



Information security manual

September 2026

First published: 07 September 2026

Guidelines for physical security

Facilities and systems

Physical access to systems

The application of the defence-in-depth principle to the protection of systems is enhanced through successive layers of physical security. The first layer of physical security for facilities that contain systems is generally the use of a security zone.

Deployable platforms should also meet physical security requirements. In some cases, physical security certification authorities may have specific requirements for deployable platforms that supersede the security controls in these guidelines. This may include perimeter controls, building standards and staffing levels. As such, an organisation implementing deployable platforms should contact their physical security certification authority to seek additional guidance.

Control: ISM-1973; Revision: 0; Updated: Dec-24; Applicable: NC; Essential 8: N/A

Non-classified systems are secured in suitably secure facilities.

Control: ISM-0810; Revision: 7; Updated: Dec-24; Applicable: OS, P, S, TS; Essential 8: N/A

Classified systems are secured in facilities that meet the requirements for a security zone suitable for their classification.

Physical access to servers, network devices and cryptographic equipment

The second layer of physical security is the use of an additional security zone for a server room or communications room. This is then further supplemented by security containers for the protection of servers, network devices and cryptographic equipment.

Control: ISM-1974; Revision: 0; Updated: Dec-24; Applicable: NC; Essential 8: N/A

Non-classified servers, network devices and cryptographic equipment are secured in suitably secure server rooms or communications rooms.

Control: ISM-1053; Revision: 5; Updated: Dec-24; Applicable: OS, P, S, TS; Essential 8: N/A

Classified servers, network devices and cryptographic equipment are secured in server rooms or communications rooms that meet the requirements for a security zone suitable for their classification.

Control: ISM-1975; Revision: 0; Updated: Dec-24; Applicable: NC; Essential 8: N/A

Non-classified servers, network devices and cryptographic equipment are secured in suitably secure security containers.

Control: ISM-1530; Revision: 3; Updated: Dec-24; Applicable: OS, P, S, TS; Essential 8: N/A

Classified servers, network devices and cryptographic equipment are secured in security containers suitable for their classification taking into account the combination of security zones they reside in.

Control: ISM-0813; Revision: 5; Updated: Dec-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A

Server rooms, communications rooms and security containers are not left in unsecured states.

Control: ISM-1074; Revision: 4; Updated: Dec-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A

Keys or equivalent access mechanisms to server rooms, communications rooms and security containers are appropriately controlled.

Physical access to network devices in public areas

Unprotected network devices in public areas could lead to accidental or deliberate physical damage resulting in an interruption of services. Alternatively, unauthorised access to network devices may allow malicious actors to reset them to factory default settings or connect directly to them to bypass network access controls. Even if access to network devices is not gained by resetting them to factory default settings, it is highly likely that it will cause an interruption of services.

Physical access to network devices can be restricted through the implementation of physical security, such as using enclosures that prevent access to their console ports and factory reset buttons, mounting them on ceilings or behind walls, or securing them in security containers.

Control: ISM-1296; Revision: 4; Updated: Jun-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A

Physical security is implemented to protect network devices in public areas from physical damage or unauthorised access.

Bringing radio frequency and infrared devices into facilities

Radio frequency (RF) devices, such as mobile devices, wireless keyboards and Bluetooth devices, as well as infrared (IR) devices, can pose a security risk to an organisation, especially when they can record or transmit audio or data. In SECRET and TOP SECRET areas, it is important that an organisation understands the security risks associated with the introduction of RF and IR devices and develops, implements, maintains and regularly verifies a register of those that have been authorised for use in such environments.

In deciding which RF or IR devices to authorise to be brought into SECRET and TOP SECRET areas, an organisation should consider any mitigating measures already in place. These include whether IR communications would be prevented from travelling outside secured spaces, whether systems of different sensitivities or classifications are used in the same spaces, and if any temporary or permanent method of blocking RF or IR transmissions has been applied to the facility.

Control: ISM-1543; Revision: 5; Updated: Jun-26; Applicable: S, TS; Essential 8: N/A

An authorised RF and IR device register for SECRET and TOP SECRET areas is developed, implemented, maintained and regularly verified.

Control: ISM-0225; Revision: 3; Updated: Sep-21; Applicable: S, TS; Essential 8: N/A

Unauthorised RF and IR devices are not brought into SECRET and TOP SECRET areas.

Control: ISM-0829; Revision: 4; Updated: Mar-19; Applicable: S, TS; Essential 8: N/A

Security measures are used to detect and respond to unauthorised RF devices in SECRET and TOP SECRET areas.

Bringing photographic and video recording devices into facilities

Photographic and video recording devices, such as cameras, video cameras and smart glasses, can pose a security risk to an organisation, especially when they can record photographs or videos in an inconspicuous manner. In SECRET and TOP SECRET areas, it is important that an organisation understands the security risks associated with the introduction of photographic and video recording devices and develops, implements, maintains and regularly verifies a register of those that have been authorised for use in such environments.

