8.1. Facilities

Objective

8.1.1. Physical security measures are applied to facilities in order to protect systems and their infrastructure.

Context

Scope

8.1.2. This section covers information on the physical security of facilities. Information on physical security controls for servers and network devices, network infrastructure and IT equipment can be found in the following sections of this chapter.

Physical security requirements for storing classified information

8.1.3. Many of the physical controls in this manual are derived from the PSR Policy framework - Physical security (PHYSEC) within the Protective Security Requirements (PSR). In particular from the minimum standard for security containers, secure rooms or lockable commercial cabinets needed for storing classified information.

Secure and unsecure areas

8.1.4. In the context of this manual a secure area may be a single room or a facility that has security measures in place for the processing of classified information, or may encompass an entire building.

Physical security certification authorities

8.1.5. The certification of an agency's physical security measures is an essential part of the certification and accreditation process. The authority and responsibility are listed in the table below:

Classification	Authority	Responsibility
SECRET	CSO	Physical
TOP SECRET	NZSIS	Physical
TOP SECRET SCIF	GCSB	Network Infrastructure Technical Security Surveillance Counter Measures

8.1.6. Top Secret (TS) physical certification should be completed before any Technical inspections and certifications occur.

Facilities located outside of New Zealand

8.1.7. Agencies operating sites located outside of New Zealand can contact GCSB to determine any additional requirements which may exist such as technical surveillance and oversight counter-measures and testing.

References

8.1.8. High-level information relating to physical security is also contained in:

Reference	Title	Publisher	Source
ISO/IEC 27002:2022	**Information security, cybersecurity and privacy protection — Information security controls**	ISO	https://www.iso.org/standard/75652.html

PSR references

8.1.9. Relevant PSR requirements can be found at:

Reference	Title	Source
PSR Mandatory Requirements	GOV2, GOV6, GOV7, INFOSEC1, INFOSEC2, INFOSEC3, INFOSEC4, PHYSEC1, PHYSEC2, PHYSEC3 and PHYSEC4	Home | Protective Security Requirements Security governance (GOV) | Protective Security Requirements Information security (INFOSEC) | Protective Security Requirements Physical security (PHYSEC) | Protective Security Requirements

Rationale & Controls

Facility physical security

8.1.10.R.01. **Rationale**

The application of defence-in-depth to the protection of systems and infrastructure is enhanced through the use of successive layers of physical security.

Typically the layers of security are:

- site;
- building;
- room;
- racks;
- approved containers;
- operational hours; and
- staffing levels.

8.1.10.R.02. **Rationale**

All layers are designed to control and limit access to those with the appropriate authorisation for the site, infrastructure and system. Deployable platforms need to meet physical security certification requirements as with any other system. Physical security certification authorities dealing with deployable platforms may have specific requirements that supersede the requirements of this manual and as such security personnel should contact their appropriate physical security certification authority to seek guidance.

8.1.10.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:1323]

Agencies MUST ensure that any facility containing a system or its associated infrastructure, including deployable systems, are certified and accredited in accordance with the PSR.

Preventing observation by unauthorised people

8.1.11.R.01. **Rationale**

Agency facilities without sufficient perimeter security are often exposed to the potential for observation through windows or open doors. This is sometimes described as the risk of oversight. Ensuring classified information on desks and computer screens is not visible will assist in reducing this security risk.

8.1.11.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:1326]

Agencies SHOULD prevent unauthorised people from observing systems, in particular desks, screens and keyboards.

8.1.11.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:1327]

Agencies SHOULD position desks, screens and keyboards away from windows and doorways so that they cannot be overseen by unauthorised persons. If required, blinds or drapes SHOULD be fixed to the inside of windows, and doors kept closed to avoid oversight.

Bringing non-agency owned devices into secure areas

8.1.12.R.01. **Rationale**

No non-agency owned devices are to be brought into TOP SECRET areas without their prior approval of the Accreditation Authority.

8.1.12.C.01. **Control System Classifications(s): Top Secret; Compliance: Must Not** [CID:1330]

Agencies MUST NOT permit non-agency owned devices to be brought into TOP SECRET areas without prior approval from the Accreditation Authority.

Technical Inspection and surveillance counter-measure testing

8.1.13.R.01. **Rationale**

Technical surveillance counter-measure testing is conducted as part of the physical security certification to ensure that facilities do not have any unauthorised listening devices or other surveillance devices installed and that physical security measures are compatible with technical controls. This testing and inspection will normally occur AFTER the physical site accreditation has been completed (in accordance with the PSR). Further testing may also be necessary after uncleared access to the secure facility, such as contractors or visitors.

8.1.13.C.01. **Control System Classifications(s): Top Secret, Confidential, Secret; Compliance: Must** [CID:1333]

Agencies MUST ensure that technical surveillance counter-measure tests are conducted as a part of the physical security certification.

8.1.13.C.02. **Control System Classifications(s): Confidential, Secret, Top Secret; Compliance: Must** [CID:1334]

Agencies MUST determine if further technical surveillance counter-measure testing is required, particularly if visitors or contractors have entered secure areas.