Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Australian Government Information Security Manual

JUNE 2021

Guidelines for Physical Security

Facilities and systems

Certification and accreditation authorities

The certification and accreditation authorities for physical security are outlined in the Attorney-General's Department (AGD)'s ***Protective Security Policy Framework*** (PSPF), ***Entity facilities*** policy.

Facilities containing systems

The application of defence-in-depth to the protection of systems is enhanced through the use of successive layers of physical security. The first layer of security is the use of Security Zones for a facility.

Deployable platforms should meet physical security requirements as per any other system. Notably, physical security certification authorities dealing with deployable platforms may have specific requirements that supersede the security controls in these guidelines. As such, personnel should contact their physical security certification authority to seek guidance.

In the case of deployable platforms, physical security requirements may also include perimeter controls, building standards and manning levels.

Security Control: 0810; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS
Any facility containing a system, including a deployable system, is certified and accredited to at least the sensitivity or classification of the system.

Server rooms, communications rooms and security containers

The second layer in the protection of systems is the use of a higher Security Zone or secure room for a server room or communications room while the final layer is the use of lockable commercial cabinets or security containers. All layers are designed to limit access to people without the appropriate authorisation to access systems at a facility.

Security Control: 1053; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
Servers and network devices are secured in server rooms or communications rooms that meet the requirements for a Security Zone or secure room suitable for their sensitivity or classification.

Security Control: 1530; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS
Servers and network devices are secured in lockable commercial cabinets or security containers suitable for their sensitivity or classification taking into account protection afforded by the Security Zone or secure room they reside in.

Security Control: 0813; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS

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

Security Control: 1074; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
Keys or equivalent access mechanisms to server rooms, communications rooms and security containers are appropriately controlled.

Network infrastructure

While physical security can provide a degree of protection to data communicated over network infrastructure, organisations can have reduced control over data when it is communicated over network infrastructure in areas not authorised for the processing of such data. For this reason, it is important that data communicated over network infrastructure outside of areas in which it is authorised to be processed is appropriately encrypted.

Security Control: 0157; Revision: 6; Updated: Jun-21; Applicability: O, P, S, TS
Data communicated over network infrastructure in areas not authorised for the processing of such data is encrypted as if it was communicated through unsecured spaces.

Controlling physical access to network devices

Adequate physical protection should be provided to network devices, especially those in public areas, to prevent an adversary physically damaging a network device with the intention of interrupting services.

Physical access to network devices can also allow an adversary to reset devices to factory default settings by pressing a physical reset button, connecting a serial interface to a device or connecting directly to a device to bypass any access controls. Resetting a network device to factory default settings may disable security settings on the device including authentication and encryption functions as well as resetting administrator accounts and passwords to known defaults. Even if access to a network device is not gained by resetting it, it is highly likely a denial of service will occur.

Physical access to network devices can be restricted through methods such as physical enclosures that prevent access to console ports and factory reset buttons, mounting devices on ceilings or behind walls, or placing devices in locked rooms or cabinets.

Security Control: 1296; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
Physical security controls are implemented to protect network devices, especially those in public areas, from physical damage or unauthorised access.

Preventing observation by unauthorised people

The inside of facilities without sufficient perimeter security are often exposed to observation through windows. Ensuring systems are not visible through windows will assist in reducing this security risk. This can be achieved by using blinds or curtains on windows.

Security Control: 0164; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
Unauthorised people are prevented from observing systems, in particular, workstation displays and keyboards.

Further information

Further information on encryption can be found in the ***Guidelines for Cryptography***.

Further information on physical security for Security Zones, secure rooms and security containers can be found in AGD's PSPF, ***Entity facilities*** policy, at https://www.protectivesecurity.gov.au/physical/entity-facilities/Pages/default.aspx.

ICT equipment and media

ICT equipment and media register

Maintaining and regularly auditing a register of authorised ICT equipment and media can assist organisations in both tracking legitimate assets and determining whether unauthorised assets have been introduced into a system or its operating environment.

Security Control: 0336; Revision: 4; Updated: Aug-19; Applicability: O, P, S, TS
An ICT equipment and media register is maintained and regularly audited.

