Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Australian Government Information Security Manual

DECEMBER 2020

Guidelines for ICT Equipment

ICT equipment usage

ICT equipment management policy

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

Security Control: 1551; Revision: 0; Updated: Aug-19; Applicability: O, P, S, TS
An ICT equipment management policy is developed and implemented.

Classifying ICT equipment

The purpose of classifying ICT equipment it to acknowledge the sensitivity or classification of information 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.

Security Control: 0293; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS
ICT equipment is classified based on the highest sensitivity or classification of information that it is approved for processing, storing or communicating.

Labelling ICT equipment

Applying protective markings to ICT equipment assists to reduce the likelihood that a user will accidentally input information 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.

Security Control: 0294; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS
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, organisations should limit the use of labels on high assurance ICT equipment.

Security Control: 0296; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS
The Australian Cyber Security Centre (ACSC)'s approval is sought before applying labels to external surfaces of high assurance ICT equipment.

Handling ICT equipment

As ICT equipment can often retain sensitive or classified information, it will need to be handled, and subsequently protected, as per the sensitivity or classification of information that it displays, processes, stores or communicates. However, applying encryption to media within ICT equipment may reduce the requirements for storage and physical transfer. Any reduction in requirements needs to be based on the original sensitivity or classification of information residing on media within the ICT equipment and the level of assurance in the encryption software being used to encrypt the media.

Security Control: 1599; Revision: 0; Updated: Aug-20; Applicability: O, P, S, TS
ICT equipment is handled in a manner suitable for its sensitivity or classification.

Further information

Further information on classifying and labelling of media can be found in the media usage section of the ***Guidelines for Media***.

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.

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 repair work is undertaken.

Security Control: 1079; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS
The ACSC's approval is sought before undertaking any repairs to high assurance ICT equipment.

On-site maintenance and repairs

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

Organisations 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.

Security Control: 0305; Revision: 5; Updated: Oct-19; Applicability: O, P, S, TS
Maintenance and repairs of ICT equipment is carried out on-site by an appropriately cleared technician.

Security Control: 0307; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS

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.

Security Control: 0306; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS
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 information 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

Organisations choosing to have ICT equipment maintained or repaired off-site should be aware of requirements for the external company's facilities to be approved to do so based on the sensitivity or classification of the ICT equipment.

Organisations choosing to have ICT equipment maintained or repaired off-site can sanitise the ICT equipment prior to transport, and subsequent maintenance or repair activities, to lower (depending on the types of media involved) its physical transfer and storage requirements.

Security Control: 0310; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS
ICT equipment maintained or repaired off-site is done so in accordance with the physical transfer and storage requirements for the sensitivity or classification of the ICT equipment.

Maintenance and repair of ICT equipment from secured spaces

When ICT equipment resides in an area that also contains ICT equipment of a higher classification, a technician could modify the lower classified ICT equipment in an attempt to compromise co-located ICT equipment of a higher classification.

Security Control: 0944; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS
ICT equipment maintained or repaired off-site is treated as per the requirements for the sensitivity or classification of the area that the ICT equipment will be returned to.

Inspection of ICT equipment following maintenance and repairs

Following the maintenance or repair of ICT equipment (either on-site or off-site), it is important that the ICT equipment is inspected to ensure that it retains its approved software configuration and that no unauthorised modifications (either accidental or deliberate) have been made by technicians.

Security Control: 1598; Revision: 0; Updated: Aug-20; Applicability: O, P, S, TS
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 the sanitisation of ICT equipment can be found in the ICT equipment sanitisation and disposal section of these guidelines.

Further information on the sanitisation of media can be found in the media sanitisation section of the ***Guidelines for Media***.

Further information on the storage and transfer of ICT equipment 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.

ICT equipment sanitisation and disposal

ICT equipment sanitisation and disposal processes and procedures

When disposing of ICT equipment, any media in the ICT equipment should be sanitised in situ or removed and sanitised separately. Once any media has been sanitised or removed, ICT equipment can be considered sanitised. As such, the ICT equipment can then be declassified and formally authorised for release into the public domain. However, if media cannot be sanitised or removed, the ICT equipment will need to be destroyed in its entirety.

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

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.

Security Control: 0313; Revision: 4; Updated: Aug-19; Applicability: O, P, S, TS
An ICT equipment sanitisation process, and supporting ICT equipment sanitisation procedures, is developed and implemented.

