



Information Security Manual

Last updated: June 2024

Guidelines for Information Technology Equipment

IT equipment usage

IT equipment management policy

Since information technology (IT) equipment is capable of processing, storing or communicating sensitive or classified data, it is important that an IT equipment management policy is developed, implemented and maintained to ensure that IT equipment, and the data it processes, stores or communicates, is protected in an appropriate manner.

Control: ISM-1551; Revision: 2; Updated: Jun-24; Applicability: All; Essential Eight: N/A

An IT equipment management policy is developed, implemented and maintained.

IT equipment selection

When selecting IT equipment, it is important that an organisation preferences vendors that have demonstrated a commitment to secure-by-design and secure-by-default principles, use of memory-safe programming languages where possible (such as C#, Go, Java, Ruby, Rust and Swift), secure programming practices, and maintaining the security of their products. This will assist not only with reducing the potential number of vulnerabilities in IT equipment, but also increasing the likelihood that timely patches, updates or vendor mitigations will be released to remediate any vulnerabilities that are found.

Control: ISM-1857; Revision: 1; Updated: Jun-24; Applicability: All; Essential Eight: N/A

IT equipment is chosen from vendors that have demonstrated a commitment to secure-by-design and secure-by-default principles, use of memory-safe programming languages where possible, secure programming practices, and maintaining the security of their products.

Hardening IT equipment configurations

When IT equipment is deployed in its default state, or with an unapproved configuration, it can lead to an insecure operating environment that may allow malicious actors to gain an initial foothold on networks. Many settings exist within IT equipment to allow them to be configured in an approved secure state in order to minimise this security risk. As such, the Australian Signals Directorate (ASD) and vendors often produce hardening guidance to assist in hardening the configuration of IT equipment. Note, however, in situations where ASD and vendor hardening guidance conflicts, precedence should be given to implementing the most restrictive guidance.

Control: ISM-1913; Revision: 1; Updated: Jun-24; Applicability: All; Essential Eight: N/A
Approved configurations for IT equipment are developed, implemented and maintained.

Control: ISM-1858; Revision: 3; Updated: Jun-24; Applicability: All; Essential Eight: N/A
IT equipment is hardened using ASD and vendor hardening guidance, with the most restrictive guidance taking precedence when conflicts occur.

IT equipment registers

Developing, implementing, maintaining and regularly verifying registers of authorised IT equipment can assist an organisation in tracking legitimate IT equipment as well as determining whether unauthorised IT equipment, such as workstations, servers and network devices, have been introduced into their organisation. In doing so, an organisation may choose to split their IT equipment register into two by focusing on whether IT equipment is connected to their network or not.

Control: ISM-0336; Revision: 9; Updated: Jun-24; Applicability: All; Essential Eight: N/A
A networked IT equipment register is developed, implemented, maintained and verified on a regular basis.

Control: ISM-1869; Revision: 1; Updated: Jun-24; Applicability: All; Essential Eight: N/A
A non-networked IT equipment register is developed, implemented, maintained and verified on a regular basis.

Labelling IT equipment

Applying protective markings to IT equipment assists to reduce the likelihood that a user will accidentally input data into it that it is not approved for processing, storing or communicating.

While text-based protective markings are typically used for labelling IT equipment, 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-0294; Revision: 5; Updated: Jun-24; Applicability: All; Essential Eight: N/A
IT equipment, with the exception of high assurance IT equipment, is labelled with protective markings reflecting its sensitivity or classification.

Labelling high assurance IT equipment

High assurance IT equipment often has tamper-evident seals placed on its external surfaces. To assist users in noticing changes to these seals, and to prevent functionality being degraded, an organisation should limit the use of labels on high assurance IT equipment.

Control: ISM-0296; Revision: 7; Updated: Jun-24; Applicability: S, TS; Essential Eight: N/A
ASD's approval is sought before applying labels to external surfaces of high assurance IT equipment.

Classifying IT equipment

The purpose of classifying IT equipment is to acknowledge the sensitivity or classification of data that it is approved for processing, storing or communicating.

Classifying IT equipment also assists in ensuring that the appropriate sanitisation, destruction and disposal processes are followed at the end of its life.

Control: ISM-0293; Revision: 6; Updated: Jun-24; Applicability: All; Essential Eight: N/A

IT equipment is classified based on the highest sensitivity or classification of data that it is approved for processing, storing or communicating.

