South Australian Protective Security Framework

# PHYSEC 1

## PHYSICAL SECURITY

# Contents

# POLICY

## PURPOSE

1. Agencies have a responsibility to ensure their people, information, and assets (resources) are protected from harm, including compromise. This policy ensures agencies take the necessary steps to minimise physical security risks to an agency's resources, while also ensuring agencies incorporate protective security requirements into the planning, selection, design, and modification of their facilities.

## CORE REQUIREMENT

**Implement physical security measures that minimise the risk of harm or compromise to people, information and physical assets**

## SUPPORTING REQUIREMENTS

2. To ensure physical security measures minimise the risk of harm or compromise to people, information and physical assets, agencies **must:**[1]

    I. identify and categorise the agency's resources that require a level of physical protection

    II. incorporate protective security in the process of planning, selecting, designing and modifying agency facilities

    III. implement physical security measures proportionate to the assessed business impact of harm or compromise to agency resources, including:

        a. zoning all work areas

        b. applying all required individual control elements

        c. ICT equipment and facilities

    IV. certify and accredit all security zones

        a. ensuring areas where sensitive or security classified information is used, transmitted, stored or discussed are certified in accordance with the applicable ASIO Technical Notes [2]

    V. dispose of physical assets securely

    VI. manage security risks associated with working away from the office

[1] This policy applies to all South Australian public sector agencies (as defined in section 3(1) of the *Public Sector Act 2009*) and to any other person or organisation that is generally subject to the direction of a Minister of the Crown; all of which are referred to in this policy as "Agencies".

[2] ASIO Technical Notes are available via GovTeams. Users will be required to register and request access to the Protective Security Policy community.

# GUIDANCE

## IDENTIFYING AND CATEGORISING RISKS TO PEOPLE, INFORMATION AND PHYSICAL ASSETS

3. South Australian Protective Security Framework (SAPSF) policy Security planning requires agencies to identify the resources that are most important to ongoing operations and therefore, require the greatest level of protection. These protections may be to prevent compromise to those resources, but they **must** also protect them from harm. The physical security measures implemented by each agency to its facilities and physical assets are an essential component of minimising risks of harm or compromise to those resources.

### PEOPLE

4. An agency's people are central to its operations and require protection from harm. This policy reinforces the requirements on agencies pursuant to the *Work Health and Safety Act 2012* to protect its employees and others from harm to their health, safety and welfare through the minimisation of risks, as well as providing support if they experience something harmful or traumatic.

### INFORMATION

5. SAPSF policy Protecting official information outlines the policy and guidance for classifying, accessing and handling information resources. For these requirements to be effective at reducing the likelihood of compromise to an agency's information, the effectiveness of the agency's physical security measures is essential.

### PHYSICAL ASSETS

6. Physical assets are tangible items that are valuable to the agency and require protection to ensure their operability and accessibility, while preventing unauthorised access, use or removal.

7. **Table 1** provides guidance for categorising physical assets, including factors to consider when determining the business impact. The type of physical security measures required or possible will depend upon how the physical asset is categorised by the agency and what the assessed business impact level resulting from compromise would be.

**Table 1 – Categories of physical assets and factors to consider for assessing business impact**

| Category/Description | Factors to consider |
|---|---|
| **Attractive**<br><br>The asset is not necessarily valuable but is desired | • The function of the asset is desirable (e.g., it holds information that may be attractive to an outside party such as a foreign adversary)<br>• Portable assets that can be easily removed without detection, regardless of the information it holds (e.g., mobile phone, tablet) |
| **Classified** | • The level of classification of the asset |

| Category/Description | Factors to consider |
|---|---|
| The asset is classified in its own right or is classified due to the confidentiality of the information held on it (e.g., ICT equipment) | • The mobility and accessibility of the classified asset (e.g. how easily removed or accessible the asset is)<br>• The assessed business impacts that resulted in the security classification |
| **Dangerous**<br>The asset has the potential to cause harm (e.g. weapons or hazardous material) | • The quantity and type of dangerous assets being stored (e.g. bulk store of weapons, large quantities of chemicals that could be weaponised or used to cause harm)<br>• The level of public awareness/concern about the presence of the assets |
| **Important**<br>The significance of the asset's integrity or availability for the agency's operations | • The integrity of the asset (e.g. sensitive data that has not been correctly classified) or<br>• The consequences should the asset be unavailable or inoperable when it is needed (e.g. firefighting equipment, medical supplies) |
| **Significant**<br>The asset has cultural, state, or national significance, regardless of monetary value | • The intrinsic value to the state or national identity<br>• The negative reputational effect of the loss or damage of the asset |
| **Valuable**<br>The asset's monetary value | • The financial viability and time required to replace or repair the asset<br>• The capability of the agency to operate without the asset or with partial functionality<br>• The level of importance the asset has to the agency's function or capability |

8. Business impact should be determined during the agency's security planning processes as required in SAPSF policy Security planning in combination with the Business Impact Level Tool under SAPSF policy Protecting official information. Table 2 includes the business impact levels of compromise or harm to an agency's physical assets.

**Table 2 – Business Impact Levels – compromise or harm to physical assets**

| Business Impact Level | Compromise or harm to resources, including physical assets expected to cause |
|---|---|
| **1**<br>**Low business impact** | Insignificant damage to an individual, organisation or government |
| **2**<br>**Low to medium business impact** | Limited damage to an individual, organisation or government |
| **3**<br>**High business impact** | Damage to individuals, organisations or the state or national interest. |
| **4**<br>**Extreme business impact** | Serious damage to individuals, organisations or the state or national interest. |

| Business Impact Level | Compromise or harm to resources, including physical assets expected to cause |
|---|---|
| **5**<br>**Catastrophic business impact** | Exceptionally grave damage to individuals, organisations or the state or national interest. |

9. Agencies should implement physical security measures that protect each asset for the highest assessed impact, which may include the need for a security classification.[3]
10. It is recommended that agencies implement an asset control system for identifying, protecting, and monitoring physical assets, which increases accountability and protects against theft, damage, and loss. Asset control procedures should include:
    I. recording the location and custodian of assets
    II. periodic auditing or assets
    III. reporting procedures for the loss or damage or assets.

## INCORPORATING PROTECTIVE SECURITY IN THE PROCESS OF PLANNING, SELECTING, DESIGNING AND MODIFYING AGENCY FACILITIES

11. The physical facilities that house an agency's physical resources and assets must be sufficient to afford the level of protection those resources or assets require, in line with the agency's risk assessments and security plans. To reduce the likelihood that an agency's resources or assets are compromised or harmed, agencies must incorporate protective security into all processes for planning, selecting, or designing new facilities as well as refurbishment or modification of existing facilities.
12. Protective security considerations for an agency's facilities should consider:
    I. the location and size of the site
    II. ownership or tenancy of the site (e.g. sole occupancy, shared tenancy, multiple entities)
    III. collateral exposure (e.g. proximity to other categories of physical assets)
    IV. access needs to the site (e.g. authorised personnel only, public access)
    V. security classification of information, activities, and assets (including ICT assets) to be stored, handled or processed in the facility, or parts of the facility
    VI. the categories of other assets stored on site
    VII. periods of greatest or increase risk (e.g. business hours or out-of-hours)

[3] As an example, a human resources database itself may not warrant a security classification, but the information it holds might be essential to the function of the agency, therefore, its category is 'important'. When considering the factors relating to essential assets, the business impact may be assessed as extreme. Therefore, while the database might only be classified to OFFICIAL: Sensitive, the physical protections around it might be greater to ensure the integrity and availability of the information critical to the agency's function.

## SITE SELECTION

13. It is recommended that the ASE and security advisers are involved in assessing:

    I. the suitability of the physical security environment of a proposed site for agency facilities

    II. if the facility can be constructed or modified to incorporate the security measures that will provide the required level of protection.[4]

14. Table 3 – Site selection factors outlines the site selection factors agencies may need to consider.

**Table 3 – Site selection factors**

| Factor | Description |
|---|---|
| **Neighbourhood** | The neighbourhood may present security-related issues, such as local crime activity or risks from neighbouring entities or businesses |
| **Standoff perimeter** | Standoff distance is how much distance can be placed between a facility and an identified threat, such as hostile persons or a vehicle-borne attack. In urban areas, it may be difficult to achieve an effective standoff distance for some threats. It is recommended agencies seek advice where specific or known threats have been identified. |
| **Site access and parking** | The ability and need to control access to pedestrians and vehicles to the site, including the facility itself, parking, and any standoff perimeter. |
| **Building access point** | The ability or need to secure all building access points, including entries and exits, emergency exits, air intakes and outlets and service ducts. |
| **Security zones** | Establishing security zones based upon:<br>• agency risk assessments<br>• business impact levels<br>• security in-depth at the site |
| **Environmental risks** | The risk of natural disasters and potential mitigation strategies |

## DESIGNING AND MODIFYING FACILITIES

15. The design, or modifications to, an agency's facilities must meet the minimum requirements to protect the highest identified risk to the agency's resources.
16. The protection of people, information and assets is achieved via a combination of procedural and physical security measures to prevent or mitigate threats or risks. Table 4 – Outcomes of different security measures contains the relevant security outcomes that can be achieved by different security measures. It is recommended that agencies seek to design or modify facilities with successive layers of physical security which achieve multiple security outcomes.

