15 Physical security for entity resources

A. Purpose

1. This policy describes the physical protections required to safeguard people (consistent with the requirements of the *Work Health and Safety Act 2011*), information and assets (including ICT equipment) to minimise or remove security risk.

B. Requirements

B.1 Core requirement

Each entity must implement physical security measures that minimise or remove the risk of:

- ***a. harm to people, and***
- ***b. information and physical asset resources being made inoperable or inaccessible, or being accessed, used or removed without appropriate authorisation.***

B.2 Supporting requirements

2. The supporting requirements help entities identify the resources that need protection and the level of physical security measures required to protect resources appropriately.

Supporting requirements for physical security for entity resources

#	Supporting requirements
Requirement 1. Physical security measures	Entities **must** put in place appropriate physical security measures to protect entity resources, commensurate with the assessed business impact level of their compromise, [Note i] loss or damage.
Requirement 2. Security containers, cabinets and rooms	Entities **must** assess security risks and select the appropriate containers, cabinets, secure rooms and strong rooms to protect entity information and assets.
Requirement 3. Disposal	Entities **must** dispose of physical assets securely.

Supporting requirements notes:

[i] Information compromise is defined in PSPF policy: Sensitive and classified information.

C. Guidance

C.1 Identifying resources

3. 'Resources' is the collective term for people, information and assets that entities use in their operations. PSPF policy: Security planning and risk management requires entities to identify the people, information and assets that are critical to the ongoing operation of the entity and the national interest and apply appropriate protections to support core government business.

C.1.1 People

4. An entity's personnel, including contractors, are central to its operations, and require protection. The WHS Act provides the framework to safeguard the health and safety of workers and workplaces.
5. Protective security elements of the WHS Act framework and other appropriate legislative frameworks include:
    a. identifying, protecting and supporting employees under threat of violence, based on a threat and risk assessment of specific situations
    b. reporting incidents to management, human resources, security and law enforcement authorities, is encouraged as appropriate
    c. providing information, training and counselling to employees
    d. maintaining thorough records and statements on reported incidents.
6. To support compliance with the WHS Act, the Attorney-General's Department recommends entities implement appropriate physical security measures to ensure the personal security of their personnel, while working in the office and away from the office. Refer to PSPF policy: Entity facilities.

C.1.2 Information

7. Information is a valuable resource and requires protection. PSPF policy: Sensitive and classified information details policy and guidance on classification and handling arrangements for protecting information resources.

C.1.3 Physical assets

8. Physical assets are tangible items that are valuable to an entity and require protection. This protection includes ensuring their continued operability and accessibility, as appropriate, and preventing any unauthorised access, use or removal.
9. Physical assets can be categorised as follows:
    a. Valuable - the asset's monetary value
    b. Classified - the asset is classified in its own right or is classified due to the confidentiality requirements of the information held on the asset, for example ICT equipment
    c. Important - the significance of the asset's integrity or availability for the entity's operations
    d. Attractive - the asset is not necessarily valuable but is desired, for example an iPad
    e. Significant - the asset has cultural or national significance, regardless of monetary value
    f. Dangerous - the asset's likelihood to inflict harm, for example weapons or chemical, biological, radiological and nuclear hazards.
10. The protections required for, and that can effectively be applied to, different physical assets will be affected by the category of asset and the business impact level of the compromise, loss or damage of the asset, as described below.

C.1.3.1 Asset control for physical assets

11. Asset control assists entities to identify their asset holdings and is an accountability mechanism that protects against theft, damage and loss. Asset control procedures may include:
    a. recording the location and authorised custodian of assets
    b. periodic auditing of assets
    c. reporting requirements for the loss or damage of assets.
12. Due to their intrinsic value, the Attorney-General's Department recommends entities implement appropriate asset control for identified physical assets. Entities may, as a result of their risk assessment, consider that more frequent audits are appropriate for higher risk assets for example valuable assets, attractive assets and assets of cultural significance.