Security Control: 1550; Revision: 0; Updated: Aug-19; Applicability: O, P, S, TS
An ICT equipment disposal process, and supporting ICT equipment disposal procedures, is developed and implemented.

Security Control: 0311; Revision: 5; Updated: Sep-18; Applicability: O, P, S, TS
When disposing of ICT equipment containing media, the ICT equipment is sanitised by sanitising the media within the ICT equipment, removing the media from the ICT equipment or destroying the ICT equipment in its entirety.

Security Control: 1217; Revision: 1; 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 the ICT equipment with its original use, are removed prior to disposal.

Security Control: 0316; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
Following sanitisation, destruction or declassification, a formal administrative decision is made to handle ICT equipment, or its waste, as 'publicly releasable' before it is released into the public domain.

Sanitisation and disposal of highly sensitive ICT equipment

The ACSC provides specific advice on how to securely dispose of high assurance ICT equipment and ICT equipment designed or modified to meet TEMPEST standards. In addition, ICT equipment located overseas that has processed or stored Australian Eyes Only (AUSTEO) and Australian Government Access Only (AGAO) material can have more severe consequences for Australian interests if not sanitised and disposed of appropriately.

Security Control: 0315; Revision: 6; Updated: Dec-20; Applicability: O, P, S, TS
When disposing of high assurance ICT equipment, it is destroyed prior to its disposal.

Security Control: 0321; Revision: 3; Updated: Dec-20; Applicability: O, P, S, TS

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

Security Control: 1218; Revision: 2; Updated: Oct-19; Applicability: S, TS
ICT equipment, including associated media, that is located overseas and has processed or stored AUSTEO or AGAO information is sanitised in situ.

Security Control: 0312; Revision: 4; Updated: Sep-18; Applicability: S, TS
ICT equipment, including associated media, that is located overseas and has processed or stored AUSTEO or AGAO information that cannot be sanitised in situ is returned to Australia for destruction.

Sanitisation and disposal of printers and multifunction devices

When sanitising and disposing of printers and MFDs, the printer cartridge or MFD print drum should be sanitised in addition to the sanitisation or removal 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, transfer rollers and platens can become imprinted with text and images over time and should be destroyed if any 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.

Security Control: 0317; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS
At least three pages of random text with no blank areas are printed on each colour printer cartridge or MFD print drum.

Security Control: 1219; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
MFD print drums and image transfer rollers are inspected and destroyed if there is remnant toner which cannot be removed or if a print is visible on the image transfer roller.

Security Control: 1220; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
Printer and MFD platens are inspected and destroyed if any images are retained on the platen.

Security Control: 1221; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
Printers and MFDs are checked to ensure no pages are trapped in the paper path due to a paper jam.

Security Control: 0318; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS
When unable to sanitise printer cartridges or MFD print drums, they are destroyed as per electrostatic memory devices.

Security Control: 1534; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS
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 information if mitigation measures are not taken during their lifetime. Cathode Ray Tube monitors and plasma screens can be affected by burn-in while Liquid Crystal Display 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 information 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 allowing them to be declassified and formally authorised for release into the public domain. However, if burn-in or persistence is not removed through these measures, televisions and computer monitors cannot be sanitised and should be destroyed.

If the television or computer monitor cannot be powered on (e.g. due to a faulty power supply) the unit cannot be sanitised and should be destroyed.

Security Control: 1076; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS

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.

Security Control: 1222; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
Televisions and computer monitors that cannot be sanitised are destroyed.

Sanitising network devices

Routers, switches, network interface cards and firewalls contain memory that is used in their operation. This memory can often retain network configuration information such as passwords, encryption keys and certificates. The correct method to sanitise a network device will depend on the configuration of the device and the type of memory within the device. Device-specific guidance provided by the ACSC, or vendor sanitisation guidance, should be consulted to determine the most appropriate method to remove information from a network device's memory.

Security Control: 1223; Revision: 4; Updated: Nov-19; Applicability: O, P, S, TS
Memory in network devices is sanitised using the following processes, in order of preference:

- *following device-specific guidance provided by the ACSC*
- *following vendor sanitisation guidance*
- *loading a dummy configuration file, performing a factory reset and then reinstalling firmware.*

Sanitising fax machines

Fax machines store information such as phone number directories and pages ready for transmission. In addition to the sanitisation or removal of any media within fax machines, the memory should be cleared and any paper jammed in the paper path should be removed.

Security Control: 1225; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
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.

Security Control: 1226; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
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, destruction and disposal of media can be found in the ***Guidelines for Media***.