[4] Physical security measures are designed to reduce the likelihood of security events, the site and design must also accommodate normal business.

**Table 4 - Outcomes of different security measures**

| Factor | Description |
|---|---|
| **Deter** | Measures that are significantly difficult to overcome or require specialist knowledge and tools for adversaries to defeat |
| **Detect** | Measures that identify unauthorised access or actions, either in real time or on review |
| **Delay** | Measures that impede an adversary during attempted entry or attack, or slow the progress of a detrimental event to allow a response |
| **Respond** | Measures that prevent, resist, or mitigate an attack or event when it is detected |
| **Recover** | Measures that help restore operations to normal levels (as soon as possible), or recover lost or stolen resources, following an event. |

## FACILITY SECURITY RISK ASSESSMENT

17. Agencies must, at the earliest point in the design or modification process, identify the protective security requirements[5] of that facility based upon the function and outcomes of a security risk assessment, to enable protective security to be addressed in an effective and efficient manner. When conducting a facility security risk assessment, agencies must consult with Police Security Services Branch (PSSB) Security Support Section where the asset is designated Critical Infrastructure-High Risk (see below).
18. Where a security risk assessment identifies a facility as High Risk, the agency must consult with PSSB to determine the appropriate risk treatments to be applied including whether the facility should be recommended for designation as Critical Infrastructure-High Risk (CI-HR) (see Critical Infrastructure and High-Risk assets).

## IMPLEMENTING SECURITY MEASURES

19. Once the business impact is assessed, the agency must implement physical security measures that are commensurate to the risk identified. Ideally, physical security measures would be capable of achieving all, or at least a combination of, the outcomes listed in **Table 4 – Outcomes of different security measures**.

## SECURITY ZONES

20. Security zones provide a methodology for scaling physical security measures based upon an agency's security risk assessments. There are five security zones, numbered one to five (1-5) with increasing restrictions and access controls as the zones progress.
21. The physical security measures[6] detailed for each zone are designed to protect sensitive and security classified information and security classified assets from compromise, either accidentally, or maliciously.[7]

5 This is included in all relevant ASIO Technical Notes, in particular ASIO Technical Note 1/15 Physical Security of Zones, which is available via GovTeams. Users will be required to register and request access to the Protective Security Policy community

6 As detailed in the applicable ASIO Technical Notes

7 In addition to zoning, agencies may need to consider further physical security measures to protect against blast, ballistic and forced entry in addition to compliance with the Building Code of Australia. See relevant ASIO Technical Notes or more detail.

22. Agencies must consider the sensitivity or security classification of information or assets to be stored or maintained within their facilities to determine the minimum and maximum zone requirements. This process should be informed by SAPSF policies Security planning and Protecting official information. **Annex Table 1 – Security zone descriptions and personnel security clearance requirements** provides a broad description of each security zone, including examples of how the zone might be used, and any security clearance requirements. Agencies must observe the storage requirements for sensitive and security classified information as described in SAPSF policy Protecting official information.

## SECURITY-IN-DEPTH

23. It is recommended that agencies apply the 'security-in-depth' principle to layer their security zones, working in front Zone One public access areas and increasing the levels of protection with each new zone. Multiple layers are a 'delay' design feature to enable more time to detect unauthorised entry and increase the opportunity to respond and prevent compromise or harm**. Figure 1 – Indicative layering of security zones in Annex B** demonstrates indicative layering of zones. In some circumstances, it may not be possible to for higher zones to be fully located within lower zones, and controls may need to be increased.

# INDIVIDUAL CONTROL ELEMENTS

24. The control elements for each security zone are used to achieve the required level of protection. Implementing the control elements provides a level of assurance against:

    I. the compromise, loss of integrity or unavailability of sensitive or security classified information

    II. the compromise, loss, or damage of sensitive or security classified assets.

25. The control elements are based on the ASIO Technical Notes for the minimum requirements to protect sensitive and security classified information and assets. **Annex Table 2 – Physical protections for security zones** provides the individual control elements required in each zone.

## USE OF SECURITY CONSTRUCTION EQUIPMENT COMMITTEE APPROVED PRODUCTS

26. The Security Construction and Equipment Committee (SCEC) is responsible for evaluating security equipment and it determines which product will be evaluated, and the priority of that evaluation.

27. Evaluated products are assigned an increasing security level (SL) rating between 1 and 4 based upon the level of security it has been assessed to provide. SL1 products provide the lowest acceptable level of security for government use.

28. Approved products are listed in the SCEC Security Equipment Evaluated Product List (SEEPL) which is available to government users via the GovTeams Protective Security Policy community.[8]

29. It is recommended for agencies to use SCEC-approved equipment even where it is not mandated. Alternatively, agencies can use suitable commercial equipment that

[8] The SCEC evaluated product list is available via GovTeams. Users will be required to register and request access to the Protective Security Policy community

complies with the identified security related Australian and International Standards for the protection of people, information, and assets.[9]

## SECURITY CONTAINERS AND CABINETS

30. Agencies must identify the need for, and appropriate type of, security cabinets or containers they require to secure information, valuable assets and potentially money. It is recommended agencies consider:
    - the category of asset (see Table 1)
    - the quantity or size of information or assets
    - the location and security zone for the information or physical assets within agency facilities
    - the structure and location of the facility
    - the access control systems
    - other physical protection measures (e.g. locks, alarm systems).
31. It is recommended that sensitive and security classified information and assets are stored in security containers and cabinets separately to physical assets as this can lower the risk of multiple compromises if valuable and/or attractive assets are stolen, while enabling security investigations to be more thorough.

## MANAGING SECURITY CONTAINERS AND CABINETS

32. Security containers and cabinets can be a security risk if not managed appropriately over their lifetime. It is recommended that keys and combinations are kept securely within an agency's perimeter and where possible, in the security zone where the containers and cabinets are located.
33. For containers or cabinets secured with a combination setting, it is recommended that the combination is changed:
    - every six months
    - following repairs
    - following change of employees
    - when there is reason to believe there has been, or may have been, a compromise.

## KEY CABINETS

34. Manual and electronic key cabinets are used to secure keys (e.g. keys for Class C containers or internal offices) and **should** be located within the security zone or in close proximity to the zone where the locks are located. Electronic key cabinets may have automated audit capacity that negates the need to maintain a key register. Electronic key cabinets may also be integrated into the Electronic Access Control System (EACS).
35. The SCEC approved Class B key cabinets provide the same level of protection as SCEC-approved Class B cabinets. SCEC-approved electronic Class C and B key containers are **recommended** to store keys for security zones four, five and Class C

[9] Annex A to PSPF policy Entity Facilities contains a Security Equipment Guide developed by ASIO-T4 to assist agencies select security equipment not tested by SCEC.

containers.[10] Commercial grade key cabinets vary in quality and provide very little protection against forced or covert access.

## SCEC-APPROVED SECURITY CONTAINERS

36. SCEC-approved security containers are for the storage of sensitive and security classified information and assets and not for the storage or valuable, important, attractive, significant, or dangerous assets. The design of these containers provides a high-level of tamper evidence from covert attack, and significantly delay surreptitious attack.

37. There are three levels of SCEC-approved containers:

    I. **Class A** – protects information that has an **extreme** or **catastrophic** business impact level in situations assessed as high risk. These containers can be extremely heavy and **may not** be suitable in some facilities with limited floor loadings.

    II. **Class B** – protects information that has an **extreme** or **catastrophic** business impact level in situations assessed as low risk. They are also used for information that has a **high** or **extreme** business impact in situations assessed as higher risk. These containers are robust filing cabinets or compactuses fitted with combination locks. Class B containers size and weight needs to be considered when selecting a location. There are broadly two types of Class B container:

        a. heavy constructed models that are suitable for use where there are minimal other physical controls

        b. lighter constructed models that are suitable for use where there are other physical security measures

    III. **Class C** – protects information up to an **extreme** business impact level in situations assessed as low risk. They are also used for information that has a **medium** business impact in situations assessed as higher risk by the agency. These containers are fitted with a SCEC-approved restricted keyed lock and are of similar construction to the lighter Class B containers. See **Annex Table 4** of SAPSF policy Protecting official information for guidance on the minimum use and storage requirements for sensitive and security classified information.

