Australian Communications-Electronic Security Instruction 33 (ACSI 33)

Point of Contact: Customer Services Team

Phone: 02 6265 0197 Email: assist@dsd.gov.au

HANDBOOK 14

PHYSICAL SECURITY

Version 1.0

Objectives

1401. These standards have been developed in conjunction with ASIO T4, and are consistent with the provisions of the Protective Security Manual (PSM). The aim of this handbook, therefore, is to complement the PSM in detailing those physical security issues specific to computer system installations not covered by the PSM. In particular, the standards for "Computer Rooms" are defined in this handbook.

Physical Security and the PSM

1402. Physical security standards for handling and storage of Government information are contained in Volume E of the PSM. In particular, Volume E discusses the following issues in detail:

a. *Principles of Effective Physical Security Practice.* A number of guiding principles are defined to set the basis for a sound approach to physical security protection of identified assets.

b. *Roles and Responsibilities for Physical Security Advice and Standards.* There are several Government agencies whose responsibilities include providing security advice, developing standards, or both.

c. *Framework.* This section of the PSM discusses the application of some key physical security principles. This includes 'security-in-depth', site

planning, accommodation planning, and review and re-evaluation.

d. *Protection of Employees and Clients.* This section addresses the risk factors to personnel safety, the creation of an appropriate security environment, and countermeasures available for the protection of personnel including procedures supporting physical security measures.

e. *Emergency Management.*Emergencies may include natural disasters, bomb threats, failure of essential services, and major accidents.

f. *Physical Protection of Classified Information and Resources.*This section covers those physical security measures specifically designed to protect classified information and other resources. It includes discussions on the risk process, site security plans, and responsibilities for establishing an appropriate environment. It defines security "areas", namely "secure", "partially secure" or "intruder resistant", and defines the provisions for the establishment of such areas. These definitions are important to this handbook, since they will be used to define "Computer Room" standards. This section of the PSM also discusses the storage requirements within the security areas, based on the level of classified information processed within those areas. Finally, some discussion on conference security is also included.

1403. The PSM makes specific reference to the ACSI 33 in establishing a physical security environment for computing equipment which is consistent with that for paper-based information. The fact that computing equipment includes (in most cases) massive electronic storage media, where these media are not able to be removed for after hours storage, means that special physical security countermeasures need to be considered. The PSM physical security standards are directed at the storage of removable media and hardcopy, but are not directly applicable for computer systems. It is therefore the purpose of this handbook to supplement the physical security standards of the PSM, and define standards appropriate for computer systems. These standards are only applicable to Australian sites. Agencies should consult with ASIO T4 on matters relating to the protection of security classified information outside Australia.

Computer Room and Workstation Standards

1404. Computer Room physical security standards are defined, and are labelled as CR1, CR2, CR3 and CR4. The Computer Room physical security standard is designed to supplement the requirements of the PSM, and provide appropriate protection for those rooms containing computer systems that incorporate fixed storage media and/or need to be online on a 24hr basis. The highest standard is the CR1 and the lowest CR4. These Computer Room standards do not provide for any significant fire resistance, however, they may be upgraded to provide this if necessary. Fire resistance requirements are the responsibility of the user organisation. The CR1, CR2 and CR3 standards are classified, and are available from DSD on request for those agencies or organisations with a need to know these standards. The CR4 standard is available at **Annex A**.

1405. Physical security standards for workstations are also included in the CR

definitions, and are labelled as WS1, WS2, WS3 and WS4. These standards are based on whether non-volatile memory is held in the workstation. The WS1, WS2 and WS3 standards are classified, and are available from DSD on request for those agencies or organisations with a need to know these standards. The WS4 standard is available at **Annex A**.

Grades of Physical Security Countermeasures

1406. The combination of Secure Area and Computer Room standards is shown in the table below. The definitions of 'secure', 'partially secure' and 'intruder resistant' are provided in the PSM. The table grades the combination of area security and Computer Room/Workstation into four grades, with Grade 4 being the highest, and Grade 1 the lowest.