C.2 Identifying the physical security measures required to protect entity resources

13. The core requirement mandates that entities implement physical security measures to minimise the risk of resources being made inoperable or inaccessible, or being accessed, used or removed without proper authorisation. The Attorney-General's Department recommends that entities protect their resources by using a combination of physical and procedural security measures to achieve this outcome. These include measures to:

    a. Deter - measures that cause significant difficulty or require specialist knowledge and tools for adversaries to defeat

    b. Detect - measures that identify unauthorised action is being taken or has already occurred

    c. Delay - measures to impede an adversary during attempted entry or attack, or slow the progress of a detrimental event to allow a response

    d. Respond - measures that prevent, resist or mitigate an attack or event when it is detected

    e. Recover - measures to restore operations to normal levels (as soon as possible) following an event.

14. In accordance with **Requirement 1**, entities must put in place appropriate physical security measures to protect entity resources, commensurate with the assessed business impact level of their compromise, loss or damage.

15. Entities determine the business impact level as part of the security risk assessment process for managing the risks associated with protecting entity resources (refer PSPF policy: Security planning and risk management). **Table 1** Business impact levels for physical assets describes, the level of damage or impact on business operations that could result from any compromise, loss or damage of physical assets. The PSPF policy: Sensitive and classified information **Table 1** details the business impact levels relating to compromise of the confidentiality of information.

Table 1 Business Impact Levels—compromise, loss or damage of physical assets[1]

Business impact level	1 Low business impact	2 Low to medium business impact	3 High business impact	4 Extreme business impact	5 Catastrophic business impact
Compromise, loss or damage of physical assets	Compromise, loss or damage of assets could be expected to cause **insignificant damage** to an individual, organisation or government.	Compromise, loss or damage of assets could be expected to cause **limited damage** to an individual, organisation or government.	Loss or damage of assets would be expected to cause **damage** to the national interest, organisations or individuals.	Compromise, loss or damage of assets would be expected to cause **serious damage** to the national interest, organisations or individuals.	Compromise, loss or damage of assets would be expected to cause **exceptionally grave damage** to the national interest, organisations or individuals.

16. Once the entity has assessed the business impact level of the compromise, loss or damage of identified resources, entities establish the commensurate security measures required to achieve effective protection by considering the type, quantity and size of the resources to be protected. When determining the physical security measures required to protect entity resources, the Attorney-General's Department recommends that entities also consider that the cost of the security measures is proportionate to the mitigation of the identified risks within the entity's agreed risk tolerance.

C.2.1 Determining the level of physical security measures for the protection of physical assets

17. Categorising physical assets can support entities to identify and consider factors that are relevant to assessing the business impact level of the compromise, loss or damage of the asset—factors that could

[1] Prior versions of the PSPF included the business impact level of 'significant business impact'. For reference, this level (3A) is provided at **Annex A**.

influence that assessment might include, for example, the desirability of the asset or its level of classification. In turn, this will assist in determining the level and types of protection to apply.

18. Table 2 describes the categories of assets and provides a number of factors to consider when assessing and determining the business impact level of the compromise, loss or damage of those types of asset.

Table 2 Categories of assets and factors to consider when assessing and determining business impact levels

Asset category	Factors to consider when assessing and determining business impact levels
Valuable assets	a. The financial viability and lead-time to replace or repair the asset. b. The capability of the entity to operate without the asset or with partial functionality of the asset. c. The percentage of overall capability to which the asset contributes.
Classified assets	a. The level of classification of the asset. b. The mobility and accessibility of the classified asset, for example, heavy military equipment. c. For assets classified due to the confidentiality requirements of information they hold, see the PSPF policy: Sensitive and classified information, business impact level tool that provides examples of potential damage due to compromise of information.
Important assets	a. The integrity of the asset, for example, data with no classification such as human resources data or geographical data for aviation. b. The availability of the asset for example a ground transport fleet or firefighting equipment.
Attractive assets	a. The desirability of the asset related to its function, for example a physical asset holding information that may be attractive to a foreign adversary. b. Portable assets that are desirable, regardless of the information stored on them, for example an iPad.
Significant assets	a. The intrinsic value to the national identity. b. The negative reputational effect of the loss or damage of the asset.
Dangerous assets	a. The bulk stores of weapons, such as firearms, explosives and ammunition. b. The quantities of hazardous materials that could be weaponised or used to cause harm.

