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

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.

Control: ISM-0332; Revision: 5; Updated: Jun-24; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
Media, with the exception of internally mounted fixed media within information technology equipment, is labelled with protective markings reflecting its sensitivity or classification.

Classifying media

Media that is not correctly classified could be stored and handled inappropriately, accessed by personnel who do not have an appropriate security clearance or used with systems it is not authorised to be used with.

Control: ISM-0323; Revision: 8; Updated: Dec-21; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
Media is classified to the highest sensitivity or classification of data it stores, unless the media has been classified to a higher sensitivity or classification.

Control: ISM-0337; Revision: 6; Updated: Dec-21; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
Media is only used with systems that are authorised to process, store or communicate its sensitivity or classification.

Reclassifying media

Some activities may necessitate or allow for a change to the sensitivity or classification of media. For example, when media is connected to a system that lacks a mechanism through which read-only access can be ensured, when media is sanitised or destroyed, or when data stored on media is subject to a sensitivity or classification change.

Control: ISM-0325; Revision: 6; Updated: Apr-21; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
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.

Control: ISM-0330; Revision: 7; Updated: Mar-22; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
Before reclassifying media to a lower sensitivity or classification, the media is sanitised or destroyed, and a formal administrative decision is made to reclassify it.

Handling media

As media can be easily misplaced or stolen, measures should be put in place to protect data stored on it. In some cases, applying encryption to media may change the manner in which it needs to be handled. Any change in handling needs to be based on the original sensitivity or classification of the media and the level of assurance in the cryptographic equipment or software being used to encrypt it.

Control: ISM-0831; Revision: 5; Updated: Sep-18; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
Media is handled in a manner suitable for its sensitivity or classification.

Control: ISM-1059; Revision: 4; Updated: Dec-21; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
All data stored on media is encrypted.

Sanitising media before first use

Sanitising media before first use can assist in reducing cyber supply chain risks, such as new media containing malicious code. In addition, sanitising media before first use in a different security domain can prevent potential data spills from occurring.

Control: ISM-1600; Revision: 1; Updated: Apr-21; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
Media is sanitised before it is used for the first time.

Control: ISM-1642; Revision: 0; Updated: Apr-21; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
Media is sanitised before it is reused in a different security domain.

Using media for data transfers

An organisation transferring data between systems belonging to different security domains is strongly encouraged to use write-once media. When done properly, such as using non-rewritable compact discs that have been finalised, this will ensure that data from the destination system cannot be accidently 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, such as 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 most non-volatile flash memory media, it will be possible to sanitise and reclassify it following a data transfer in order to allow it to be connected to other systems again. This is not possible for SECRET and TOP SECRET non-volatile flash memory media as it cannot be reclassified following sanitisation.

Control: ISM-0347; Revision: 5; Updated: Apr-21; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
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.

Control: ISM-0947; Revision: 6; Updated: Apr-21; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
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 cyber supply chain risk management can be found in the cyber supply chain risk management section of the *Guidelines for procurement and outsourcing*.

Further information on the protection of media can be found in the Department of Home Affairs' *Protective Security Policy Framework*.

Further information on securing media when not in use can be found in the IT equipment and media section of the *Guidelines for physical security*.

Further information on encrypting media 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 data transfers section of the *Guidelines for data transfers*.

Media sanitisation

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 sanitisation processes and procedures

Using approved methods to sanitise media provides a level of assurance that, to the extent possible, no data will be left following sanitisation. 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.

Control: ISM-0348; Revision: 5; Updated: Dec-22; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
Media sanitisation processes, and supporting media sanitisation procedures, are developed, implemented and maintained.

Volatile media sanitisation

When sanitising volatile media, the specified time to wait following the removal of power is based on applying a safety factor to the time recommended by research into preventing the recovery of data. In addition to the removal of power, SECRET and TOP SECRET volatile media should be overwritten at least once in its entirety with a random pattern followed by a read back for verification.

Control: ISM-0351; Revision: 6; Updated: Dec-21; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
Volatile media is sanitised by removing its power for at least 10 minutes.

Control: ISM-0352; Revision: 4; Updated: Dec-21; Applicability: S, TS; Essential Eight: N/A
SECRET and TOP SECRET volatile media is sanitised by overwriting it at least once in its entirety with a random pattern followed by a read back for verification.

Treatment of volatile media following sanitisation

Research suggests that short-term remanence effects are likely in volatile media. For example, up to minutes at normal room temperatures and up to hours in extremely cold temperatures. Furthermore, some volatile media can suffer from long-term remanence effects resulting from physical changes due to the continuous storage of static data for extended periods 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, or a static image being displayed on a device and stored in volatile media for a period of months.