Physical Security Grade	Secure Area	Partially Secure Area	Intruder Resistant
Grade 4	CR2 & WS2	CR1 & WS1	No Standard
Grade 3	CR3 & WS3	CR2 & WS2	CR1 & WS1
Grade 2	CR3 & WS3	CR3 & WS3	CR2 & WS2
Grade 1	CR4 & WS4	CR4 & WS4	CR3 & WS3

ANNEX A

CR4 AND WS4 STANDARDS

A1. This Annex describes those standards defined as CR4 and WS4.

Revised August 2000

CR4 STANDARD

a. General. The Computer Room shall be constructed as a single unit with floor, walls and roof to be in accordance with this specification. The walls should not form part of an external wall of the building. The roof, floors and walls should not form part of a common barrier of an adjoining area for which the custodian does not have security control.

b. Door and Door Frame. The door shall be a SCEC endorsed 38mm, flush panel, block timber solid core door. The door shall open out unless a security door is being fitted to the outside for access control during normal working hours. Opening out doors shall be fitted with SCEC endorsed security hinge bolts and a SCEC endorsed lock bolt protector. Door locks

shall be SCEC endorsed double cylinder mortice locks, endorsed for Intruder Resistant Areas. The door locks shall be fitted with SCEC endorsed cylinders suitable for Intruder Resistant Areas. The door frame shall be fabricated from cold formed steel with a minimum thickness of 1.6mm. The door hinges shall be screw fixed to the frame with a minimum of three hinges per door. The door frame shall be permanently fixed to the adjoining wooden wall studs. The door shall be fitted with a heavy-duty, two stage door closer.

c. Air-conditioning. If air-conditioning ducts or other air vents are required then the openings prepared in the wall, roof or floor of the CR4/WS4 Room shall not exceed either 150mm diameter for circular ducts, or 150mm for any one side of rectangular section ducts. General ductwork and other services shall not traverse through the room.

d. Intruder Resistant Area. The area is to be an 'Intruder Resistant Area' in accordance with the Protective Security Manual.

e. Electrical and other wiring. Electrical wiring for power points, lighting, fire and intrusion alarms shall be run in either surface mounted conduit or surface mounted mineral insulated metal sheathed (MIMS) cable. Power points and other like fittings shall be surface mounted.

f. Finish. Both the inner and outer surfaces of secure room walls and the ceiling shall be finished using an appropriate sealer and semi gloss paint applied with a paint roller to provide a light textured finish.

g. Access Control. Access Control may be used for day locking (while the area is occupied). Electronic access control with an entry and exit access audit log is the preferred option. Electronic access control shall not be integrated with the Security Alarm System (SAS).

h. Construction.

h.1. Walls. The walls should extend from the floor to the underside of the above floor slab or secured roof structure.

The walls may be constructed out of either: steel or wooden stud framing clad with gyprock sheeting on both the internal and external faces; single brick/stud veneer; or relocatable office partitioning that is fastened top and bottom on the secure side.

Where the existing walls extend only to a suspended ceiling, the slab-to-slab requirements shall be met by the installation of a suitable barrier between the top of the walls to the above floor slab or secured roof structure. This barrier shall be from AS1304 – 1991, F82 steel reinforcing mesh, and shall be permanently fixed to both the walls and the above floor slab or the roof structure with tamper-proof fasteners.

i. Backup Power (UPS). A backup power supply shall allow for six hours of operations while off mains power supply.

j. Off-Site storage. Premises for the off-site storage of R/IC data and material are also required to meet this construction standard.

WS4 STANDARD

Consideration, based on a risk assessment, should be given to providing physical security countermeasures to protect the workstations and associated storage media, such as hard disks or other non-volatile media. Countermeasures may include, the removal of non-volatile media after hours, physical sealing of the workstation, or protecting the media via logical security means.

A2. If it is considered that any part of this specification is unachievable for site specific reasons, consult ASIO - T4 Protective Security for advice, Ph 02 62341217.

© Copyright Commonwealth of Australia