19. The Attorney-General's Department recommends that entities determine the business impact level of the compromise, loss or damage of the asset in accordance with **Table 2** and adopts the necessary security measures to protect the asset for the highest assessed business impact level noting that any Business Impact Level for confidentiality will require application of a security classification.

20. By way of an example, in considering a human resources database, an entity may determine that the information it holds does not warrant classification as the business impact level of the compromise of its confidentiality is assessed as medium. However, the information the database holds is essential to the business operations of the entity which indicates that the most relevant categorisation of the database may be as an important asset. By considering the factors relevant to important assets and the integrity and availability of the asset, the entity may determine that the business impact level in relation to compromise of its integrity and availability would be extreme. In this instance the information within the database would be marked and handled as Official: Sensitive. However, due to the higher business impact level of the database, it would have greater protections applied to ensure integrity of the information and availability of the database.

C.3 Measures to protect entity information and assets

21. There are a range of physical security measures entities can implement to protect entity resources from being made inoperable or inaccessible, or being accessed, used or removed without proper authorisation. Entities enhance the protection of their physical resources by using successive layers or combinations of procedural and physical security measures, including:

    a. security zones—refer to the PSPF policy: Entity facilities
    b. security containers and cabinets
    c. commercial safes and vaults
    d. secure rooms, strongrooms
    e. armouries and magazines
    f. ICT facilities.

22. **Requirement 2** mandates that entities assess security risks and select the appropriate secure room, container or cabinet to protect entity information and assets. Internal and external security risk factors may be relevant to selecting the appropriate secure room, container or cabinet—these include:
    a. levels of public access
    b. shared facilities with other tenants
    c. work areas with diverse programs and personnel with different levels of security clearances
    d. levels of neighbourhood crime.

C.3.1 Use of Security Construction and Equipment Committee approved products

23. The Security Construction and Equipment Committee (SCEC) is responsible for evaluating security equipment for their suitability for use by the Australian Government. The SCEC determines which products will be evaluated and the priority of evaluation. Evaluated security products protect classified information of which the compromise would result in a business impact level of high or above.
24. Evaluated products are assigned a security level (SL) rating numbered 1 to 4. SL4 products offer high level security, while SL1 products offer the lowest acceptable level of security for government use. Approved items are listed in the SCEC Security Equipment Evaluated Product List, which is only available to Australian Government security personnel and can be obtained from the protective security policy community on GovTEAMS.
25. Entities may use SCEC-approved security equipment even where it is not mandated. Alternatively, entities can use suitable commercial equipment that complies with identified security related Australian and International Standards for the protection of people and information and physical assets that do not have a confidentiality BIL of medium or above. ASIO-T4 has developed the Security Equipment Guides to assist entities to select security equipment not tested by SCEC. See the PSPF policy: Entity facilities **Annex A**.
26. SCEC only considers the security aspects of products when evaluating suitability for use in government. Other aspects like the products or safety features, are not considered by SCEC. The Attorney-General's Department recommends that entities consider safety requirements prior to product selection.

C.3.2 Security containers and cabinets

27. Suitably assessed security containers and cabinets are used to secure information, portable and valuable assets and money. When choosing the most appropriate security container or cabinet the Attorney-General's Department recommends entities consider:
    a. the type of asset, see Table 2
    b. the quantity or size of information and assets
    c. the location of the information or physical assets within the facility
    d. the structure and location of the facility
    e. the access control systems
    f. other physical protection systems—for example locks and alarms.
28. The Attorney-General's Department recommends that sensitive and security classified information and assets are stored in security containers and cabinets separately from physical assets. This can lower the risk of compromise of information if valuable and attractive physical assets are stolen and can assist investigators to determine the reason for the incidents involving unauthorised access.

C.3.2.1 SCEC-approved security containers

29. SCEC approved security containers are for storage of sensitive and security classified information and assets and are not for the storage of valuable, important, attractive, significant or dangerous assets. The designs of these containers provide a high level of tamper evidence of covert attack and significant delay from surreptitious attack, but provide limited protection from a forcible attack.
30. There are three levels of SCEC-approved containers:

a. 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.

b. 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 level 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 containers:

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

   ii. lighter constructed models that are used in conjunction with other physical security measures.

c. 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 level in situations assessed as higher risk by the entity. These containers are fitted with a SCEC-approved restricted keyed lock and are of similar construction to the lighter Class B containers.

