Australian Government Information Security Manual

Guidelines for physical security

Facilities and systems

Certification and accreditation authorities

Information on 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 certification and accreditation requirements as per any other system. Physical security certification authorities dealing with deployable platforms can have specific requirements that supersede the security controls in this document and, as such, personnel should contact their appropriate 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; Priority: Must
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; Priority: Must
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; Priority: Must
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; Priority: Must
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; Priority: Must
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 information communicated over network infrastructure, organisations can have reduced control over information when it is communicated over network infrastructure in areas not authorised for the processing of such information. For this reason, it is important that information communicated over network infrastructure outside of areas in which it is authorised to be processed is appropriately encrypted.

Security Control: 0157; Revision: 5; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
Information communicated over network infrastructure in areas not authorised for the processing of such information 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; Priority: Must
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 and information 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; Priority: Should
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 using 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/.

ICT equipment and media

Accounting for ICT equipment and media

Maintaining and regularly auditing an inventory 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: 3; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
All ICT equipment and media are registered with a unique identifier in an appropriate register.

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

Securing ICT equipment and media

When not in use, ICT equipment and media should be stored in accordance with its sensitivity or classification. This can be achieved by:

- ensuring ICT equipment and media always resides in an appropriate Security Zone
- storing ICT equipment and media in an appropriate secure room or security container
- using ICT equipment with a removable hard drive which is in an appropriate secure room or security container as well as sanitising the ICT equipment's random-access memory (RAM)
- using ICT equipment without a hard drive as well as sanitising the ICT equipment's RAM
- using encryption software to reduce the physical storage requirements of the hard drive in ICT equipment as well as sanitising the ICT equipment's RAM.

In some circumstances however, it may not be feasible to secure ICT equipment as discussed above. In such cases, the physical storage requirements for ICT equipment can be reduced if appropriate logical controls are applied. This can be achieved by configuring systems to prevent the storage of specific information on hard drives (e.g. storing profiles and work documents on network shares) and enforcing scrubbing of swap files and other temporary data at logoff or shutdown in addition to the practice of sanitising the ICT equipment's RAM.

It should be noted though that there is no guarantee that preventing the storage of specific information on hard drives and scrubbing swap files and other temporary data at logoff or shutdown will always work effectively or will not be bypassed due to circumstances such as an unexpected loss of power. As such, hard drives will retain their sensitivity or classification for the purposes of reuse, reclassification, declassification, sanitisation, destruction and disposal.

Security Control: 0161; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
ICT equipment and media are secured in accordance with their sensitivity or classification.

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 management*** and ***Guidelines for media management***.

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

Wireless devices and Radio Frequency transmitters

Pointing devices

Since wireless RF pointing devices can pose an emanation security risk, they are not to be used in TOP SECRET areas unless in an RF screened building.

Security Control: 0221; Revision: 2; Updated: Sep-18; Applicability: TS; Priority: Must
Wireless RF pointing devices are not used in TOP SECRET areas unless used 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; Priority: Should
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; Priority: Must
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; Priority: Must
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.*

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 information. As such, sensitive or classification information communicated using Bluetooth will need to be limited to within RF screened buildings.

Security Control: 1058; Revision: 1; Updated: Sep-18; Applicability: O, P; Priority: Should
Bluetooth and wireless keyboards are not used unless in an RF screened building.

Security Control: 1155; Revision: 1; Updated: Sep-18; Applicability: S, TS; Priority: Must
Bluetooth and wireless keyboards are not used unless in an RF screened building.

Radio Frequency devices

Many RF devices, such as mobile devices, pose a threat in highly classified areas as they are capable of picking up and recording or transmitting background conversations. Furthermore, many RF devices can connect to ICT equipment and act as unauthorised data storage devices.

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

Security Control: 0829; Revision: 3; Updated: Sep-18; Applicability: S, TS; Priority: Should
Security measures are used to detect active RF devices in SECRET and TOP SECRET areas.

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 network management***.