## COMMERCIAL SAFES AND VAULTS

38. Commercial safes and vaults provide a level of protection against forced entry. A vault is a secure space that is generally built-in place and normally larger than a safe. A safe is normally smaller and may be portable or movable. The effectiveness of a safe or vault depends on its construction, use and location.

39. Safes and vaults can be fire resistant (for document or data protection), burglar resistant or a combination of the two. It is **recommended** that agencies seek advice from qualified locksmiths or manufacturers when deciding the criteria to apply to select an appropriate commercial safe or vault.[11] **Annex Table 3** provides the

[10] For advice refer to ASIO SEG-013 Electronic Key Cabinets available via GovTeams. Users will be required to register and request access to the Protective Security Policy community.

[11] Further guidance can be found in Australian Standard 3809 Safes and strongrooms and ASIO-T4 Security Equipment Guide SEG-022 Safes-Protection of Assets, which is available via GovTeams. Users will be required to register and request access to the Protective Security Policy community.

minimum commercial safe and vault requirements in the applicable zones, based upon the business impact level.

## VEHICLE SAFES

40. Agencies **may** consider fitting vehicles with field safes to carry valuable assets and official information. Vehicle safes provide some level of protection against opportunistic theft, but only when vehicles are also fitted with other anti-theft controls.

## SECURE ROOM AND STRONGROOMS

41. Secure rooms and strongrooms **may** be used instead of containers to secure large quantities of official information, classified assets and valuable assets, where the compromise or harm would have a high business impact level.
42. Secure rooms are designed to protect its contents from a covert attack and have some degree of fire protection of the contents, if constructed properly. Secure rooms are suitable for open storage of large quantities of official information and classified assets, while maintaining the levels of protection provided by a Class A, B or C container.[12]

## MAGAZINES, ARMOURIES AND EXPLOSIVE STOREHOUSES

43. Advice on magazines, armouries and explosive storehouses is available from the Department of Defence, South Australia Police (SAPOL) Firearms Branch or SafeWork SA's Chemical Hazards & Explosive Materials Team.

## AUDIO SECURITY MEASURES

44. In areas where sensitive or security classified discussions or meetings are held, it is **recommended** agencies implement audio security measures to prevent deliberate or accidental overhearing.
45. Meeting rooms or areas that might be expected to hold such discussions **should** be acoustically treated so that any sound created within the space is unintelligible to a person or device outside that area. Appropriate and effective sound insulation is critical to achieving the required level of security for sensitive and security classified discussions.
46. Consistent with the requirements of this policy, agencies **must** consider the need for sensitive and security classified discussions throughout the processes or planning, selecting, designing, and modifying agency facilities.[13]
47. If sensitive or security classified discussions need to be held in unsecured or untreated areas, agencies are **recommended** to take all available steps to reduce the likelihood that those conversations are overheard, including moving away from public spaces and/or work areas.

## SECURITY ALARM SYSTEMS

48. Security Alarm Systems (SAS) provide detection or unauthorised access to an agency's facilities. SAS are only effective, however, if used in conjunction with other measures designed to delay or respond to that unauthorised access.

---

[12] Advice on construction specification for secure and strongrooms is detailed in the ASIO Technical notes 7-06 Class A Secure Room, 8-06 Class B Secure Room and 9-06 Class C Secure Room available via GovTeams. Users will be required to register and request access to the Protective Security Policy community.

[13] ASIO Technical Note 1/15 – Physical Security of Zones, Section 16: Audio Security is available via GovTeams. Users will be required to register and request access to the Protective Security Policy community.

49. All South Australian Government agencies **must** obtain SAS monitoring services through Police Security Services Branch (PSSB).[14] Client Connection Forms and processes for alarm connections and modifications can be obtained by emailing SAPOLPSSBControlCentre@police.sa.gov.au.

50. It is **recommended** that SAS are configured to monitor high-risk areas (e.g., infrequently accessed, roof spaces, inspection hatches and underfloor cavities).

51. Agencies **must** undertake periodic maintenance and testing on SAS from an authorised service provider. It is **recommended** that maintenance and testing occur at least every two years to ensure all systems are operational.

52. SAS can be broadly divided into two types:

    - perimeter (external) intrusion detection systems (PIDS) or alarms
    - internal security alarm systems

## PERIMETER ALARMS

53. PIDS **may** be of value to agencies that have facilities enclosed within a perimeter fence or for facilities located on a large land holding. PIDS provide detection of unauthorised breaches of the perimeter. Agencies are **recommended** to seek specialist advice when installing PIDS. The SEEPL contains suitable and approved external alarm components.

## INTERNAL ALARMS

54. It is **recommended** that a combination of commercial and SCEC-approved SAS be used to protect an agency's facilities, after consideration of the zone requirements and the agency's risks assessment.

55. SAS can be single sector or sectionalised to give coverage to specific areas of risk. Sectionalised SAS allow greater flexibility as highly sensitive areas can remain secured when not in use, but other parts of the facility are open.

56. SAS in zones Three, Four and Five **must** be sectionalised, unless the agency opts to use separate SAS across each different security zone.

## ZONES FOUR AND FIVE

57. If an agency determines it has need for a Zone Four or Zone Five area, they **must** use:

    I. a SCEC-approved Type 1A or Type 1 SAS in accordance with the Type 1A SAS transition policy with SCEC-approved detection devices[15]

    II. SCEC-endorsed Security Zone Consultant to design and commission the SCEC-approved Type 1A alarm system.[16]

14 PSSB SAS monitoring services comprises the centralised monitoring of SAS including duress, intruder and critical systems failure

15 The transition policy is available via GovTeams. Users will be required to register and request access to the Protective Security Policy community.

16 The SCEC Security Zone Consultant Register on the SCEC website lists SCEC-endorsed Security Zone Consultants by state and territory. SCEC-endorsed Security Zone Consultants are endorsed to provide physical security advice at the request of government agencies regarding:

- design, acceptance testing and commissioning of Type 1A SAS
- design and construction of security zones as defined in the SAPSF and ASIO-T4 Technical Notes.

## COMMERCIAL ALARM SYSTEMS

58. Commercial alarm systems are graded on the level of protection they provide. The AS/NZS 2201.1 levels of security alarm systems include:

    I. Class 1 or 2 are only suitable for domestic use

    II. Class 3 or 4 are suitable for the protection of normal business operations in most agencies

    III. Class 5 is suitable for protection of information and physical assets up to an **extreme** business impact level.

59. Agencies **must** only use commercial alarm systems up to Zone Three. It is **recommended** that agencies consider and determine:

    I. whether a commercial alarm system is appropriate for agency facilities (including temporary sites)

    II. the SAS specifications required.

60. Agencies **should** have procedures in place for the use, management, monitoring and response arrangements of commercial alarm systems. It is **recommended** that agencies adopt the administration and management principles set out in the Type 1 security alarm system Implementation and Operation Guide.

61. It is **recommended** that agencies seek to integrate any SAS with other building management systems, such as duress, intruder and critical systems failure alarms, closed-circuit television (CCTV) and electronic access control systems, to reduce the vulnerabilities of unauthorised access and tampering.

## SECURITY GUARDS

62. Security guards can provide a both a physical presence at agency facilities and a rapid response to security incidents. Stationary guards or guard patrols **may** be useful, either separately or in conjunction with other security measures. It is **recommended** that security guard response time be less than the delay given by the total of all other individual control elements, especially if guards are off-site.

63. In considering the use of security guards, it is **recommended** that agencies consider:

    I. the level of threat and/or risk identified

    II. whether guards need to be on-site or off-site (on-site provides higher level of assurance)

    III. any security clearance requirements based on the security zone requirements and frequency of access[17]

    IV. ensuring guards hired are licenced in South Australia.

## CRITICAL INFRASTRUCTURE AND HIGH-RISK ASSETS

64. Critical infrastructure assets are physical facilities, supply chains, information technologies and communications networks which, if destroyed, disrupted, degraded, or rendered unavailable for an extended period will significantly impact on the social

[17] See SAPSF policy Accessing official information for more guidance.

or economic well-being of the State, or affect the State's contribution to National security or defence.