Handling IT equipment

When IT equipment displays, processes, stores or communicates sensitive or classified data, it will need to be handled as per the sensitivity or classification of that data. However, applying encryption to media within the IT equipment 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 data residing on media within the IT equipment and the level of assurance in the cryptographic equipment or software being used to encrypt it.

Control: ISM-1599; Revision: 1; Updated: Jun-24; Applicability: All; Essential Eight: N/A

IT equipment is handled in a manner suitable for its sensitivity or classification.

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 secure-by-design behaviours to look for in IT equipment, especially in Internet of Things devices, can be found in ASD's [IoT Secure-by-Design Guidance for Manufacturers](#) publication.

Further information on securing IT equipment 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 within IT equipment can be found in the cryptographic fundamentals section of the [Guidelines for Cryptography](#).

Further information on the protection of IT equipment can be found in the Department of Home Affairs' [Protective Security Policy Framework](#), [Physical security for entity resources](#) policy.

IT equipment maintenance and repairs

Maintenance and repairs of high assurance IT equipment

Due to the nature of high assurance IT equipment, it is important that ASD's approval is sought before any maintenance or repairs are undertaken.

Control: ISM-1079; Revision: 7; Updated: Jun-24; Applicability: S, TS; Essential Eight: N/A

ASD's approval is sought before undertaking any maintenance or repairs to high assurance IT equipment.

On-site maintenance and repairs

Undertaking unauthorised maintenance or repairs to IT equipment could impact its integrity. As such, using appropriately cleared technicians to maintain and repair IT equipment on site is considered the most secure approach. This ensures that if data is disclosed during the course of maintenance or repairs, the technicians are aware of the requirements to protect such data.

An organisation choosing to use technicians that are not appropriately cleared to maintain or repair IT equipment should be aware of the requirement for cleared personnel to escort the technicians during maintenance and repair activities.

Control: ISM-0305; Revision: 7; Updated: Jun-24; Applicability: All; Essential Eight: N/A

Maintenance and repairs of IT equipment is carried out on site by an appropriately cleared technician.

Control: ISM-0307; Revision: 4; Updated: Jun-24; Applicability: All; Essential Eight: N/A

If an appropriately cleared technician is not used to undertake maintenance or repairs of IT equipment, the IT equipment and associated media is sanitised before maintenance or repair work is undertaken.

Control: ISM-0306; Revision: 7; Updated: Jun-24; Applicability: All; Essential Eight: N/A

If an appropriately cleared technician is not used to undertake maintenance or repairs of IT equipment, the technician is escorted by someone who:

- *is appropriately cleared and briefed*
- *takes due care to ensure that data is not disclosed*
- *takes all responsible measures to ensure the integrity of the IT equipment*
- *has the authority to direct the technician*
- *is sufficiently familiar with the IT equipment to understand the work being performed.*

Off-site maintenance and repairs

An organisation choosing to have IT equipment maintained or repaired off site should do so at facilities approved for handling the sensitivity or classification of the IT equipment. However, an organisation may be able to sanitise the IT equipment prior to transport, and subsequent maintenance or repair activities, to change how it needs to be handled.

Control: ISM-0310; Revision: 8; Updated: Jun-24; Applicability: All; Essential Eight: N/A

IT equipment maintained or repaired off site is done so at facilities approved for handling the sensitivity or classification of the IT equipment.

Inspection of IT equipment following maintenance and repairs

Following the maintenance or repair of IT equipment, it is important that the IT equipment is inspected to ensure that it retains its approved software configuration and that no unauthorised modifications have been made by technicians.

Control: ISM-1598; Revision: 1; Updated: Jun-24; Applicability: All; Essential Eight: N/A

Following maintenance or repair activities for IT equipment, the IT equipment is inspected to confirm it retains its approved software configuration and that no unauthorised modifications have taken place.

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 sanitisation of media can be found in the media sanitisation section of the [Guidelines for Media](#).

IT equipment sanitisation and destruction

IT equipment sanitisation processes and procedures

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

Control: ISM-0313; Revision: 7; Updated: Jun-24; Applicability: All; Essential Eight: N/A

IT equipment sanitisation processes, and supporting IT equipment sanitisation procedures, are developed, implemented and maintained.