31. For information on selecting security containers to store official information, see PSPF policy: Sensitive and classified information, **Annexes A to E**. See the ASIO-T4 Security Equipment Evaluated Products List for SCEC approved secure containers.

C.3.2.2 Commercial safes and vaults

32. 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 is normally larger than a safe. A safe is normally smaller than a vault and may be moveable. Safes and vaults provide varying degrees of protection depending on the construction and may be used to store valuable physical assets.

33. Safes and vaults can be fire resistant (to protect documents or data), burglar resistant or a combination of the two. The Attorney-General's Department recommends entities seek advice from qualified locksmiths or manufacturers when deciding the criteria to apply to select commercial safes and vaults. Guidance is also available in Australian Standard 3809 Safes and strongrooms and ASIO-T4 Security Equipment Guide SEG-022 Safes—Protection of Assets from the protective security policy community on GovTEAMS (for Australian Government security personnel only).

34. **Table 3** sets out the minimum commercial safe and vault requirements in the applicable zones based on the business impact level of the compromise, loss or damage to physical assets that are not classified or do not hold any classified information.

Table 3 Selecting commercial safes and vaults to protect physical assets, other than classified assets

Business impact level	1 Low business impact	2 Low to medium business impact	3 High business impact	4 Extreme business impact	5 Catastrophic business impact
Zone One	Determined by an entity risk assessment, locked commercial container recommended.	Determined by an entity risk assessment, commercial safe or vault recommended.	AS 3809 commercial safe or vault.	AS 3809 high security safe or vault.	Not to be held unless unavoidable.
Zone Two	Determined by an entity risk assessment, locked commercial container recommended.	Determined by an entity risk assessment.	Commercial safe or vault.	AS 3809 medium security safe or vault recommended.	Not to be held unless unavoidable.

Business impact level	1 Low business impact	2 Low to medium business impact	3 High business impact	4 Extreme business impact	5 Catastrophic business impact
Zone Three	Determined by an entity risk assessment.	Determined by an entity risk assessment.	Determined by an entity risk assessment, commercial safe or vault recommended.	AS 3809 commercial safe or vault recommended.	AS 3809 high or very high security safe or vault recommended.
Zone Four	Determined by an entity risk assessment.	Determined by an entity risk assessment.	Determined by an entity risk assessment.	Commercial safe or vault recommended.	AS 3809 medium or high security safe or vault recommended.
Zone Five	Determined by an entity risk assessment.	Determined by an entity risk assessment.	Determined by an entity risk assessment	Commercial safe or vault recommended.	AS 3809 medium or high security safe or vault recommended.

35. The Attorney-General's Department recommends that entities implement other physical controls that give the same level of intrusion resistance and delay where physical assets cannot be secured in commercial safes and vaults. These physical controls may include individual item alarms, alarm circuits or additional out-of-hours guarding.

C.3.2.3 Vehicle safes

36. Entities may consider fitting vehicles used by field staff with field safes to carry valuable assets and official information. Vehicle safes give some protection against opportunist theft and are only of value when vehicles are fitted with other anti-theft controls.

C.3.2.4 Managing security containers and cabinets

37. Security containers and cabinets can be a source of security risk if not managed appropriately over their lifetime. The Attorney-General's Department recommends that keys to security containers and cabinets are secured in key cabinets within a facility's secure perimeter and where possible within the security zone where the containers and cabinets are located.

38. For security containers and cabinets that are secured using combination settings, the Attorney-General's Department recommends combination settings are changed:

    a. regularly—not less frequently than every six months

    b. following repairs

    c. following change of personnel

    d. when there is reason to believe the setting has been, or may have been compromised.

C.3.2.5 Key cabinets

39. Manual and electronic key cabinets are used to secure keys, for example keys for C Class containers or internal offices, and are normally 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.

40. 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 containers. For advice refer to ASIO SEG-013 Electronic Key Cabinets available for Australian Government security personnel only from the protective security policy community on GovTEAMS.