65. Critical Infrastructure-High Risk (CI-HR) assets are *designated by Cabinet* following the endorsement of a recommendation made to the State Emergency Management Committee (SEMC) following a security risk assessment conducted by PSSB and the relevant agency(ies). These assets are those which if destroyed, disrupted, degraded, harmed or rendered unavailable would significantly affect the reputation of the State or significantly reduce community confidence in the Government's ability to effectively conduct business.
66. A recommendation to designate an asset as CI-HR is undertaken by the relevant agency(ies) through the following process:
    - Consult with PSSB to determine the appropriateness of designation
    - Undertake or validate an existing security risk assessment of the asset
    - Identify appropriate risk treatments aligned with the security risk assessment, including the need for deployment of Police Security Officers (PSOs)
    - Prepare a report for SEMC with a recommendation for designation, including resource and funding implications for the agency
67. SEMC will consider the report and recommendation made by the agency. If endorsed, the report will be returned to the agency who will be responsible for drafting a Cabinet Submission. Cabinet will consider the proposal and recommendation for designation of the asset as CI-HR. The Commissioner of Police (delegated to PSSB) will maintain a secure register of designated CI-HR assets.
68. Agencies **must** conduct security risk assessments and site reviews of any designated CI-HR asset in consultation with PSSB. It is **recommended** that reviews are undertaken every 2-3 years. Where any changes are proposed to the designation of a CI-HR asset, the relevant agency is to prepare a report for consideration by SEMC. A copy of each risk assessment and site review **must** be provided to PSSB.
69. Following designation, the agency(ies) responsible for the CI-HR asset **must** obtain protective security services from PSSB, comprised of:
    I. monitoring of electronic security devices such as closed-circuit television (CCTV)
    II. physical security services including: security advice, support and training, mobile and static security, and alarm response services provided by PSOs.
70. PSOs are employees of and remain under the operational management of SAPOL. PSOs will be deployed and subject to the conditions of contractual agreements between SAPOL and the relevant agency. PSOs are deployed to agencies on a cost recovery basis which will be outlined in the relevant contract.
71. Agencies **may** obtain protective security services from PSSB relating to assets not designated CI-HR.

## PROTECTED PERSONS, PLACES AND VEHICLES

72. Information regarding determinations by the Minister that specified persons, places or vehicles are in need of protective security can be found under Section 63B(1)(b) of the *Police Act 1998* (SA) should be sought from PSSB.
73. Following a designation of CI-HR by Cabinet, the agency responsible for the asset **must** make application to the Minister for Police to declare the site a *'protected place'* under the Act.

# SECURITY SIGNAGE

74. It is **recommended** that agencies install security signage that supports physical security and mayact as to deter intruders or adversaries where:

    I. CCTV is installed

    II. required pursuant to the *Police Act 1998* (SA) relative to protected persons, places and/or vehicles deemed in need of protection by the Minister. [18]

# ACCESS CONTROL SYSTEMS

75. Access control systems are measures that allow authorised personnel, vehicles, and equipment to pass through protective barriers while preventing unauthorised access. Forms of access control can be:

    I. security guards located at entry and exit points

    II. security guards located at central points who monitor and control entry and exit points using intercoms, videophones and CCTV

    III. mechanical locking devices operated by keys or codes

    IV. electronic access control systems

    V. psychological or symbolic barriers (e.g., signage or crime prevention through environmental design).[19]

## AUTHORISED PERSONNEL ACCESS

76. Access to Zones Two to Five **must** be restricted to authorised personnel. This includes:

    I. agency employees (including those on contract or seconded staff) who require access to agency facilities, information or assets (see SAPSF policy Recruiting employees)

    II. personnel engaged by contracted service providers who need access to agency facilities, information or assets as covered by the terms of the contract (see SAPSF policy Managing the security of contractors and service providers)

    III. personnel who, due to business need (although not directly engaged by the agency or contracted service provider) require ongoing access that is authorised by the accountable authority (e.g., Senior Executives or personnel from another portfolio agency who require regular, unescorted access to attend meetings etc.).

77. The accountable authority (or Agency Security Executive (ASE)) is **responsible for** authorising ongoing (or regular) access for people who are not directly engaged or covered by the terms of a contract or agreement. The accountable authority (or ASE) **must** ensure:

    I. the person has the required level of security clearance required for the respective security zones they **may** need to access

    II. the appropriate business need (e.g., a documented business case and risk assessment).

[18] PSSB can provide signage to an agency or advise on the required wording where an agency wishes to design its own

[19] **May** be used for deterrence but are **not recommended** as an effective access control measure.

## ELECTRONIC ACCESS CONTROL SYSTEMS (EACS)

78. EACS **must** be used for Zones Three to Five where there are no other suitable identity verification and access control measures in place. Zones Three to Five **must:**

    I. have sectionalised access control systems and full audit

    II. be regularly reviewed for unusual or prohibited activity or access.

79. It is **recommended** that agencies:

    I. seek specialist advice when selecting and designing EACS

    II. use an appropriate installer recommended by the manufacturer to install and commission the systems

    III. regularly audit all EACS across all agency security zones in accordance with their risk assessments and security plan and identify and remove personnel no longer requiring ongoing access.

## IDENTITY CARDS

80. Identity cards allow recognition of personnel across agency facilities. Agencies **must** use identity cards with personal identity verification in Zones Three to Five, however, it is **recommended** that agencies use identity cards across all facilities, regardless of the level of security zone.
81. Identity cards **should** only be issued to employees or people who have had their identity established as per the requirements of SAPSF policy Recruiting employees. It is **recommended** that agencies use the National Identity Proofing Guidelines to at least Level 3 for personnel not covered by the SAPSF policies (such as contracted service providers). It is also **recommended** agencies consider implementing this standard in Zones One and Two also.
82. Identity cards **should** be:

    I. uniquely identifiable

    II. worn and clearly displayed by authorised personnel while on agency premises

    III. regularly audited in accordance with the agency's risk assessments and security plan.

83. Identity card making equipment and spare, blank, or returned cards, **should** be secured within a Zone Two or higher zone, based on the security risk assessment.

## AUTHENTICATION FACTORS

84. There are three authentication factors that can be used to validate identity:

    I. What you have (e.g., keys, identity cards, passes)

    II. What you know (e.g., pin numbers, passwords)

    III. What you are (e.g., visual recognitions, biometrics)

85. It is **strongly recommended** agencies implement dual factor authentication within all agency facilities (e.g., factors from two different categories above). Agencies **must** use dual factor authentication for access to Zone Five areas.

## VISITOR CONTROLS

86. A visitor is any person who does not have authorised ongoing access to all or part of an agency's facilities. Visitor control is an administrative process but can be supported by EACS.
87. Agencies **must** control access to Zones Three to Five, which **should** include recording visitor details and issuing visitor passes. Visitor registers **should** record name, agency, or entity they represent, purpose of visit, person responsible for the visit, and date and time of entry and exit. It is **recommended** visitor access processes are also implemented for Zone Two areas.
88. Visitor passes **should** be:
    I. visible at all times
    II. collected and disabled at the end of the visit
    III. audited regularly (e.g., daily)
    IV. if EACS is available, visitor passes **should** be enabled only for the areas the visitor requires access to.
89. It is **recommended** that specific or sensitive areas have separate visitor registers and processes in place at the entry.
90. Visitors **must** be escorted at all times in Zones Three to Five, and it is **recommended** visitors are also escorted in Zone Two areas, unless unescorted access is approved.
91. Regardless of the entry control method or other controls in place, it is **recommended** that unescorted access only be given if the person:
    I. has a legitimate need for unescorted access to the area
    II. has the appropriate level security clearance (if required)
    III. is able to show a suitable form of identification.

## PERIMETER ACCESS CONTROL

92. Perimeter access control **may** be required for agencies with larger, multi-building facilities. Perimeter control can increase the level of deterrence, detection, and delay. Some types of perimeter control include:
    I. fences and walls to define the perimeter[20]
    II. pedestrian barriers and/or entry/exit points
    III. vehicle security barriers.
93. The level of protection provided by a fence or wall depends on the height, construction, materials, access controls and any other features to increase its performance or effectiveness (e.g., lighting, signage, SAS). It is **recommended** that

[20] Refer to the ASIO-T4 Security Equipment Guide SEG-003 Perimeter Security Fences and SEG-024 Access Control Portals and Turnstiles, available for authorised security personnel only from the Protective Security Policy community on Govdex. Related Australian Standards:

- AS 1725–Chain-link fabric security fencing and gates
- AS/NZS 3016–Electrical installations–Electric security fences.

entry and exit points are at least as strong as the fence or wall used. The SEEPL contains details on perimeter intrusion detection devices.

## LOCKS AND DOOR HARDWARE

94. Locks can deter or delay unauthorised access to information and physical assets. It is **recommended** that all access points are secured, including doors and windows, using commercial-grade or SCEC-approved locks and hardware. Agencies **must** use SCEC-approved locks and hardware in Zones Three to Five.

