

Table 2 Security zone descriptions and personnel security clearance requirements for the protection of sensitive and security classified information and assets

Security zone	Security zone description, including permitted use ^{Note i} and storage ^{Note ii} of sensitive and security classified resources	Personnel security clearance requirement for access to the resources stored in the zone	Examples
Zone One	<p>Public access areas. (The inner perimeter of Zone One may move to the building or premise perimeter out-of-hours if exterior doors are secured.</p> <ul style="list-style-type: none"> a. Sensitive and security classified information and assets with a business impact level of low to medium that are needed to do business may be used and stored. b. Sensitive and security classified information and assets with business impact level of high may be used. Storage is not recommended but is permitted if unavoidable. c. Sensitive and security classified information and assets with a business impact level greater than high may only be used under exceptional circumstances and requires the approval of the originating or owning entity. No storage is permitted. 	Employment screening sufficient, security clearance not required.	<ul style="list-style-type: none"> a. Building perimeters and public foyers. b. Interview and front-desk areas where there is no segregation of authorised personnel from clients and the public. c. Out-of-office temporary work areas where the entity has no control over access. d. Fieldwork, including most vehicle-based work. e. Exhibition areas with no security controls.
Zone Two	<p>Entity office areas. Restricted public access. Unrestricted access for authorised personnel. May use single factor authentication for access control.</p> <ul style="list-style-type: none"> a. Sensitive and security classified information and assets with a business impact level up to high may be used and stored. b. Sensitive and security classified information and assets with a business impact level of extreme may be used, but not normally stored in the zone. No storage of these assets is permitted without originator's approval. c. Sensitive and security classified information and assets with business impact level of catastrophic may only be used under exceptional circumstances to meet operational imperatives and requires the originator's approval. No storage is permitted. 	<p>Minimum requirements for ongoing access to the security zone are determined by an entity risk assessment.</p> <p>If security classified information and assets are stored in the zone, a security clearance is required for ongoing access at the level required for the highest classified resources the individual will access in the zone.</p> <p>Ongoing access to the zone can be given to individuals without a security clearance or holding different levels of security clearances.</p>	<ul style="list-style-type: none"> a. Entity office environments. b. Out-of-office or home-based worksites where the entity has control of access to the part of the site used for entity business. c. Airside work areas. d. Interview and front-desk areas where there is segregation of authorised personnel from clients and the public. e. Court houses. f. Vehicle-based work where the vehicle is fitted with a security container, alarm and immobiliser.
Zone Three	<p>Entity restricted office areas. No public access. Visitor access only for visitors with a need to know and with close escort. Restricted access for authorised personnel. Single factor authentication for access control.</p> <ul style="list-style-type: none"> a. Sensitive and security classified information and assets with a business impact level up to extreme may be used and stored. b. Sensitive and security classified information with a business impact level of catastrophic may be used, but not normally stored, in the zone. Use and storage of catastrophic information requires the originators approval. Temporary storage may be permitted up to five consecutive days. 	<p>Minimum requirements for ongoing access to the security zone are determined by an entity risk assessment.</p> <p>If security classified information and assets are stored in the zone, a security clearance is required for ongoing access at the level required for the highest classified resources the individual will access in the zone.</p> <p>Ongoing access to the zone can be given to individuals without a security clearance or holding different levels of security clearances.</p>	<ul style="list-style-type: none"> a. Security areas within entity premises with additional access controls on authorised personnel. b. 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 entities.
Zone Four	<p>Entity restricted office area. No public access. Visitor access only for visitors with a need to know and with close escort. Restricted access for authorised personnel with appropriate security clearance.</p> <ul style="list-style-type: none"> a. Single factor authentication for access control. Sensitive and security classified information with business impact levels up to extreme may be used and stored. b. Sensitive and security classified information with a business impact level of catastrophic may be used, but not normally stored in the zone. 	<p>If security classified information and assets are stored in the zone, a security clearance is required for ongoing access at the level required for the highest classified resources stored in the zone.</p> <p>Ongoing access is given to individuals who hold the same level of security clearance for the information and assets stored in the zone.</p>	<ul style="list-style-type: none"> a. Security areas within entity premises with additional access controls on authorised personnel. b. 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.
Zone Five	<p>Entity highly restricted office area. No public access. Visitor access only for visitors with a need to know and with close escort. Restricted access for authorised personnel with appropriate security clearance. Dual authentication for access control.</p> <ul style="list-style-type: none"> a. Information classified TOP SECRET or 	<p>Security clearance required for ongoing access at the level required for the highest security classified information and assets stored in the zone.</p> <p>Ongoing access is given to individuals who hold the same level of security</p>	<ul style="list-style-type: none"> a. Highest security areas in entity premises. b. Australian Intelligence Community facilities.

	other information with a business impact level of catastrophic may be used and stored. ^{Note iii}	clearance for the information and assets stored in the zone.
--	--	--

Table 2 notes:

- ⁱ Use of information includes handling, processing and discussions.
- ⁱⁱ For advice on containers applicable for storage of information with the identified business impact level in each zone see the PSPF policy: [Sensitive and classified information](#).
- ⁱⁱⁱ Mandated in **Requirement 8b** for Zone Five areas used to access sensitive compartmented information, the space must achieve ASIO-T4 Zone Five physical security certification and ASD Sensitive Compartmented Information Facility Accreditation.