41. Commercial grade key cabinets vary in quality and provide very little protection against forced or covert access.

C.3.3 Secure room and strongrooms

42. 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, loss or damage would have a business impact level. Secure rooms are designed to protect its contents from covert attack and have some degree of fire protection of the contents if the secure room is 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.

43. Advice on construction specifications for secure rooms is detailed in the ASIO Technical notes available for Australian Government security personnel only from the protective security policy community on GovTEAMS:

    a. Technical Note 7-06 Class A Secure Room

    b. Technical Note 8-06 Class B Secure Room

    c. Technical Note 9-06 Class C Secure Room.

44. SCEC-approved commercial Class A and B doors and demountable security rooms are listed on the Security Equipment Evaluated Products List.

C.3.4 Magazines, armouries and explosive storehouses

45. Advice on magazines, armouries and explosive storehouses is available from the Department of Defence.

C.4 Measures for the protection of sensitive and classified discussions

46. The core requirement to implement physical security measures that minimise or remove the risk of resources being made inoperable or inaccessible, or being accessed, used or removed without appropriate authorisation is consistent with PSPF policy: Sensitive and classified information core requirement that each entity must implement operational controls for sensitive and classified information proportional to their value, importance and sensitivity. To meet these requirements, the Attorney-General's Department recommends that, in areas where sensitive or classified discussions are held, entities implement physical and audio security measures to prevent deliberate or accidental overhearing.

47. The risk of deliberate or accidental overhearing can be minimised by controlling the environment where the discussion is taking place. This may be achieved by treating the room, area or entire facility acoustically, combined with other physical and procedural security measures.

48. To provide protection for sensitive or classified discussions, it is necessary for the sound created within the room to be unintelligible to a person or device located outside that room. Appropriate and effective sound insulation is critical to achieving the required level of security for sensitive and classified discussions as it is extremely difficult for an entity to ensure that only low-volume voice levels are used for sensitive and classified discussions or that background noise will always exist in the receiving area.

49. When designing an audio secure room suitable for security classified discussions, the Attorney-General's Department recommends entities consider a number of factors that may influence the specification and construction techniques used. These include:

    a. the sensitivity and classification of information being discussed

    b. the regularity of discussions.

50. Consistent with the core PSPF requirement for entity facilities, the Attorney-General's Department recommends entities consider the need to conduct sensitive or classified discussions throughout the process of planning, selecting, designing and modifying their facilities, to ensure the required physical security measures can be accommodated with the facilities. For guidance see the ASIO Technical Note 1/15 – Physical Security of Zones, Section 16: Audio Security.

51. It may be operationally critical to hold security classified conversations where an audio secure room is not available. The Attorney-General's Department recommends that these conversations are not held in public places or where the conversation may be overheard, for example hire cars, hotel rooms, airport lounges, aeroplanes or cafes.

C.5 Measures for the protection of ICT equipment

52. The purpose of ICT equipment is to facilitate electronic processing, storage and transfer of entity information. ICT equipment requires specific protection because of its:
    a. classification, either classified in its own right or classified due to the classification of the confidentiality requirements of the information held on the asset
    b. criticality of integrity or availability of the information held or processed on the asset
    c. potential attractiveness, either attractive in its own right (eg an iPad) or the attractiveness of the information held on the asset
    d. aggregation of information, which may increase the business impact level of the asset's compromise.
53. ICT equipment includes:
    a. movable physical assets, for example computers, scanners, photocopiers, multifunction devices, landline and mobile phones, digital devices and electronic storage media
    b. system equipment for example the hardware and software that provide an entity's network connectivity and communication
    c. building management systems and security systems.
54. ICT system equipment is used to maintain an ICT system and is normally operational 24 hours a day. ICT system equipment includes:
    a. servers, for example dedicated devices and laptops used as servers
    b. communication network devices, for example PABX systems
    c. supporting network infrastructure, for example cabling, patch panels
    d. gateway devices, for example routers and network access devices.
55. To identify the appropriate physical security measures to protect ICT assets and the information held or communicated on ICT equipment, the Attorney-General's Department recommends that entities determine the level of protection required based on the highest business impact level of the compromise of the aggregate of information on the equipment or:
    a. its communication over the network infrastructure
    b. the compromise, loss or damage of the ICT equipment.