95. Locks **may** be electronic, combination or keyed, and all combinations, keys and electronic tokens **should** be assigned the same classification as the highest classification of information or asset secured by that lock.

96. All agencies are **recommended** to consider the level of protection required by doors frames when selecting locks, as they are only as strong as their fittings or hardware. It is also **recommended** that agencies:

    I. Use SCEC-endorsed locksmiths when using SCEC-approved locks (list available from ASIO-T4 and SCEC)

    II. Use doors that provide a similar level of protection to the locks and hardware fitted; refer to Australian Standard AS 3555.1–Building elements–Testing and rating for intruder resistance–Intruder-resistant panels.[21]

## KEYING SYSTEMS

97. Restricted keying systems provide a level of assurance to agencies that unauthorised duplicate keys have not been made. Controls for keying systems include:

    I. legal controls (e.g., registered designs and patents)

    II. level of difficulty in obtaining or manufacturing key blanks and the machinery used to cut duplicate keys

    III. levels of protection against compromise techniques, such as picking, impressioning and decoding.

98. It is **recommended** that when selecting keying systems, agencies evaluate:

    I. the level of protection provided against common forms of compromise

    II. the extent of legal protection offered by the manufacturer

    III. supplier protection of agency keying data within their facilities

    IV. the transferability of the system and any associated costs

    V. commissioning and ongoing maintenance costs.

99. The number of master keys should be strictly limited as the loss of a master key may result in the need to re-key all the locks under that master. Key control measures should include regular auditing of key registers to confirm the location of all keys in accordance with the agency's risk assessments and security plan.

[21] This standard is now expired and has not yet been superseded. Advice from Commonwealth Attorney-General's Department is that the guidance in the standard remains correct until a new standard has been issued.

100. Key cabinets should be located within a facility's secure perimeter and, where possible, within the perimeter of the zone where the locks are located.

## TECHNICAL SURVEILLANCE COUNTERMEASURES

101. TSCMs are implemented to protect security classified discussion from technical compromise. It is recommended that agencies undertake TSCM inspections to assist in identifying any technical weaknesses or vulnerabilities within agency facilities that may be used for security classified discussions.

102. TSCM inspections should be carried out:

I. at the conclusion of initial construction, room renovations or alterations to fittings (e.g., lighting and furnishings)

II. as a part of programmed technical security inspections undertaken at random intervals

III. before an event (e.g., where visitors may enter the area)

IV. following a security breach (e.g., unauthorised disclosure of a sensitive discussion).

103. Agencies seeking advice on TSCM inspections can contact ASIO-T4 for more information and assistance. Requests can be made in accordance with the Protective Security Circular No 165 Facilitating TSCM inspections in Australia, available for authorised security personnel only from the Protective Security Policy community on GovTeams.

## CLOSED CIRCUIT TELEVISION

104. CCTV may be used as a visual deterrent to unauthorised access, theft or violence and can assist in post-incident investigations and alarm activation investigations. CCTV must not be used as a substitute for physical barriers.

105. For CCTV to be effective, agencies **should** install a sufficient number of cameras to monitor:

I. the entire perimeter of the tenanted area or building, particularly publicly accessible areas such as reception, lobby, or entry points

II. all facility access points, including car park entrances

III. public access hallways, stairwells, and lift lobbies

IV. inside loading docks

V. public area boundaries (e.g., the delineation between public areas and security zones).

106. CCTV images from security incidents to be used in investigations **should** be security stored in an appropriate security container to protect the evidentiary integrity.

## SECURITY LIGHTING

107. Internal and external lighting is an important contributor to physical security. It can act as a deterrent to intruders, illuminate areas to meet requirements for CCTV, assist response teams when responding to security incidents and provide safety lighting for personnel in car parks and building entrances. Motion-detecting devices **may** be useful to activate additional lighting as a further deterrent.

# ICT EQUIPMENT AND FACILITIES

## ICT EQUIPMENT

108. ICT equipment facilitates the electronic processing, storage, and transfer of agency information. The equipment itself **must** be protected due to:
    I. the classification or business impact of the information held on the asset, or the classification of the asset itself
    II. the criticality of integrity or availability of the information held or processed on the asset
    III. the potential attractiveness of either the information held of the asset itself
    IV. the aggregation of information, which may increase the business impact level of the asset's compromise.

109. ICT equipment includes:
    I. movable physical assets (e.g., computers, photocopiers, multi-function devices, mobile phones, storage media etc.)
    II. system equipment (e.g., hardware and software)
    III. building management systems and security systems.

110. ICT system equipment is generally operational 24-hours a day, which may include:
    I. servers
    II. communication network devices (e.g., PABX systems)
    III. supporting network infrastructure (e.g., cabling)
    IV. gateway devices (e.g., routers, network access devices.

111. To identify the appropriate physical security measures to protect ICT assets or the information held or communicated on them, it is **recommended** that the protections align with the highest business impact level of that information.

112. Additional physical security measures for specific types of ICT equipment are contained in **Annex A: Table 4**.

## ICT FACILITIES

113. An ICT facility is a designated space or floor of an agency's building used to house the agency's ICT systems, components of the ICT systems or ICT equipment. These facilities include:
    I. server and gateway rooms
    II. datacentres
    III. backup repositories
    IV. storage areas for ICT equipment that hold official information
    V. communication and patch rooms.

114. All agencies **must** certify[22] and accredit any security zone that is to hold sensitive or security classified information.[23] It is **recommended** that agencies locate ICT

[22] Compartments within the Zone Five may be certified by the ASE or delegated security adviser
[23] Agencies must ensure any TOP SECRET information ICT facilities are in compartments with a Zone Five area accredited by ASIO-T4 and comply with all applicable ASIO Technical Notes. Agencies must also obtain ASIO-T4 physical security certification for outsourced ICT facilities to hold information that, if compromised, would have a

facilities in security zones that are specific to the facility and are separate to other agency functions.

115. The physical security of containers or rooms housing ICT equipment in an ICT facility **may** sometimes be lowered if the ICT facility is a separate security zone within an existing security zone suitable for the information held. This process is consistent with the 'security-in-depth principle (See **Annex A: Table 5** for more detail).

## ACCESS CONTROL TO ICT FACILITIES AND EQUIPMENT

116. If the business impact is lower than **catastrophic**, agencies **may** consider the following control to limit access to ICT facilities:

    I. a dedicated section of the SAS, or an EACS

    II. personnel at the entrance administering access to authorised people

117. It is also **recommended** that agencies seal access to ICT equipment within ICT facilities by using SCEC-approved tamper-evident wafer seals suitable for application to hard surfaces. These seals give a visual indication of unauthorised access to equipment if the seals are removed or broken. See the SEEPL for SCEC-approved seals.

## SECURING ICT EQUIPMENT WHEN NOT IN USE

118. ICT equipment not in use of unattended **must** be secured commensurate with the classification or business impact level of the information held or the asset itself. It is **recommended** that any movable equipment is secured in an appropriate security zone and that out-of-hours, all security containers, and the ICT facility itself are secured from unauthorised access.

119. For ICT equipment that cannot be secured in ICT facilities, security containers or secure rooms when not in use, it is **recommended** that agencies:

    I. remove non-volatile media (hard drives) and, if possible, store in an appropriate container

    II. store ICT equipment where the non-volatile media cannot be removed in an appropriate security zone (see **Annex A: Table 1**)

    III. seek advice from the ASD about additional logical or technological solutions that may be available to lower the risk of compromise.

# SECURITY ZONE CERTIFICATION AND ACCREDITATION

120. Certification and accreditation are measures to increase the level of confidence in the ability of an agency to share, access and protect information according to the required protections. As such, agencies are **required to** certify and accredit their security zones in accordance with the requirements of the SAPSF and relevant ASIO Technical Notes.

## CERTIFICATION

121. Certification of security zones establishes each zone's compliance with the minimum physical security requirements to the satisfaction of the relevant certification authority. For Zones One to Four, the ASE (or delegated security adviser) may certify that the control elements have been implemented and are

catastrophic business impact level. See ASIO Protective Security Circular PSV 149 Physical Security Certification of Outsourced ICT facilities for more detail.

operating effectively.[24] **Annex A: Table 6** summarises the certification authorities for the relevant control measures.