Control: ISM-0835; Revision: 4; Updated: Dec-21; Applicability: TS; Essential Eight: N/A
Following sanitisation, TOP SECRET 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

Non-volatile magnetic media encompasses non-volatile magnetic hard drives, magnetic tape and floppy disks. While non-volatile magnetic tape and floppy disks can be sanitised by overwriting them at least once (or three times if pre-2001 or under 15 GB) in their entirety with a random pattern followed by a read back for verification, additional considerations apply to non-volatile magnetic hard drives due to their use of a host-protected area, device configuration overlay table and growth defects table.

The host-protected area and device configuration overlay table of non-volatile magnetic hard drives are normally not visible to a computer's Unified Extensible Firmware Interface or operating system. Therefore, any sanitisation of the readable sectors of non-volatile magnetic hard drives will leave any data contained in sectors listed in the host-protected area and device configuration overlay table untouched. Some sanitisation programs include the ability to reset non-volatile magnetic hard drives to their default state, thereby removing any host-protected areas or device configuration overlays. This allows the sanitisation program to see the entire contents of non-volatile magnetic hard drives during subsequent sanitisation processes.

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

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

Control: ISM-0354; Revision: 6; Updated: Dec-21; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
Non-volatile magnetic media is sanitised by overwriting it at least once (or three times if pre-2001 or under 15 GB) in its entirety with a random pattern followed by a read back for verification.

Control: ISM-1065; Revision: 3; Updated: Dec-21; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
The host-protected area and device configuration overlay table are reset prior to the sanitisation of non-volatile magnetic hard drives.

Control: ISM-1067; Revision: 4; Updated: Dec-21; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
The ATA secure erase command is used, in addition to block overwriting software, to ensure the growth defects table of non-volatile magnetic hard drives is overwritten.

Treatment of non-volatile magnetic media following sanitisation

Due to concerns with the sanitisation processes for non-volatile magnetic media, SECRET and TOP SECRET non-volatile magnetic media retains its classification following sanitisation.

Control: ISM-0356; Revision: 6; Updated: Dec-21; Applicability: S, TS; Essential Eight: N/A
Following sanitisation, SECRET and TOP SECRET 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), three times the manufacturer's specification for ultraviolet erasure time should be applied to provide additional certainty in sanitisation processes.

Subsequently, the non-volatile EPROM media should be overwritten at least once in its entirety with a random pattern followed by a read back for verification.

Control: ISM-0357; Revision: 5; Updated: Dec-21; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
Non-volatile EPROM media is sanitised by applying three times the manufacturer's specified ultraviolet erasure time and then overwriting it 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, followed by a read back for verification, is considered suitable for sanitising non-volatile electrically erasable programmable read-only memory (EEPROM) media.

Control: ISM-0836; Revision: 3; Updated: Dec-21; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
Non-volatile EEPROM media is sanitised by overwriting it 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 recovery of data from non-volatile EPROM and EEPROM media, SECRET and TOP SECRET EPROM and EEPROM media retains its classification following sanitisation.

Control: ISM-0358; Revision: 6; Updated: Dec-21; Applicability: S, TS; Essential Eight: N/A
Following sanitisation, SECRET and TOP SECRET non-volatile EPROM and EEPROM media retains its classification.

Non-volatile flash memory media sanitisation

For 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 at least twice, and followed by a read back for verification, as this helps to ensure that all memory blocks are overwritten.

Control: ISM-0359; Revision: 4; Updated: Dec-21; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
Non-volatile flash memory media is sanitised by overwriting it 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 the potential for bad memory blocks, it is possible that not all memory blocks will be overwritten during sanitisation processes. For this reason, SECRET and TOP SECRET non-volatile flash memory media retains its classification following sanitisation.

Control: ISM-0360; Revision: 6; Updated: Dec-21; Applicability: S, TS; Essential Eight: N/A
Following sanitisation, SECRET and TOP SECRET non-volatile flash memory media retains its classification.

Media that cannot be successfully sanitised

In some cases, attempts to sanitise media, or verify the sanitisation of media, will be unsuccessful. For example, due to the media being faulty or damaged. In such cases, the media will need to be destroyed prior to its disposal.

Control: ISM-1735; Revision: 1; Updated: Sep-24; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
Media that cannot be successfully sanitised is destroyed prior to its disposal.