C.5.1 ICT equipment secured in ICT facilities

56. ICT equipment may be permanently housed or temporarily stored in an ICT facility (a designated space or floor of an entity's building used to house an entity's ICT systems, components of their ICT systems or ICT equipment). These facilities include:
    a. server and gateway rooms
    b. datacentres
    c. backup repositories
    d. storage areas for ICT equipment that hold official information
    e. communication and patch rooms.
57. The physical security of containers and/or rooms required to house ICT equipment in an ICT facility may be lowered when the ICT facility is a separate security zone within an existing security zone that is suitable for the aggregation of the information held. Table 4 details the impact of applying the 'Security-in-Depth' principle (the 'Security-in-Depth' principle is detailed in PSPF policy: Entity facilities) and provides the revised physical security standard required.

Table 3 Storage container requirements for electronic information in ICT facilities

Business impact level of aggregated electronic information	Security zone of the 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 Low business impact	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 Low to medium business impact	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 High business impact	Zone Three or 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 Extreme business impact	Zone Four	SCEC Class C	Zone Three or 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 Catastrophic business impact	Zone Five	SCEC Class B	Compartment (certified by CSO)	SCEC Class C

58. The PSPF policy: Entity facilities includes requirements and guidance on the location, certification and accreditation of ICT facilities to achieve the appropriate level of protection commensurate with the business impact level of the loss, compromise or damage of the information and ICT equipment housed in an entity's ICT facilities.

C.5.1.1 Securing ICT equipment in ICT facilities when not in use

59. Subject to the entity's risk assessment, when not in use or unattended, some moveable ICT equipment can be stored in an ICT facility that is within a security zone of the work area, see Table 4.

60. Outside of business hours the Attorney-General's Department recommends entities secure:

    a. any security containers that hold ICT equipment within the ICT facility

    b. the ICT facility itself.

61. Refer to the PSPF policy: Entity facilities for details on security zone protections.

C.5.1.2 Security of ICT equipment that cannot be kept in ICT facilities, security containers or secure rooms when not in use

62. Where an entity is unable to secure ICT equipment (eg desktops computers, printers and multifunctional devices) in an ICT facility, container or secure room when not in use or unattended, the Attorney-General's Department recommends:

    a. storage of removable non-volatile media (hard drives) in an appropriate security container

    b. storage of ICT equipment where the non-volatile media cannot be removed in an appropriate security zone

    c. seek advice from the Australian Signals Directorate (ASD) about additional logical or technological solutions available to lower the risk of compromise of ICT equipment and its information.

63. **Table 5** sets out the recommended physical security zones for ICT equipment that cannot be held in a security container or secure room when not in use or unattended. Recommended security zones are based on the identified business impact level of the compromise of the information available on the ICT equipment.

Table 4 Business Impact Level and zone requirement for ICT equipment when not in use that cannot be held in a security container or security room

Business impact level of aggregated electronic information	1 Low business impact	2 Low to medium business impact	3 High business impact	4 Extreme business impact	5 Catastrophic business impact
Minimum security zone required	Zone Two or as determined by an entity risk assessment.	Zone Two or as determined by an entity risk assessment.	Zone Three or as determined by an entity risk assessment.	Zone Three or above unless additional logical controls are applied to lower the risks to a level acceptable to the entity.	Zone Five unless additional logical controls are applied to lower the risks to a level acceptable to the originating entity of the information.

C.5.2 Physical security for specific types of ICT equipment

C.5.2.1 Equipment with solid state drives or hybrid hard drives

64. Solid state drives and hybrid hard drives cannot be made safe through normal data wiping processes when switched off. The Attorney-General's Department recommends that entities using equipment fitted with these drives seek advice from ASD on methods to secure these types of equipment (eg encryption).

C.5.2.2 Deployable ICT systems

65. Entities may have difficulty in applying suitable physical security measures when using deployable ICT systems, particularly in high risk environments. The Attorney-General's Department recommends entities seek advice from ASD on suitable logical controls to help mitigate any risks identified as a result of using deployable ICT systems.