## ACCREDITATION

122. Accreditation of security zones involved compiling and reviewing all applicable certifications and other deliverables for the zone to determine and accept the residual security risks. Approval for the security zone to operate at the desired level is granted for a specified time. For Zones One to Five, the ASE (or delegated security adviser) is the accrediting authority when the controls are certified as meeting the requirements of **Annex A: Table 6**.[25]

## RECERTIFICATION AND REACCREDITATION

123. Security zone certification is time-limited and compliance is based upon the facility and the assets contained at the time of certification. As such, facilities **must** be recertified and reaccredited by circumstances including:

    I. expiry of the certification due to the passage of time

        a. 10 years for Zone Two

        b. 5 years for Zones Three to Five

    II. changes in the assessed business impact level associated with the sensitive or security classified information or assets handled or stored with in the zone

    III. significant changes to the architecture of the facility or the physical security controls used

    IV. any other conditions stipulated by the accreditation authority, such as changes to the threat level or other environmental factors of concern.

# DISPOSAL OF PHYSICAL ASSETS

124. An agency's physical resources **may** need to be disposed of due to a number of factors (e.g. advances in technology, end of life cycle, changes to business requirements). All agencies **must ensure disposal of physical assets is secure and minimises risk to the South Australian Government.**

125. Prior to decommissioning or disposing of physical assets, such as security containers, cabinets, vaults, strongrooms, and secure rooms, it is **recommended** that agencies:

    I. reset combination locks (electronic and mechanical) to factory settings

    II. visually inspect and remove all contents from the physical assets.

126. Secure disposal of ICT equipment **may** be achieved through sanitisation, in accordance with the Australian Government Information Security Manual (ISM). In some circumstances, ICT equipment cannot be sanitised and will required destruction.

127. See SAPSF policy Protecting official information for advice on appropriate methods of destruction for South Australian Government information and resources.

[24] Compartments within the Zone Five may be certified by the ASE or delegated security adviser

[25] The Australian Signals Directorate must accredit Zone Five facilities used to secure and access sensitive compartmented information and sensitive compartmented information facilities (SCIF). ASD is responsible for management of all SCIFs in Australia. Recertification and reaccreditation of Zone Fives and SCIFs, it is recommended to seek advice from ASIO-T4.

# WORKING AWAY FROM THE OFFICE

128. Agencies **must** consider the security measures required to enable employees to work securely away from the office, while managing any security risks that arise (e.g. the environment where the work is being undertaken, the type or sensitivity of the work being undertaken etc.)

## MOBILE COMPUTING AND COMMUNICATIONS

129. Mobile computing and communication involved creating access to agency systems and information from locations outside of the agency's control using portable devices. Most areas being used for mobile work arrangements are public areas with few, or no, protective security measures in place, and would therefore be rated no greater than a Zone One security area. As such, it is **recommended** that agencies implement mobile computing and communications controls to minimise any residual risk, such as requiring that all employees and personnel maintain positive control (not left unattended) at any time.

130. As it **may not** be possible to implement appropriate zoning requirements away from the office, agencies **should** consider ICT logical security controls to protect their information and assets. Advice on suitable logical controls can be found in the ISM.

## TELEWORKING

131. Teleworking allows employees and other personnel to undertake work away from the office from alternate locations. Examples of teleworking include:

    I. working from personal residences on a regular basis

    II. working from an alternate office space:

        a. within agency facilities in another location (e.g. regional sites)

        b. in another Australian, state or territory government's facilities

        c. in another location where the agency has some ability to apply protective security (e.g. contracted service provider's premises)

132. Most teleworking locations will not be greater than a Zone Two security zone, and agencies **must** consider appropriate security measures to minimise any residual risk.

## PROTECTING RESOURCES WHILE WORKING AWAY FROM THE OFFICE

133. Agencies **must** maintain the protections of their resources commensurate with the assessed business impact level of compromise. Where possible, agencies **should** accredit proposed work sites outside of the office in line with the type of work expected to be undertaken. In determining the viability of work away from the office, agencies **must** consider:

    I. if sensitive or security classified information can be appropriately secured 26

    II. if the workspace can be independently secured

    III. if the workspace can be protected from oversight or overhearing by other people

[26] The minimum protections of SAPSF policy Protecting official information for sensitive and security classified information **must** be maintained. ASIO-T4 certification **must** also be sought for any areas used to store **TOP SECRET** information.

IV. if the ICT equipment being used can be secured or segregated from the agency's ICT system.

134. An agency's physical assets are vulnerable to loss or compromise outside of government facilities. It is **recommended** that agencies consider:

I. asset control procedures

II. limiting the removal of agency assets from the office to only those absolutely necessary

III. the need for portable alarm systems in private residences.[27]

## SECURITY OF RESOURCES IN FACILITIES NOT MANAGED BY THE AGENCY

135. It **may** be difficult to secure an agency's information that is being held in facilities or areas not controlled by the originating agency. These areas could include commercial facilities, private residences, or a service provider's premises. It is **recommended** that agencies consider all areas outside of the agency's control as Zone One, unless it is able to confirm and certify any security measures in place that would indicate otherwise.

[27] Refer to ASIO-T4 Protective Security Circular 162 Private residence security assessment, available for authorised security personnel only from the Protective Security Policy community on Govdex.

# DOCUMENT CONTROL

| | |
|---|---|
| Approved by: Chief Executive, Department of the Premier and Cabinet | Date of first approval: 20 April 2020 |
| Revision number: 2.0 | Date of review: 26 October 2022 |
| Next review date: December 2024 | Contact person: sapsf@sa.gov.au |

# CHANGE LOG

| Version | Date | Changes |
|---|---|---|
| 1.0 | 20/04/2020 | First issue of policy |
| 1.1 | 21/08/2020 | Definition of 'personnel' updated |
| 2.0 | 26/10/2022 | Updated guidance added to Facility Security Risk Assessments (para 17)<br>Updated guidance added to Security Alarm Systems (para 48)<br>Updated guidance added to Critical Infrastructure High and-Risk Assets (paras 64-70)<br>Guidance added to Protected persons, places and vehicles (paras 70-71)<br>Guidance added to Security Signage (para 73) |

# ANNEX A: TABLES

## ANNEX A: TABLE 1 - SECURITY ZONE DESCRIPTIONS AND PERSONNEL SECURITY CLEARANCE REQUIREMENTS

| Security Zone | Description (included permitted use and storage) | Security clearance requirements | Examples |
|---|---|---|---|
| **Zone One** | **Public access areas**[28]<br>**a.** Information and assets classified up to and including OFFICIAL: Sensitive, with a business impact of low to medium that are needed to do business may be used and stored<br>**b.** Information and assets classified PROTECTED, or with a high business impact may be used. Storage is not recommended but is permitted if unavoidable.<br>**c.** Information and assets classified SECRET or higher, or with a business impact of extreme, may only be used in exceptional circumstances with prior approval from originating or owning entity. Storage is not permitted. | No security clearance requirements for accessing Zone One. Employment screening for employees is sufficient.<br>Personnel accessing or using security classified information in Zone One must hold a security clearance at the appropriate level for the information and assets being used or stored in the zone. | • Building perimeter and public foyers.<br>• Interview and front desk areas where there is no segregation of authorised personnel from clients and the public.<br>• Out-of-office temporary work areas where the agency has no control over access.<br>• Fieldwork, including most vehicle-based work.<br>• Exhibition areas with no security controls. |
| **Zone Two** | **Agency office areas**<br>Restricted public access. Unrestricted access for authorised personnel. May use single factor authentication for access control.<br>**a.** Information and assets classified up to and including PROTECTED, or with a business impact up to high, may be used and stored.<br>**b.** Information and assets classified SECRET, or with a business impact of extreme, may be used, but not normally stored. Storage is not permitted without prior approval from the originator or owner.<br>**c.** Information and assets classified TOP SECRET, or with a business impact of catastrophic, may only be used in exceptional circumstances to meet operational imperatives with prior approval from originating or owning agency. Storage is not permitted. | Minimum requirements for ongoing access to Zone Two are determined by the agency's risk assessments.<br>If security classified information and assets are stored in the zone, a security clearance at the appropriate level for the information and assets being used or stored in the zone is required for ongoing access.<br>Ongoing access may be given to personnel without the appropriate security clearance or holding a lower-level security clearance following a risk assessment. | • Agency office environments<br>• Out-of-office or home-based worksites where the agency has control of access to the part of the site used for agency business.<br>• Airside work areas.<br>• Interview and front-desk areas where there is segregation of authorised personnel from clients and the public.<br>• Court houses<br>• Vehicle-based work where the vehicle is fitted with a security container, alarm, and immobiliser |
| **Zone Three** | **Agency restricted office areas**<br>No public access. Visitor access only for visitors with a need-to-know and with close escort.<br>Restricted access for authorised personnel. Single factor authentication for access control.<br>a. Information and assets classified up to and including SECRET, or with a business impact up to extreme, may be used and stored.<br>b. Information and assets TOP SECRET, or a business impact of catastrophic, may be used, but not normally stored. Use and storage is not permitted without prior approval from the originator or owner. Storage must not exceed five consecutive days. | If security classified information and assets are stored in the zone, a security clearance at the appropriate level for the information and assets being used or stored in the zone is required for ongoing access. | Security areas within agency premises with additional access controls on authorised personnel<br>Work area where the majority of work performed is up to PROTECTED and there is a limited requirement for personnel to have a clearance at the Negative Vetting Level 1. For example, non-National security agencies. |
| **Zone Four** | **Agency restricted office areas**<br>No public access. Visitor access only for visitors with a need-to-know and with close escort.<br>Restricted access for authorised personnel who hold an appropriate security clearance. Single factor authentication for access control.<br>a. Information and assets classified up to and including SECRET, or with a business impact up to extreme, may be used and stored. | If security classified information and assets are stored in the zone, a security clearance at the appropriate level for the information and assets being used or stored in the zone is required for ongoing access. | Security areas within agency premises with additional access controls on authorised personnel.<br>Work areas where all personnel are required to be cleared at the Negative Vetting Level 1 due to the classification of work performed in the zone. |