Further information

Further information on the random-access memory testing tool MemTest86 can be obtained from PassMark Software.

Further information on the graphics card random-access memory testing tools MemtestG80 and MemtestCL can be obtained from their GitHub projects.

Further information on HDDerase is available from the Center for Memory and Recording Research at the University of California San Diego. 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.

Media destruction

Media destruction processes and procedures

Developing, implementing and maintaining processes and procedures for media destruction will ensure that an organisation carries out media destruction in an appropriate and consistent manner.

Control: ISM-0363; Revision: 4; Updated: Dec-22; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
Media destruction processes, and supporting media destruction procedures, are developed, implemented and maintained.

Media that cannot be sanitised

Some media types are incapable of being sanitised. As such, they will need to be destroyed prior to their disposal.

Control: ISM-0350; Revision: 5; Updated: Dec-21; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
The following media types are destroyed prior to their disposal:

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

Media destruction equipment

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

Approved equipment includes destruction equipment listed on the Security Construction and Equipment Committee's *Security Equipment Evaluated Products List*, and in the Australian Security Intelligence Organisation's (ASIO) Security Equipment Guide-009, *Optical Media Shredders* and Security Equipment Guide-018, *Destructors*. ASIO's Security Equipment Guides 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 the *NSA/CSS Evaluated Products List for Magnetic Degaussers* and information on common types of magnetic media and their associated magnetic field strengths and orientations.

Control: ISM-1361; Revision: 3; Updated: Jun-22; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
Security Construction and Equipment Committee-approved equipment or ASIO-approved equipment is used when destroying media.

Control: ISM-1160; Revision: 2; Updated: Aug-20; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
If using degaussers to destroy media, degaussers evaluated by the United States' National Security Agency are used.

Media destruction methods

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

Control: ISM-1517; Revision: 0; Updated: Sep-18; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
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.

Control: ISM-1722; Revision: 1; Updated: Mar-22; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
Electrostatic memory devices are destroyed using a furnace/incinerator, hammer mill, disintegrator or grinder/sander.

Control: ISM-1723; Revision: 1; Updated: Mar-22; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
Magnetic floppy disks are destroyed using a furnace/incinerator, hammer mill, disintegrator, degausser or by cutting.

Control: ISM-1724; Revision: 1; Updated: Mar-22; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
Magnetic hard disks are destroyed using a furnace/incinerator, hammer mill, disintegrator, grinder/sander or degausser.

Control: ISM-1725; Revision: 1; Updated: Mar-22; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
Magnetic tapes are destroyed using a furnace/incinerator, hammer mill, disintegrator, degausser or by cutting.

Control: ISM-1726; Revision: 1; Updated: Mar-22; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
Optical disks are destroyed using a furnace/incinerator, hammer mill, disintegrator, grinder/sander or by cutting.

Control: ISM-1727; Revision: 1; Updated: Mar-22; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
Semiconductor memory is destroyed using a furnace/incinerator, hammer mill or disintegrator.

Control: ISM-0368; Revision: 8; Updated: Mar-22; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
Media destroyed using a hammer mill, disintegrator, grinder/sander or by cutting results in media waste particles no larger than 9 mm.

Treatment of media waste particles

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

Control: ISM-1728; Revision: 0; Updated: Dec-21; Applicability: S; Essential Eight: N/A
The resulting media waste particles from the destruction of SECRET media is stored and handled as OFFICIAL if less than or equal to 3 mm, PROTECTED if greater than 3 mm and less than or equal to 6 mm, or SECRET if greater than 6 mm and less than or equal to 9 mm.

Control: ISM-1729; Revision: 0; Updated: Dec-21; Applicability: TS; Essential Eight: N/A
The resulting media waste particles from the destruction of TOP SECRET media is stored and handled as OFFICIAL if less than or equal to 3 mm, or SECRET if greater than 3 mm and less than or equal to 9 mm.

Degaussing magnetic media

Degaussing magnetic media changes its magnetic properties, thereby, permanently corrupting data. When degaussing magnetic media, care needs to be taken as a degausser of insufficient magnetic field strength will not be effective. In addition, since 2006 perpendicular magnetic media has progressively replaced longitudinal magnetic media. As some older degaussers are only capable of destroying longitudinal magnetic media, care needs to be taken to ensure that a degausser with a suitable magnetic orientation is also used. Furthermore, to ensure that degaussers are being used in the correct manner to effectively destroy magnetic media, product-specific directions provided by degausser manufacturers should be followed. Finally, to provide an additional level of assurance following the use of a degausser, magnetic media should be physically damaged by deforming any internal platters.