Security Control: 0159; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS
All ICT equipment and media are accounted for on a regular basis.

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, 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 (e.g. by 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 circumstances such as an unexpected 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.

Security Control: 0161; Revision: 5; Updated: Mar-19; Applicability: O, P, S, TS
ICT equipment and media are secured when not in use.

Further information

Further information on ICT equipment and media can be found in the fax machines and multifunction devices section of the ***Guidelines for Communications Systems*** as well as in the ***Guidelines for ICT Equipment*** and ***Guidelines for Media***.

Further information on the encryption of media can be found in the ***Guidelines for Cryptography***.

Further information on the storage 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.

Wireless devices and Radio Frequency transmitters

Radio Frequency devices

Many RF devices, such as mobile devices, can pose a security risk to organisations when they are capable of picking up and recording or transmitting background conversations. In highly classified environments, it is important that

organisations understand the security risks associated with the introduction of RF devices and should maintain a register of those that have been authorised for use in such environments.

Security Control: 1543; Revision: 1; Updated: Aug-19; Applicability: S, TS
An authorised RF devices for SECRET and TOP SECRET areas register is maintained and regularly audited.

Security Control: 0225; Revision: 2; Updated: Sep-18; Applicability: S, TS
Unauthorised RF devices are not brought into SECRET and TOP SECRET areas.

Security Control: 0829; Revision: 4; Updated: Mar-19; Applicability: S, TS
Security measures are used to detect and respond to unauthorised RF devices in SECRET and TOP SECRET areas.

Bluetooth and wireless keyboards

While there have been a number of revisions to the Bluetooth protocol that have made incremental improvements to its security over time, there have also been trade-offs that have limited these improvements, such as maintaining backward compatibility with earlier versions of the protocol. While newer versions of the Bluetooth protocol have addressed many of its historical weaknesses, it still provides inadequate security for the communication of sensitive or classified data. As such, sensitive or classification data communicated using Bluetooth will need to be limited to within RF screened buildings.

Security Control: 1058; Revision: 2; Updated: Oct-19; Applicability: O, P, S, TS
Bluetooth and wireless keyboards are not used unless in an RF screened building.

Infrared keyboards

When using infrared keyboards with SECRET systems, drawn curtains that block infrared transmissions are an acceptable method of protection.

When using infrared keyboards with a TOP SECRET system, windows with curtains that can be opened are not acceptable as a method of permanently blocking infrared transmissions.

Security Control: 0222; Revision: 2; Updated: Sep-18; Applicability: O, P
When using infrared keyboards, infrared ports are positioned to prevent line of sight and reflected communications travelling into an unsecured space.

Security Control: 0223; Revision: 4; Updated: Sep-18; Applicability: S
When using infrared keyboards, the following activities are prevented:

- *line of sight and reflected communications travelling into unsecured spaces*
- *multiple infrared keyboards for different systems being used in the same area*
- *other infrared devices being used in the same area*
- *infrared keyboards operating in areas with unprotected windows.*

Security Control: 0224; Revision: 4; Updated: Sep-18; Applicability: TS
When using infrared keyboards, the following activities are prevented:

- *line of sight and reflected communications travelling into unsecured spaces*
- *multiple infrared keyboards for different systems being used in the same area*
- *other infrared devices being used in the same area*
- *infrared keyboards operating in areas with windows that have not had a permanent method of blocking infrared transmissions applied to them.*

Wireless RF pointing devices

As many wireless RF pointing devices used Bluetooth, they along with other wireless RF pointing devices can pose an unacceptable emanation security risk, unless used in an RF screened building.

Security Control: 0221; Revision: 2; Updated: Sep-18; Applicability: TS
Wireless RF pointing devices are not used in TOP SECRET areas unless used in an RF screened building.

Further information

Further information on the use of mobile devices can be found in the ***Guidelines for Enterprise Mobility***.

Further information on the use of Bluetooth devices with mobile devices can be found in the mobile device management section of the ***Guidelines for Enterprise Mobility***.

Further information on wireless networks can be found in the wireless networks section of the ***Guidelines for Networking***.