IT equipment destruction processes and procedures

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

Control: ISM-1741; Revision: 2; Updated: Jun-24; Applicability: All; Essential Eight: N/A

IT equipment destruction processes, and supporting IT equipment destruction procedures, are developed, implemented and maintained.

Sanitising IT equipment

When sanitising IT equipment, any media within the IT equipment should be removed or sanitised. Once any media has been removed or sanitised, IT equipment can be considered sanitised. However, if media cannot be removed or sanitised, the IT equipment should be destroyed as per media destruction requirements.

Media typically found in IT equipment includes:

- electrostatic memory devices, such as laser printer cartridges used in multifunction devices (MFDs)
- non-volatile magnetic memory, such as hard disks
- non-volatile semiconductor memory, such as flash cards and solid-state drives
- volatile memory, such as random-access memory sticks.

Control: ISM-0311; Revision: 7; Updated: Jun-24; Applicability: All; Essential Eight: N/A

IT equipment containing media is sanitised by removing the media from the IT equipment or by sanitising the media in situ.

Control: ISM-1742; Revision: 1; Updated: Jun-24; Applicability: All; Essential Eight: N/A

IT equipment that cannot be sanitised is destroyed.

Sanitising highly sensitive IT equipment

IT equipment located overseas that has processed, stored or communicated Australian Eyes Only (AUSTEO) or Australian Government Access Only (AGAO) data can have more severe consequences for Australian interests if not sanitised appropriately.

Control: ISM-1218; Revision: 5; Updated: Jun-24; Applicability: S, TS; Essential Eight: N/A

IT equipment, including associated media, that is located overseas and has processed, stored or communicated AUSTEO or AGAO data, is sanitised in situ.

Control: ISM-0312; Revision: 7; Updated: Jun-24; Applicability: S, TS; Essential Eight: N/A

IT equipment, including associated media, that is located overseas and has processed, stored or communicated AUSTEO or AGAO data that cannot be sanitised in situ, is returned to Australia for destruction.

Destroying high assurance IT equipment

Due to the nature of high assurance IT equipment, and many of the protective mechanisms it employs, sanitisation alone is not sufficient prior to its disposal. As such, all high assurance IT equipment should be destroyed prior to its disposal.

Control: ISM-0315; Revision: 9; Updated: Jun-24; Applicability: S, TS; Essential Eight: N/A

High assurance IT equipment is destroyed prior to its disposal.

Sanitising printers and multifunction devices

When sanitising printers and MFDs, the printer cartridge or MFD print drum should be sanitised in addition to the removal or sanitisation of any media. This can be achieved by printing random text with no blank areas on each colour printer cartridge or MFD print drum. In addition, image transfer rollers and platens can become imprinted with text and images over time and should be destroyed if any text or images have been retained. Finally, any paper jammed in the paper path should be removed.

When printer cartridges and MFD print drums cannot be sanitised due to a hardware failure, or when they are empty, there is no other option available but to destroy them. Printer ribbons cannot be sanitised and should be destroyed.

Control: ISM-0317; Revision: 3; Updated: Sep-18; Applicability: All; Essential Eight: N/A

At least three pages of random text with no blank areas are printed on each colour printer cartridge or MFD print drum.

Control: ISM-1219; Revision: 2; Updated: Dec-21; Applicability: All; Essential Eight: N/A

MFD print drums and image transfer rollers are inspected and destroyed if there is remnant toner which cannot be removed or a print is visible on the image transfer roller.

Control: ISM-1220; Revision: 2; Updated: Dec-21; Applicability: All; Essential Eight: N/A

Printer and MFD platens are inspected and destroyed if any text or images are retained on the platen.

Control: ISM-1221; Revision: 1; Updated: Sep-18; Applicability: All; Essential Eight: N/A

Printers and MFDs are checked to ensure no pages are trapped in the paper path due to a paper jam.

Control: ISM-0318; Revision: 3; Updated: Sep-18; Applicability: All; Essential Eight: N/A

When unable to sanitise printer cartridges or MFD print drums, they are destroyed as per electrostatic memory devices.

Control: ISM-1534; Revision: 0; Updated: Sep-18; Applicability: All; Essential Eight: N/A

Printer ribbons in printers and MFDs are removed and destroyed.

Sanitising televisions and computer monitors

All types of televisions and computer monitors are capable of retaining data if mitigating measures are not taken during their lifetime. Cathode Ray Tube monitors and plasma screens can be affected by burn-in while Liquid Crystal Display and Organic Light Emitting Diode screens can be affected by image persistence.

