Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Information Security Manual

Published: 01 December 2022

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 the use of successive layers of physical security. The first layer of physical security being the use of a security zone for facilities containing systems.

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

Control: ISM-0810; Revision: 5; Updated: Dec-21; Applicability: O, P, S, TS; Essential Eight: N/A
Systems are secured in facilities that meet the requirements for a security zone suitable for their sensitivity or 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 the use of security containers or secure rooms for the protection of servers, network devices and cryptographic equipment.

Control: ISM-1053; Revision: 3; Updated: Dec-21; Applicability: O, P, S, TS; Essential Eight: N/A
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 sensitivity or classification.

Control: ISM-1530; Revision: 1; Updated: Dec-21; Applicability: O, P, S, TS; Essential Eight: N/A
Servers, network devices and cryptographic equipment are secured in security containers or secure rooms suitable for their sensitivity or classification taking into account the combination of security zones they reside in.

Control: ISM-0813; Revision: 4; Updated: Dec-21; Applicability: All; Essential Eight: N/A
Server rooms, communications rooms, security containers and secure rooms are not left in unsecured states.

Control: ISM-1074; Revision: 3; Updated: Dec-21; Applicability: All; Essential Eight: N/A
Keys or equivalent access mechanisms to server rooms, communications rooms, security containers and secure rooms 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 an adversary to reset them to factory default settings, thereby removing any controls, or connect directly to them in order 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; Applicability: All; Essential Eight: 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 are capable of recording or transmitting 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 develop, implement and maintain 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, such as whether IR communications would be prevented from travelling outside secured spaces, whether systems of different sensitives 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: 4; Updated: Dec-22; Applicability: S, TS; Essential Eight: N/A
An authorised RF and IR device register for SECRET and TOP SECRET areas is developed, implemented, maintained and verified on a regular basis.

Control: ISM-0225; Revision: 3; Updated: Sep-21; Applicability: S, TS; Essential Eight: N/A
Unauthorised RF and IR devices are not brought into SECRET and TOP SECRET areas.

Control: ISM-0829; Revision: 4; Updated: Mar-19; Applicability: S, TS; Essential Eight: N/A
Security measures are used to detect and respond to unauthorised RF devices in 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; Applicability: All; Essential Eight: 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 Attorney-General's Department (AGD)'s *Protective Security Policy Framework* (PSPF), *Entity facilities* policy.

Further information on the physical security requirements for specific security zones can be found in AGD's PSPF, *Entity facilities* policy.

Further information on selecting security zones, security containers and secure rooms for the protection of ICT equipment can be found in AGD's PSPF, *Physical security for entity resources* policy.

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*.

ICT equipment and media

Securing ICT equipment and media

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

- securing ICT equipment and media in an appropriate security container or secure room
- using ICT equipment without hard drives and sanitising memory at shut down
- encrypting hard drives of ICT equipment and sanitising memory at shut down
- sanitising memory of ICT 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 ICT 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. It should be noted though that there is no guarantee that 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: 5; Updated: Mar-19; Applicability: All; Essential Eight: N/A
ICT equipment and media are secured when not in use.

Further information

Further information on the handling of ICT equipment can be found in the ICT equipment usage section of the *Guidelines for ICT 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, security containers and secure rooms for the protection of ICT equipment can be found in AGD's PSPF, *Physical security for entity resources* policy.