



# Information Security Manual

Published: 22 June 2023

## Guidelines for ICT Equipment

### ICT equipment usage

#### ICT equipment management policy

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

**Control: ISM-1551; Revision: 1; Updated: Dec-22; Applicability: All; Essential Eight: N/A**

*An ICT equipment management policy is developed, implemented and maintained.*

#### ICT equipment selection

When selecting ICT 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 security vulnerabilities in ICT equipment, but also increasing the likelihood that timely patches, updates or vendor mitigations will be released to remediate any security vulnerabilities that are found.

**Control: ISM-1857; Revision: 0; Updated: Jun-23; Applicability: All; Essential Eight: N/A**

*ICT 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 ICT equipment configurations

When ICT equipment is deployed in its default state it can lead to an insecure operating environment that may allow an adversary to gain an initial foothold on networks. Many configuration settings exist within ICT equipment to allow them to be configured in a secure state in order to minimise this security risk. As such, the Australian Cyber Security Centre (ACSC) and vendors often produce hardening guidance to assist in hardening the configuration of ICT equipment. Note, however, in situations where ACSC and vendor hardening guidance conflicts, preference should be given to implementing ACSC hardening guidance.

**Control: ISM-1858; Revision: 0; Updated: Jun-23; Applicability: All; Essential Eight: N/A**

*ACSC and vendor hardening guidance for ICT equipment is implemented.*

## ICT equipment register

Developing, implementing, maintaining and regularly verifying a register of authorised ICT equipment can assist an organisation in tracking legitimate ICT equipment as well as determining whether unauthorised ICT equipment, such as workstations, servers and network devices, have been introduced into their organisation.

**Control: ISM-0336; Revision: 7; Updated: Dec-22; Applicability: All; Essential Eight: N/A**

*An ICT equipment register is developed, implemented, maintained and verified on a regular basis.*

## Labelling ICT equipment

Applying protective markings to ICT 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 ICT 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: 4; Updated: Sep-18; Applicability: All; Essential Eight: N/A**

*ICT equipment, with the exception of high assurance ICT equipment, is labelled with protective markings reflecting its sensitivity or classification.*

## Labelling high assurance ICT equipment

High assurance ICT 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 ICT equipment.

**Control: ISM-0296; Revision: 5; Updated: Dec-21; Applicability: S, TS; Essential Eight: N/A**

*The ACSC's approval is sought before applying labels to external surfaces of high assurance ICT equipment.*

## Classifying ICT equipment

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

Classifying ICT 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: 5; Updated: Jun-21; Applicability: All; Essential Eight: N/A**

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

## Handling ICT equipment

When ICT 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 ICT 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 ICT equipment and the level of assurance in the cryptographic equipment or software being used to encrypt it.

**Control: ISM-1599; Revision: 0; Updated: Aug-20; Applicability: All; Essential Eight: N/A**

*ICT 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 ICT equipment, especially in Internet of Things devices, can be found in the ACSC's [IoT Code of Practice – Guidance for Manufacturers](#) publication.

Further information on securing ICT equipment when not in use can be found in the ICT equipment and media section of the [Guidelines for Physical Security](#).

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

Further information on the protection of ICT equipment can be found in the Attorney-General's Department's [Protective Security Policy Framework](#), [Physical security for entity resources](#) policy.

## ICT equipment maintenance and repairs

### Maintenance and repairs of high assurance ICT equipment

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

**Control:** *ISM-1079; Revision: 5; Updated: Dec-21; Applicability: S, TS; Essential Eight: N/A*

*The ACSC's approval is sought before undertaking any maintenance or repairs to high assurance ICT equipment.*

### On-site maintenance and repairs

Undertaking unauthorised maintenance or repairs to ICT equipment could impact its integrity. As such, using appropriately cleared technicians to maintain and repair ICT 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 uncleared technicians to maintain or repair ICT equipment should be aware of the requirement for cleared personnel to escort uncleared technicians during maintenance or repair activities.

**Control:** *ISM-0305; Revision: 6; Updated: Dec-21; Applicability: All; Essential Eight: N/A*

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

**Control:** *ISM-0307; Revision: 2; Updated: Sep-18; Applicability: All; Essential Eight: N/A*

*If an uncleared technician is used to undertake maintenance or repairs of ICT equipment, the ICT equipment and associated media is sanitised before maintenance or repair work is undertaken.*

**Control:** *ISM-0306; Revision: 5; Updated: Jun-21; Applicability: All; Essential Eight: N/A*

*If an uncleared technician is used to undertake maintenance or repairs of ICT 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 ICT equipment*
- *has the authority to direct the technician*
- *is sufficiently familiar with the ICT equipment to understand the work being performed.*

## Off-site maintenance and repairs

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

**Control: ISM-0310; Revision: 7; Updated: Mar-22; Applicability: All; Essential Eight: N/A**

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

## Inspection of ICT equipment following maintenance and repairs

Following the maintenance or repair of ICT equipment, it is important that the ICT 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: 0; Updated: Aug-20; Applicability: All; Essential Eight: N/A**

*Following maintenance or repair activities for ICT equipment, the ICT 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](#).

## ICT equipment sanitisation and destruction

### ICT equipment sanitisation processes and procedures

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

**Control: ISM-0313; Revision: 6; Updated: Dec-22; Applicability: All; Essential Eight: N/A**

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

### ICT equipment destruction processes and procedures

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

**Control: ISM-1741; Revision: 1; Updated: Dec-22; Applicability: All; Essential Eight: N/A**

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

## Sanitising ICT equipment

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

Media typically found in ICT 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: 6; Updated: Mar-22; Applicability: All; Essential Eight: N/A**

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

**Control: ISM-1742; Revision: 0; Updated: Mar-22; Applicability: All; Essential Eight: N/A**

*ICT equipment that cannot be sanitised is destroyed.*

### **Sanitising highly sensitive ICT equipment**

ICT 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: 4; Updated: Dec-21; Applicability: S, TS; Essential Eight: N/A**

*ICT 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: 6; Updated: Dec-21; Applicability: S, TS; Essential Eight: N/A**

*ICT 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 ICT equipment**

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

**Control: ISM-0315; Revision: 8; Updated: Mar-22; Applicability: S, TS; Essential Eight: N/A**

*High assurance ICT 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](#).

## ICT equipment disposal

### ICT equipment disposal processes and procedures

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

**Control: ISM-1550; Revision: 2; Updated: Dec-22; Applicability: All; Essential Eight: N/A**

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

### Disposal of ICT equipment

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

**Control: ISM-1217; Revision: 2; Updated: Dec-21; Applicability: All; Essential Eight: N/A**

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

**Control: ISM-0321; Revision: 4; Updated: Dec-21; Applicability: S, TS; Essential Eight: N/A**

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

**Control: ISM-0316; Revision: 3; Updated: Dec-21; Applicability: All; Essential Eight: N/A**

*Following sanitisation, destruction or declassification, a formal administrative decision is made to release ICT equipment, or its waste, into the public domain.*