Televisions and computer monitors can be visually inspected by turning up the brightness and contrast to their maximum level to determine if any data has been burnt into or persists on the screen. If burn-in or image persistence

is removed by this activity, televisions and computer monitors can be considered sanitised. However, if burn-in or persistence is not removed through these measures, televisions and computer monitors cannot be sanitised and should be destroyed.

If televisions or computer monitors cannot be powered on, such as due to a faulty power supply, they cannot be sanitised and should be destroyed.

Control: ISM-1076; Revision: 2; Updated: Sep-18; Applicability: All; Essential Eight: N/A

Televisions and computer monitors with minor burn-in or image persistence are sanitised by displaying a solid white image on the screen for an extended period of time.

Control: ISM-1222; Revision: 1; Updated: Sep-18; Applicability: All; Essential Eight: N/A

Televisions and computer monitors that cannot be sanitised are destroyed.

Sanitising network devices

As network devices can store network configuration data or credentials in their memory, the memory should be sanitised prior to the disposal of the network devices. The correct method to sanitise network devices will depend on their configuration and the type of memory they use. As such, device-specific guidance provided in evaluation documentation, or vendor sanitisation guidance, should be consulted to determine the most appropriate method to sanitise memory in network devices.

Control: ISM-1223; Revision: 6; Updated: Dec-21; Applicability: All; Essential Eight: N/A

Memory in network devices is sanitised using the following processes, in order of preference:

- *following device-specific guidance provided in evaluation documentation*
- *following vendor sanitisation guidance*
- *loading a dummy configuration file, performing a factory reset and then reinstalling firmware.*

Sanitising fax machines

As fax machines can store pages that are ready for transmission in their memory, the memory should be sanitised prior to the disposal of the fax machines. This can be achieved by removing the paper tray, transmitting a fax message with a minimum length of four pages, then re-installing the paper tray and allowing a fax summary page to be printed. In addition, any paper that becomes trapped in the paper path should be removed prior to disposal.

Control: ISM-1225; Revision: 2; Updated: Sep-18; Applicability: All; Essential Eight: N/A

The paper tray of the fax machine is removed, and a fax message with a minimum length of four pages is transmitted, before the paper tray is re-installed to allow a fax summary page to be printed.

Control: ISM-1226; Revision: 2; Updated: Sep-18; Applicability: All; Essential Eight: N/A

Fax machines are checked to ensure no pages are trapped in the paper path due to a paper jam.

Further information

Further information on the sanitisation of media can be found in the media sanitisation section of the [Guidelines for Media](#).

Further information on the destruction of media can be found in the media destruction section of the [Guidelines for Media](#).

Further information on the sanitisation of network devices is available from vendors and can be found in evaluation documentation on the Common Criteria's [Certified Products List](#).

IT equipment disposal

IT equipment disposal processes and procedures

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

Control: ISM-1550; Revision: 3; Updated: Jun-24; Applicability: All; Essential Eight: N/A

IT equipment disposal processes, and supporting IT equipment disposal procedures, are developed, implemented and maintained.

Disposal of IT equipment

Before IT equipment can be released into the public domain, it needs to be sanitised, destroyed or declassified. As sanitised, destroyed or declassified IT equipment 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 IT equipment with its prior use will ensure it does not draw undue attention following its disposal.

Control: ISM-1217; Revision: 3; Updated: Jun-24; Applicability: All; Essential Eight: N/A

Labels and markings indicating the owner, sensitivity, classification or any other marking that can associate IT equipment with its prior use are removed prior to its disposal.

Control: ISM-0321; Revision: 6; Updated: Jun-24; Applicability: S, TS; Essential Eight: N/A

When disposing of IT equipment that has been designed or modified to meet emanation security standards, ASD is contacted for requirements relating to its disposal.

Control: ISM-0316; Revision: 4; Updated: Jun-24; Applicability: All; Essential Eight: N/A

Following sanitisation, destruction or declassification, a formal administrative decision is made to release IT equipment, 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.

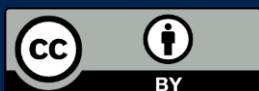
The Commonwealth accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.

Copyright

© Commonwealth of Australia 2024.

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/government/commonwealth-coat-arms).

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

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



Australian Government

Australian Signals Directorate