



Australian Government

Department of Education, Employment and Workplace Relations

PSPSEC301A Secure government assets

Revision Number: 3

PSPSEC301A Secure government assets

Modification History

Release	TP Version	Comments
3	PSP12V1	Unit descriptor edited.
2	PSP04V4.2.	Layout adjusted. No changes to content.
1	PSP04V4.1	Primary release.

Unit Descriptor

This unit covers implementation of security requirements for the organisation's assets. It includes protecting assets from security threats, implementing access restrictions, advising third parties of security requirements and minimising security risk.

In practice, securing government assets may overlap with other generalist or specialist public sector work activities such as acting ethically, complying with legislation, working effectively, working with diversity, organising information.

No licensing, legislative, regulatory or certification requirements apply to this unit at the time of endorsement.

Application of the Unit

Not applicable.

Licensing/Regulatory Information

Not applicable.

Pre-Requisites

Not applicable.

Employability Skills Information

This unit contains employability skills.

Elements and Performance Criteria Pre-Content

Elements are the essential outcomes of the unit of competency. Together, performance criteria specify the requirements for competent performance. Text in ***bold italics*** is explained in the Range Statement following.

Elements and Performance Criteria

ELEMENT	PERFORMANCE CRITERIA
1. Protect assets from security threats	1.1 <i>Assets</i> are stored and accessed in accordance with organisational policies, procedures and guidelines. 1.2 Assets are regularly checked to ensure security. 1.3 Suspicious activity is investigated and dealt with in accordance with organisational policy and procedures. 1.4 <i>Expert advice</i> is obtained as required in accordance with organisational policy and procedures.
2. Implement access restrictions	2.1 Access is <i>restricted</i> to authorised personnel. 2.2 Potential threats are identified. 2.3 Breaches are identified and reported to appropriate personnel in accordance with organisational policy and procedures. 2.4 Action is taken to deal with a breach in accordance with legislation, policy and guidelines.
3. Advise third parties of security requirements	3.1 The needs, expectations, attitudes, and current level of knowledge of <i>third parties</i> are confirmed. 3.2 Risks related to possible confrontations are identified and managed in accordance with organisational risk management and procedures. 3.3 Third parties are advised of the organisation's security requirements. 3.4 Advice is provided that is current, timely and meets the specific needs of the parties in its range, depth and form of presentation. 3.5 Feedback is obtained on the party's level of understanding, and additional information or explanation is used to clarify requirements if needed.
4. Minimise security risk	4.1 Changes in circumstance are identified and reported to appropriate personnel in accordance with organisational policy and procedures. 4.2 Documentation is completed in accordance with organisational policies, procedures and guidelines. 4.3 <i>Actions</i> are taken to reduce the likelihood of breaches reoccurring in accordance with the organisation's security plan.

Required Skills and Knowledge

This section describes the essential skills and knowledge and their level, required for this unit.

Skill requirements

Look for evidence that confirms skills in:

- applying legislation, regulations and policies relating to government security management
- applying analysis and problem solving
- tailoring communication to the needs of a diverse range of people inside and outside the organisation
- completing documentation and writing reports requiring attention to detail, and formality of language and structure
- responding to diversity, including gender and disability
- applying procedures relating to occupational health and safety and environment in the context of government security management

Knowledge requirements

Look for evidence that confirms knowledge and understanding of:

- legislation, regulations, policies, procedures and guidelines relating to government security management
- standards for management of classified information and assets
- available sources of expert advice
- international protocols and treaties impacting on government security management
- equal employment opportunity, equity and diversity principles
- public sector legislation such as occupational health and safety and environment in the context of government security management

Evidence Guide

The Evidence Guide specifies the evidence required to demonstrate achievement in the unit of competency as a whole. It must be read in conjunction with the Unit descriptor, Performance Criteria, the Range Statement and the Assessment Guidelines for the Public Sector Training Package.

Units to be assessed together

- *Pre-requisite* units that must be achieved prior to this unit: *Nil*
- *Co-requisite* units that must be assessed with this unit: *Nil*
- *Co-assessed units* that may be assessed with this unit to increase the efficiency and realism of the assessment process include, but are not limited to:
 - PSPETHC301B Uphold the values and principles of public service
 - PSPGOV301B Work effectively in the organisation
 - PSPGOV307B Organise workplace information
 - PSPLEGN301B Comply with legislation in the public sector
 - PSPSEC302A Respond to government security incidents
 - PSPSEC303A Conduct security awareness sessions
 - PSPSEC304A Undertake information technology security audits

Overview of evidence requirements

In addition to integrated demonstration of the elements and their related performance criteria, look for evidence that confirms:

- the knowledge requirements of this unit
- the skill requirements of this unit
- application of the Employability Skills as they relate to this unit (see Employability Summaries in Qualifications Framework)
- securing government assets in a range of (3 or more) contexts (or occasions, over time)

Resources required to carry out assessment

These resources include:

- legislation, policy, procedures and protocols relating to security of government assets
- case studies and workplace scenarios to capture the range of situations likely to be encountered when securing government assets

Where and how to assess evidence

Valid assessment of this unit requires:

- a workplace environment or one that closely resembles normal work practice and replicates the range of conditions likely to be encountered when securing government assets,

including coping with difficulties, irregularities and breakdowns in routine

- securing government assets in a range of (3 or more) contexts (or occasions, over time)

Assessment methods should reflect workplace demands, such as literacy, and the needs of particular groups, such as:

- people with disabilities
- people from culturally and linguistically diverse backgrounds
- Aboriginal and Torres Strait Islander people
- women
- young people
- older people
- people in rural and remote locations

Assessment methods suitable for valid and reliable assessment of this competency may include, but are not limited to, a combination of 2 or more of:

- case studies
- portfolios
- projects
- questioning
- scenarios
- simulation or role plays
- authenticated evidence from the workplace and/or training courses such as a risk management plan specific to assets

For consistency of assessment

Evidence must be gathered over time in a range of contexts to ensure the person can achieve the unit outcome and apply the competency in different situations or environments

Range Statement

The Range Statement provides information about the context in which the unit of competency is carried out. The variables cater for differences between States and Territories and the Commonwealth, and between organisations and workplaces. They allow for different work requirements, work practices and knowledge. The Range Statement also provides a focus for assessment. It relates to the unit as a whole. Text in ***bold italics*** in the Performance Criteria is explained here.

Assets may include:

- information
- documents
- people
- property
- networks
- systems
- intellectual property
- in Australia
- overseas

Assets may be:

- owned
- on lease
- hired
- owned by others

Expert advice may include:

- agency security adviser/s
- specialist agencies such as:
 - Australian Security Intelligence Organisation
 - Department of Foreign Affairs and Trade
 - Australian Public Service Commission
 - Defence Signals Directorate
 - Australian Federal Police
 - Attorney-General's Department
 - Australian National Audit Office
 - Office of the Australian Information Commissioner (OAIC)

Access may be restricted to information that is:

- national security classified
- non-national security classified
- classified by third parties

Third parties may include:

- other staff
- contractors
- members of the public
- visitors to the organisation

Actions may include:

- advice to responsible officers
- disciplinary
- formal counselling
- prosecution
- referral to third parties
- strengthening of security
- training

Unit Sector(s)

Not applicable.

Competency field

Government Security Management.