Control: ISM-2069; Revision: 1; Updated: Jun-26; Applicable: S, TS; Essential 8: N/A

An authorised photographic and video recording device register for SECRET and TOP SECRET areas is developed, implemented, maintained and regularly verified.

Control: ISM-2070; Revision: 0; Updated: Sep-25; Applicable: S, TS; Essential 8: N/A

Unauthorised photographic and video recording devices are not brought into SECRET and TOP SECRET areas.

Bringing medical devices into facilities

Medical devices are devices approved by the Therapeutic Goods Administration under the [Therapeutic Goods \(Medical Devices\) Regulations 2002](#) for diagnostic or therapeutic purposes. The use of medical devices in SECRET and TOP SECRET areas requires active management, similar to RF

devices, as they may contain communications functionality that could compromise the security of SECRET or TOP SECRET areas or systems within such areas.

Control: ISM-2007; Revision: 1; Updated: Jun-26; Applicable: S, TS; Essential 8: N/A

An authorised medical device register for SECRET and TOP SECRET areas is developed, implemented, maintained and regularly verified.

Control: ISM-2008; Revision: 1; Updated: Jun-26; Applicable: S, TS; Essential 8: N/A

Medical devices authorised to be brought into SECRET and TOP SECRET areas meet, at a minimum, the following criteria:

- *are listed on the Australian Register of Therapeutic Goods*
- *have been prescribed by a legally qualified medical practitioner*
- *have been commercially purchased within Australia*
- *do not have inbuilt cellular connectivity*
- *can operate independently of mobile devices*
- *where possible, have Wi-Fi, Bluetooth and other forms of wireless connectivity disabled when operating within SECRET and TOP SECRET areas.*

Control: ISM-2009; Revision: 0; Updated: Mar-25; Applicable: S, TS; Essential 8: N/A

Unauthorised medical devices are not brought into SECRET and TOP SECRET areas.

Preventing observation by unauthorised people

Without sufficient perimeter security, the inside of a facility is often observable by unauthorised people, such as via direct observation or by using equipment with a telephoto lens. Ensuring systems, in particular workstation displays and keyboards, are not visible through windows, such as via the use of blinds, curtains, privacy films or workstation positioning, will assist in reducing this security risk.

Control: ISM-0164; Revision: 3; Updated: Dec-21; Applicable: NC, OS, P, S, TS; Essential 8: N/A

Unauthorised people are prevented from observing systems, in particular workstation displays and keyboards, within facilities.

Further information

Further information on the certification and accreditation authorities for physical security can be found in the Department of Home Affairs' [Protective Security Policy Framework](#).

Further information on the physical security requirements for specific security zones can be found in the Department of Home Affairs' [Protective Security Policy Framework](#).

Further information on selecting security zones and security containers for the protection of information technology (IT) equipment can be found in the Department of Home Affairs' [Protective Security Policy Framework](#).

Further information on emanation security considerations associated with usage of RF devices in SECRET and TOP SECRET areas can be found in the 'Emanation security' section of the [Guidelines for communications infrastructure](#).

Further information on medical devices approved by the Therapeutic Goods Administration for diagnostic or therapeutic purposes can be found on the [Australian Register of Therapeutic Goods](#).

IT equipment and media

Securing IT equipment and media

IT equipment and media need to be secured when not in use. This can be achieved by implementing one of the following approaches:

- securing IT equipment and media in an appropriate security container
- using IT equipment without hard drives and sanitising memory at shut down
- encrypting hard drives of IT equipment and sanitising memory at shut down
- sanitising memory of IT equipment at shut down and removing and securing any hard drives.

If none of the above approaches are feasible, an organisation may wish to minimise the potential impact of not securing IT equipment when not in use. This can be achieved by preventing sensitive or classified data from being stored on hard drives, storing user profiles and documents on network shares, removing temporary user data at logoff, scrubbing virtual memory at shut down, and sanitising memory at shut down. However, there is no guarantee such measures will always work effectively or will not be bypassed due to unexpected circumstances, such as the loss of power. Therefore, hard drives in such cases will retain their sensitivity or classification for the purposes of reuse, reclassification, declassification, sanitisation, destruction and disposal.

Control: ISM-0161; Revision: 6; Updated: Jun-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
IT equipment and media are secured when not in use.

Further information

Further information on the handling of IT equipment can be found in the 'IT equipment usage' section of the [Guidelines for information technology equipment](#).

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

Further information on encrypting media can be found in the 'Cryptographic fundamentals' section of the [Guidelines for cryptography](#).

Further information on selecting security zones and security containers for the protection of IT equipment can be found in the Department of Home Affairs' [Protective Security Policy Framework](#).

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 2026

With the exception of the Coat of Arms and where otherwise stated, all material presented in this publication is provided under a Creative Commons Attribution 4.0 International license

<https://creativecommons.org/licenses/by/4.0/>.

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



The details of the relevant license conditions are available on the Creative Commons website as is the full legal code for the CC BY 4.0 license <https://creativecommons.org/licenses/by/4.0/legalcode.en>.

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 <https://www.pmc.gov.au/resources/commonwealth-coat-arms-information-and-guidelines>.