C.5.2.3 Network infrastructure

66. Protection of network infrastructure requires a combination of physical security measures and system encryption. Where ASD approved encryption is applied, the physical security protection requirements can be lowered in accordance with the Australian Government Information Security Manual (ISM). For information on protection of network infrastructure see the PSPF policy: Robust ICT systems.

67. Tampering of network infrastructure is a security risk. The Attorney-General's Department recommends entities secure network infrastructure equipment, such as patch panels, fibre distribution panels and structured wiring enclosures in containers and secure rooms. Where this is not possible it is recommended that entities meet system encryption requirements set out in the ISM.

C.5.2.4 ICT system gateway devices

68. The unauthorised access to gateway devices is a security risk. The Attorney-General's Department recommends that gateway devices are located in dedicated ICT facilities. For information on securing ICT system gateway devices see the ISM.

C.6 Protection of resources against loss of power supply

69. Loss of power supply can have a significant effect on the security of entity resources (for example loss of power could affect the operation of access control systems and security alarm systems) and is one of a number of considerations when developing the entity security plan, (refer to PSPF policy: Security planning and risk management).

C.7 Disposal of physical assets

70. Entities may need to dispose of entity physical resources due to, advances in technology, the end of the usable life of the physical asset, downsizing and changes in business requirements. Requirement 3 mandates that entities dispose of physical assets securely.

71. Prior to decommissioning and disposal of physical assets such as security containers, cabinets, vaults, strongrooms and secure rooms, the Attorney-General's Department recommends entities:

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

    b. visually inspect and remove all contents from these physical assets.

72. Secure disposal of ICT equipment may be achieved through sanitisation in accordance with the ISM—Product sanitisation and disposal. However, in some instances, ICT equipment cannot be sanitised and will require destruction.

C.7.1 Destruction equipment

73. Destruction equipment is used for sensitive and security classified information (paper-based and ICT media) so that resultant waste particles cannot be reconstructed to enable the recovery of information. For requirements and guidance on disposal of sensitive and security classified information, see the PSPF policy: Sensitive and classified information.

C.8 Working away from the office

74. Working away from the office covers all work undertaken by personnel away from entity facilities, including using mobile computing and communications and by teleworkers (see C.8.2). The Attorney-General's Department recommends that entities consider the security risks of the environments in which their personnel operate, the type of information that will be used and how that information will be accessed as these can vary and may have a significant impact on security requirements.

C.8.1 Mobile computing and communications

75. Mobile computing and communications encompasses work using portable computing and communications devices, such as laptops, notebooks, tablets, smart mobile phones and personal digital assistants. Mobile computing locations may include airport lounges, hotel rooms and conference facilities, as well as other entities' office facilities or work sites. Many mobile computing locations are public access areas with few or no protective security measures in place and would be rated no greater than a Zone One security area. To effectively protect entity resources in these instances, the Attorney-General's Department recommends that personnel carry portable computing and communications devices with them at all times and not leave them unattended.

76. It may not be possible to apply suitable physical security measures to satisfy a higher security zone requirement for mobile computing and communications. Entities may need to rely on administrative and ICT logical security controls to protect their information and assets. Refer to the ISM for logical controls.

C.8.2 Teleworking

77. Teleworking allows personnel to work away from the office facilities and from alternate locations. Teleworking requires using remote ICT systems in fixed locations such as:

    a. working from personal residences on a regular basis, and

    b. working from an alternative office space:

        i. within entity facilities in another location—for example regional sites

        ii. located in another Australian, state or territory government entity's facilities

        iii. provided to the entity in premises where the entity has some capability to provide protective security, for example offices operated by an entity's client or by a service provider contracted by the entity.

78. Without significant modifications to the teleworking site many teleworking locations will meet Zone Two physical security requirements.