| | | | |
|---|---|---|---|
| | b. Information and assets classified TOP SECRET, or with a business impact of catastrophic, may be used, but not normally stored | | |
| **Zone Five** | **Agency highly restricted office areas**<br>No public access. Visitor access only for visitors with a need-to-know and with close escort.<br>Restricted access for authorised personnel who hold an appropriate security clearance.<br>Dual authentication for access control.<br>a. Information and assets classified up to and including TOP SECRET, or with a business impact of catastrophic, may be used and stored. | Ongoing access to the zone must only be given to personnel holding a security clearance at the appropriate level for the information and assets stored in the zone. | • Highest security areas in agency premises<br>• Australian Intelligence Community facilities |

## ANNEX A: TABLE 2 - PHYSICAL PROTECTIONS FOR SECURITY ZONE

| Control Element | Zone One | Zone Two | Zone Three | Zone Four | Zone Five |
|---|---|---|---|---|---|
| **Building Construction** | In accordance with agency risk assessment | In accordance with applicable sections of ASIO Technical Note 1/15 – Physical Security of Zones.<br>**<u>When only used during business hours</u>**<br>Normal construction to the Building Code of Australia.<br>**<u>When also used out of business hours</u>**<br>Normal construction and:<br>a. slab-to-slab construction, or<br>b. tamper-evident ceilings, or<br>c. applicable sections of ASIO Technical Note 1/15 – Physical Security of Zones. | In accordance with applicable sections of ASIO Technical Note 1/15 – Physical Security of Zones.<br>For protection of valuable physical assets, recommend aligning building construction with level 4 (or above) of the Australian Standard 3555.1. In such cases, construction will be considered to meet minimum security zone protections mandated by this policy. | As for Zone Three. | Construction complies with:<br>a. ASIO Technical Note 1/15 – Physical Security of Zones<br>b. b. ASIO Technical Note 5/12 – Physical Security of Zone 5 (TOP SECRET) areas. |
| **Perimeter doors and hardware** | | | | | |
| **a. doors** | In accordance with agency risks assessment. | Constructed in accordance with ASIO Technical Note 1/15 – Physical Security Zones | As for Zone Two | As for Zone Two | Constructed in accordance with ASIO Technical Note 5/12 – Physical Security Zones (TOP SECRET) areas. |
| **b. locks** | In accordance with agency risks assessment. May use commercial locking system. | As for Zone One. | Minimum SCEC-approved SL3 locks and hardware. | As for Zone Three | As for Zone Three |
| **c. Keyring systems** | Recommend SCEC-approved SL1 or SL2 keying system. | As for Zone One. | SCEC-approved minimum SL3 keying system. | As for Zone Three | As for Zone Three |
| **Out-of-hours security alarm system (SAS)** | In accordance with agency risk assessment. | In accordance with agency risk assessment. In an office environment, recommend Class 3-4 SAS[29] hard wired in the zone. | Type 1 SAS, or Class 5 SAS[30] hard wired in the zone. If no SAS, guard patrols performed at random intervals within every four hours required. | Use in accordance with the Type 1A SAS transition policy:<br>a. for new or significantly expanded sites, SCEC-approved Type 1A SAS with SCEC approved detection devices (designed and commissioned by SCEC-endorsed Security Zone Consultants)<br>b. for existing sites, SCEC Type 1 SAS with SCEC-approved detection devices. | As for Zone Four |
| **a. detection devices** | In accordance with agency risk assessment | Hard wired within the zone. Recommend SCEC approved SL2 or SL3 detection devices | As for Zone Two. | SCEC-approved SL3 or SL4 detection devices. | As for Zone Four |

| | | | | | |
|---|---|---|---|---|---|
| **b. SAS contractor clearance requirements** | In accordance with agency risk assessment | Contractors who maintain these systems provided with short term access to security classified resources[31] at the appropriate level for the information stored within the zone | As for Zone Two | Contractors who maintain these systems cleared at the appropriate level for the information stored within the zone. | As for Zone Four |
| **c. Management of security alarm systems** | In accordance with agency risk assessment | As for Zone One. | Control of alarm systems directly managed by the agency.<br>Privileged alarm systems operators and users appropriately trained and security cleared to the level of the security zone.<br>All alarm system arming and disarming personal identification numbers are secure | As for Zone Three | As for Zone Three |
| **d. Monitoring and response** | All alarm systems to be monitored and responded to in a timely manner. Response capability appropriate to the threat and risk. | As for Zone One | As for Zone One | As for Zone One | As for Zone One |
| **Interoperability of alarm system and other building management system** | In accordance with agency risk assessment | In accordance with agency risk assessment.<br>If a separate SAS and EACS are used, ensure the alarm cannot be disabled by the access control system. | Ensure the alarm cannot be disabled by the access control system. | Ensure limited one-way interoperability in accordance with the Type 1 SAS for Australian Government—Product Integration specification. | Ensure limited one-way interoperability in accordance with the Type 1 SAS for Australian Government—Product: Integration specification.<br>The alarm system may disable access control system when activated. |
| **Access control systems** | In accordance with agency risk assessment | In accordance with agency risk assessment.<br>Recommend using identity access card in office environments. | Use identity card and sectionalised access control systems.<br>Use Electronic Assess Control Systems (EACS) where there are no other suitable verification and access control measures in place.<br>Verify the identity of all personnel, including contractors, issued with EACS access cards at the time of issue (using the National Identity Proofing Guidelines to a minimum level 3).<br>Regularly audit EACS. | As for Zone Three, with full audit trail of access control systems.<br>Directly managed and controlled by the entity.<br>Maintained by appropriately cleared contractors Privileged operators and users are appropriately trained and security cleared to the level of the security zone.<br>Regularly audit EACS | As for Zone Four, with full audit trail of access control systems and dual authentication. |
| **Technical surveillance countermeasures (TSCM)** | No requirement | No requirement | As determined by a risk assessment | As for Zone Three | TSCM and audio security inspection:<br>a. for areas where TOP SECRET discussions are regularly held, or the compromise of other discussions may have a catastrophic business impact level<br>b. before conferences and meetings where TOP SECRET discussions are to be held<br>Seek advice from ASIO-T4 and refer ASIO Technical Note 5/12 Physical Security of Zone Five (TOP SECRET) areas. |

| | | | | | |
|---|---|---|---|---|---|
| **Visitor control** | In accordance with agency risk assessment | In accordance with agency risk assessment. Recommended to record visitors, issue passes and escort in sensitive areas. | Visitor and contractor access only for visitors with a need to know and with close escort.<br>Recommend providing receptionists and guards with:<br>• detailed auditable visitor control and access instructions<br>• secure method of calling for immediate assistance if threatened. | As for Zone Three and visitor and contractor access with a need to know and with close escort with constant line of sight. | As for Zone Four. |

