

Table 3 Physical protections for security zones—level of assurance required for sharing of sensitive and security classified information and assets

| Control element | Zone One | Zone Two | Zone Three | Zone Four | Zone Five |
|---|--|---|--|--|--|
| Building construction | In accordance with entity risk assessment. | <p>In accordance with applicable sections of ASIO Technical Note 1/15 – Physical Security of Zones.ⁱ</p> <p><u>When only used during business hours</u> Normal construction to the Building Code of Australia.</p> <p><u>When also used out of business hours</u> Normal construction and:</p> <ol style="list-style-type: none"> slab-to-slab construction, or tamper-evident ceilings, or applicable sections of ASIO Technical Note 1/15 – Physical Security of Zones. | <p>In accordance with applicable sections of ASIO Technical Note 1/15 – Physical Security of Zones.</p> <p>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.</p> | As for Zone Three. | <p>Construction complies with:</p> <ol style="list-style-type: none"> ASIO Technical Note 1/15 – Physical Security of Zones ASIO Technical Note 5/12 – Physical Security of Zone 5 (TOP SECRET) areas. |
| Perimeter doors and hardware | | . | | | |
| a. Doors | In accordance with entity risk 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 entity risk assessment. May use commercial locking systems. | As for Zone One. | Minimum SCEC-approved SL3 locks and hardware. | As for Zone Three. | As for Zone Three. |
| c. Keying 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 entity risk assessment. | <p>In accordance with entity risk assessment.</p> <p>In an office environment, recommend Class 3-4 SAS ^{Note ii} hard wired in the zone.</p> | <p>Type 1 SAS, or Class 5 SAS ^{Note ii} hard wired in the zone.</p> <p>If no SAS, guard patrols performed at random intervals within every four hours required.</p> | <p>Use in accordance with the Type 1A SAS transition policy:</p> <ol style="list-style-type: none"> 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) for existing sites, SCEC Type 1 SAS with SCEC-approved detection devices. | As for Zone Four. |
| a. Detection devices | In accordance with entity 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 entity risk assessment. | Contractors who maintain these systems provided with short term access to security classified resources ^{Note iii} 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 entity risk assessment. | As for Zone One. | <p>Control of alarm systems directly managed by the entity.</p> <p>Privileged alarm systems operators and users appropriately trained and security cleared to the level of the security zone.</p> <p>All alarm system arming and disarming personal identification numbers are secure.</p> | As for Zone Three. | As for Zone Three. |

| Control element | Zone One | Zone Two | Zone Three | Zone Four | Zone Five |
|--|--|--|--|---|--|
| 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 entity risk assessment. | In accordance with entity risk assessment. 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. The alarm system may disable access control system when activated. |
| Access control systems | In accordance with entity risk assessment. | In accordance with entity risk assessment. Recommend using identity access card in office environments. | Use identity card and sectionalised access control systems. Use Electronic Assess Control Systems (EACS) where there are no other suitable verification and access control measures in place. 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). Regularly audit EACS. | As for Zone Three, with full audit trail of access control systems. Directly managed and controlled by the entity. Maintained by appropriately cleared contractors Privileged operators and users are appropriately trained and security cleared to the level of the security zone. Regularly audit EACS. | As for Zone Four, with full audit trail of access control systems and dual authentication. |
| Technical surveillance counter-measures (TSCM) | No requirement. | No requirement. | As determined by a risk assessment. | As for Zone Three. | TSCM and audio security inspection: a. for areas where TOP SECRET discussions are regularly held, or the compromise of other discussions may have a catastrophic business impact level b. before conferences and meetings where TOP SECRET discussions are to be held c. 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 entity risk assessment. | In accordance with entity 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. Recommend providing receptionists and guards with: a. detailed auditable visitor control and access instructions b. 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. |

Table 3 notes:

ⁱ Access to ASIO Technical Notes is available to Australian Government security personnel via the PSPF community on [GovTEAMS](#).

ⁱⁱ Australian Standard [AS/NZS 2201.1](#) provides guidance on alarm systems.

ⁱⁱⁱ Refer to PSPF policy: [Access to information](#) for guidance on short term access to security classified resources.