Control: ISM-0361; Revision: 4; Updated: Dec-21; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
Magnetic media is destroyed using a degausser with a suitable magnetic field strength and magnetic orientation.

Control: ISM-0362; Revision: 4; Updated: Mar-22; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
Product-specific directions provided by degausser manufacturers are followed.

Control: ISM-1641; Revision: 2; Updated: Mar-22; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
Following the use of a degausser, magnetic media is physically damaged by deforming any internal platters.

Supervision of destruction

To verify that media is appropriately destroyed, destruction processes need to be supervised by at least one cleared person.

Control: ISM-0370; Revision: 6; Updated: Sep-23; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
The destruction of media is performed under the supervision of at least one cleared person.

Control: ISM-0371; Revision: 4; Updated: Dec-21; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
Personnel supervising the destruction of media supervise its handling to the point of destruction and ensure that the destruction is completed successfully.

Supervision of accountable material destruction

The successful destruction of media storing accountable material is more important than for other media. As such, its destruction should be supervised by at least two cleared personnel who sign a destruction certificate afterwards.

Control: ISM-0372; Revision: 6; Updated: Sep-23; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
The destruction of media storing accountable material is performed under the supervision of at least two cleared personnel.

Control: ISM-0373; Revision: 4; Updated: Dec-21; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
Personnel supervising the destruction of media storing accountable material supervise its handling to the point of destruction, ensure that the destruction is completed successfully and sign a destruction certificate afterwards.

Outsourcing media destruction

While media storing accountable material cannot be outsourced, media storing non-accountable material can be outsourced when using a National Association for Information Destruction AAA certified destruction service with

endorsements, as specified in ASIO's Protective Security Circular-167, *External destruction of security classified information*. This publication is available from the Protective Security Policy GovTEAMS community or ASIO by email.

Control: ISM-0839; Revision: 3; Updated: Dec-21; Applicability: OS, P, S, TS; Essential Eight: N/A
The destruction of media storing accountable material is not outsourced.

Control: ISM-0840; Revision: 4; Updated: Jun-22; Applicability: OS, P, S; Essential Eight: N/A
When outsourcing the destruction of media storing non-accountable material, a National Association for Information Destruction AAA certified destruction service with endorsements, as specified in ASIO's Protective Security Circular-167, is used.

Further information

Further information on cyber supply chain risk management can be found in the cyber supply chain risk management section of the *Guidelines for procurement and outsourcing*.

Media disposal

Media disposal processes and procedures

Developing, implementing and maintaining processes and procedures for media disposal will ensure that an organisation carries out media disposal in an appropriate and consistent manner.

Control: ISM-0374; Revision: 4; Updated: Dec-22; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
Media disposal processes, and supporting media disposal procedures, are developed, implemented and maintained.

Disposal of media

Before media can be released into the public domain, it needs to be sanitised, destroyed or declassified. As sanitised, destroyed or declassified media still presents a security risk, albeit very minor, an appropriate authority needs to formally authorise its release into the public domain. Furthermore, as part of disposal processes, removing labels and markings indicating the owner, sensitivity, classification or any other marking that can associate media with its prior use will ensure it does not draw undue attention following its disposal.

Control: ISM-0378; Revision: 4; Updated: Dec-21; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
Labels and markings indicating the owner, sensitivity, classification or any other marking that can associate media with its prior use are removed prior to its disposal.

Control: ISM-0375; Revision: 6; Updated: Dec-21; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
Following sanitisation, destruction or declassification, a formal administrative decision is made to release media, or its waste, into the public domain.

Disclaimer

The material in this guide is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances.

The Commonwealth accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.

Copyright

© Commonwealth of Australia 2025.

With the exception of the Coat of Arms, the Australian Signals Directorate logo and where otherwise stated, all material presented in this publication is provided under a Creative Commons Attribution 4.0 International licence (www.creativecommons.org/licenses).

For the avoidance of doubt, this means this licence only applies to material as set out in this document.

The details of the relevant licence conditions are available on the Creative Commons website as is the full legal code for the CC BY 4.0 licence (www.creativecommons.org/licenses).

Use of the Coat of Arms

The terms under which the Coat of Arms can be used are detailed on the Department of the Prime Minister and Cabinet website (www.pmc.gov.au/resources/commonwealth-coat-arms-information-and-guidelines).

For more information, or to report a cybersecurity incident, contact us:

cyber.gov.au | 1300 CYBER1 (1300 292 371)

Australian Government

Australian Signals Directorate