C.8.3 Protecting resources while working away from the office

79. **Requirement 1** mandates that entities protect their resources commensurate with the assessed business impact level of their compromise, loss or damage. The Attorney-General's Department recommends entities determine procedures to ensure appropriate accreditation of proposed work sites outside of the office. This may require a security inspection of the proposed work site. Prior to authorising such work arrangements the Attorney-General's Department recommends that entities consider the resources that will be used or stored in the work space to determine:
    a. if sensitive or classified information can be appropriately secured
    b. if the work space can be independently secured
    c. if the work space can be protected from oversight, or overhearing, by other people, including family and children
    d. if the ICT equipment being used can be secured or segregated from the entity's ICT system.
80. Minimum protections for storage of sensitive and security classified information used for working away from the office are set out in PSPF policy: Sensitive and classified information **Annexes A-E**. Additionally, PSPF policy: Entity facilities **Requirement 7** mandates that entities obtain ASIO-T4 certification for any security areas used to store TOP SECRET information.
81. Entity physical assets are vulnerable to loss outside of government facilities. The Attorney-General's Department recommends that appropriate protections and procedures are put in place. These protections and procedures may include:
    a. asset controls, see C.1.3.1
    b. limiting assets to be removed from facilities to those necessary for performance of the out-of-the-office duties
    c. evaluating the need for a portable security alarm system (refer to ASIO-T4 Protective Security Circular 162 Private residence physical security assessment).

C.8.3.1 Physical security of official information in facilities not managed by the entity

82. It may be difficult to secure entity information when the working environment is not controlled or managed by the entity. For example the work environment is:
    a. located inside commercial facilities or in private client facilities for which the entity is providing services
    b. the private residence of the entity's personnel
    c. the facility of an industry providing services to the entity to collect, use and/or store official information or other security protected Commonwealth resources.
83. The Attorney-General's Department recommends entities treat any non-Australian Government facilities as Zone One areas for storage and/or use of Commonwealth information and assets unless the entity has:
    a. full control over the work space occupied by their personnel in commercial and client facilities
    b. confirmed appropriate physical and procedural security measures are in place for a higher level zone.

D. Find out more

84. Other information and policies:
    a. ASIO-T4 publications—available for Australian Government security personnel only from the protective security policy community on GovTEAMS:
        i. ASIO Technical Notes

ii. Security Equipment Evaluated Products List

iii. Security Equipment Guides (SEGs)

b. Other PSPF policy and guidelines available on the Protective Security Policy website:

i. PSPF policy: Sensitive and classified information

ii. PSPF policy: Security planning and risk management

iii. PSPF policy: Entity facilities

c. Work Health and Safety Act 2011

d. Australian Government Information Security Manual.

D.1 Change log

Table 5 Amendments in this policy

Version	Date	Section	Amendment
v2018.1	Sep 2018	Throughout	Not applicable. This is the first issue of this policy
V2018.2	May 2019	C.5.1	Table 4 relocated from C.5.1.1 to C.5.1 for clarity

Annex A. Historical business impact levels

Annex A Table 1 Business Impact Level 3A – Significant damage to the national interest, organisations or individuals

Sub-impact categories	Significant damage is:
Impacts on national security	causing damage to national security
Impacts on entity operations	a. causing a severe degradation in, or loss of, organisational capability to an extent and duration that the entity cannot perform one or more of its functions for an extended time b. resulting in major long term harm to entity assets.
Australian financial and economic impacts	a. undermining the financial viability of, or causing substantial financial damage to, a number of major Australia-based or Australian-owned organisations or companies b. causing long term damage to the Australian economy to an estimated total of $10 to $20 billion c. causing major, short term damage to global trade or commerce, leading to short term recession or hyperinflation in Australia.
Impacts on government policies	a. significantly disadvantaging Australia in international negotiations or strategy b. temporarily damaging the internal stability of Australia or friendly countries c. causing significant damage or disruption to diplomatic relations, including resulting in formal protest or retaliatory action.
Impacts on personal safety	endangering small groups of individuals – the compromise of information could lead to serious harm or potentially life threatening injuries to a small group of individuals.
Impacts on crime prevention	causing major, long-term impairment to the ability to investigate serious offences (ie offences resulting in two or more years imprisonment).
Impacts on defence operations	causing damage to the operational effectiveness or security of Australian or allied forces that could result in risk to life.
Impacts on intelligence operations	causing damage to Australian or allied intelligence capability.
Impacts on national infrastructure	damaging or disrupting significant national infrastructure.