## ANNEX A: TABLE 3 - BUSINESS IMPACT LEVELS COMMERCIAL SAFES AND VAULTS

| Business Impact Level | 1<br>Low | 2<br>Low to medium | 3<br>High | 4<br>Extreme | 5<br>Catastrophic |
|---|---|---|---|---|---|
| **Zone One** | Determined by an agency risk assessment, locked commercial container recommended | Determined by an agency risk assessment, locked commercial container recommended | AS 3809 commercial vault or safe | AS 3809 high security safe or vault | Not to be held unless unavoidable |
| **Zone Two** | Determined by an agency risk assessment, locked commercial container recommended | Determined by an agency risk assessment | Commercial safe or vault | AS 3809 medium security safe or vault recommended | Not to be held unless unavoidable |
| **Zone Three** | Determined by an agency risk assessment | Determined by an agency risk assessment | Determined by an agency risk assessment, locked commercial container recommended | AS 3809 commercial vault or safe | AS 3809 high or very high security safe or vault recommended |
| **Zone Four** | Determined by an agency risk assessment | Determined by an agency risk assessment | Determined by an agency risk assessment | Commercial safe or vault recommended | AS 3809 medium or high security safe or vault recommended |
| **Zone Five** | Determined by an agency risk assessment | Determined by an agency risk assessment | Determined by an agency risk assessment | Commercial safe or vault recommended | AS 3809 medium or high security safe or vault recommended |

## ANNEX A: TABLE 4 - PHYSICAL SECURITY FOR SPECIFIC TYPES OF ICT EQUIPMENT

| Specific ICT Equipment | Physical Security Requirement |
|---|---|
| **Solid state drives or hybrid hard drives** | Solid state drives and hybrid drives cannot be made safe through normal data wiping processes when switched off. It is recommended that agencies using equipment with these drives seek advice from ASD on methods to secure this equipment (e.g. encryption) |
| **Deployable ICT systems** | Physical security measures may be difficult to apply when using deployable ICT systems, particularly in high-risk environments. It is recommended that agencies seek advice from ASD on suitable controls to help mitigate any risks from using deployable systems |
| **Network infrastructure** | Protection of network infrastructure requires a combination of physical security measures and system encryption. If the encryption used is approved by ASD, the physical security requirements can be lowered in accordance with the Australian Government Information Security Manual (ISM). For information on the protection of network infrastructure, see SAPSF policy Robust ICT and cyber security.<br><br>Tampering of network infrastructure is a security risk. It is recommended that agencies secure network infrastructure equipment (e.g. patch panels, fibre distribution panels and structure wiring enclosures in containers and secure rooms. If this is not possible, it is recommended that agencies meet the system encryption requirements of the ISM. |
| **ICT system gateway devices** | Unauthorised access to gateway devices is a security risk. It is recommended that gateway devices are located within dedicated ICT facilities. Guidance for securing ICT system gateway devices is available in the ISM. |

## ANNEX A: TABLE 5 - BUSINESS IMPACT LEVELS – STORAGE REQUIREMENTS FOR ELECTRONIC INFORMATION IN ICT FACILITIES

| Business Impact Level of aggregated electronic information | Physical Security zone of work area | Security container or secure room ordinarily required | Additional security zone within work area for ICT facility | Security container or secure room required for ICT equipment |
|---|---|---|---|---|
| **1**<br><br>**Low** | Zone Two | Lockable commercial cabinet | No additional zone required | Lockable commercial cabinet |
| | Zone One | Lockable commercial cabinet | Zone Two or above | Lockable commercial cabinet |
| **2**<br><br>**Low to medium** | Zone Two | Lockable commercial cabinet | No additional zone required | Lockable commercial cabinet |
| | Zone One | SCEC Class C | Zone Two or above | Lockable commercial cabinet |
| **3**<br><br>**High** | Zone Three of above | SCEC Class C recommended for Zone Three. Lockable commercial cabinet for Zones Four and Five | No additional zone required | SCEC Class C recommended for Zone Three. Lockable commercial cabinet for Zones Four and Five |
| | Zone Two | SCEC Class C | Zone Three or Above | Lockable commercial cabinet |
| | | | Zone Two | SCEC Class C |
| **4**<br><br>**Extreme** | Zone Four | SCEC Class C | Zone Three of above | Lockable commercial cabinet |
| | | | Zone Two | SCEC Class C |
| | Zone Three | SCEC Class B | Zone Four or above | Lockable commercial cabinet |
| | | | Zone Three | SCEC Class C |
| | | | Zone Two | SCEC Class B |
| **5**<br><br>**Catastrophic** | Zone Five | SCEC Class B | Compartment (certified by ASE) | SCEC Class C |

## ANNEX A: TABLE 6 - SUMMARY OF CONTROL MEASURES AND CERTIFICATION AUTHORITY

| Control Measure | Zone One | Zone Two | Zone Three | Zone Four | Zone Five |
|---|---|---|---|---|---|
| **Agency specific threat assessments** | ASE (or security adviser) if the need is identified in the risk assessment | ASE (or security adviser) if the need is identified in the risk assessment | ASE (or security adviser) if the need is identified in the risk assessment | ASE (or security adviser) if the need is identified in the risk assessment | ASE (or security adviser) if the need is identified in the risk assessment |
| **Agency security risk assessment** | ASE (or security adviser) | ASE (or security adviser) | ASE (or security adviser) | ASE (or security adviser) | ASE (or security adviser) |
| **Site security plan** | ASE (or security adviser) | ASE (or security adviser) | ASE (or security adviser) | ASE (or security adviser) | ASE (or security adviser) |
| **SCEC-approved Type 1A** | N/A | N/A | N/A | SCEC-endorsed security zone consultant (regular servicing by authorised provider required)[28] | SCEC-endorsed security zone (regular servicing by authorised provider required)[29] |
| **SCEC-approved Type 1 SAS** | SCEC-endorsed security zone consultant[30] [31] [32](regular servicing by authorised provider required) | SCEC-endorsed security zone consultant [25] [28](regular servicing by authorised provider required) | SCEC-endorsed security zone consultant [25] [28](regular servicing by authorised provider required) | SCEC-endorsed security zone consultant [25] (regular servicing by authorised provider required) | SCEC-endorsed security zone consultant [25] (regular servicing by authorised provider required) |
| **Commercial alarm system** | Suitably qualified system installer or designer [27] (regular servicing by authorised provider required) | Suitably qualified system installer or designer [27] [28] (regular servicing by authorised provider required) | Suitably qualified system installer or designer [28] (regular servicing by authorised provider required) | N/A | N/A |
| **Electronic access control system[33]** | Suitably qualified system installer or designer, (current software patches and no obsolete components required) | Suitably qualified system installer or designer, (current software patches and no obsolete components required) | Suitably qualified system installer or designer, (current software patches and no obsolete components required) | Suitably qualified system installer or designer, (current software patches and no obsolete components required) | Suitably qualified system installer or designer, (current software patches and no obsolete components required) |
| **Other zone requirements** | ASE (or security adviser) | ASE (or security adviser) | ASE (or security adviser) | ASE (or security adviser) | ASE (or security adviser) |

[28] SCEC-endorsed security zone consultants design and commission SCEC Type1A SAS and SCEC Type 1 SAS in accordance with the requirements of the Type 1 SAS Implementation and Operation Guide
[29] SCEC-endorsed security zone consultants design and commission SCEC Type1A SAS and SCEC Type 1 SAS in accordance with the requirements of the Type 1 SAS Implementation and Operation Guide
[30] Inclusion of an alarm system or EACS in Zones One and Two are at the agency's discretion.
[31] Out-of-hours guard patrols or commercial alarm systems are not used instead.
[32] SCEC-endorsed security zone consultants design and commission SCEC Type1A SAS and SCEC Type 1 SAS in accordance with the requirements of the Type 1 SAS Implementation and Operation Guide
[33] Inclusion of an alarm system or EACS in Zones One and Two are at the agency's discretion

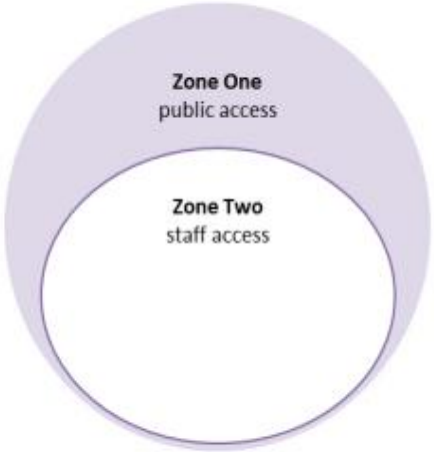
| | | | | | |
|---|---|---|---|---|---|
| **Certification (including site inspection)** | ASE (or security adviser) | ASE (or security adviser) | ASE (or security adviser) | ASE (or security adviser) | ASIO-T4 |

# ANNEX B: FIGURES

## FIGURE 1: INDICATIVE LAYERING OF SECURITY ZONES


Entity with all business impact levels


Entity with low-to-medium business impact levels and high public interaction




Entity with high business impact levels


Entity with mostly extreme to catastrophic business impact levels


Entity with potentially difficult clients or valuable assets


Facility where all public access is controlled at the outer perimeter



Government
of South Australia