Australian Government
Department of Education, Employment and Workplace Relations

PSPSEC405A Handle security classified information

Revision Number: 3

INDUSTRY SKILLS COUNCILS
Creating Australia's Future

PSPSEC405A Handle security classified information

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 the requirements related to handling security classified information. It includes receiving, dealing with and maintaining security classified information.

In practice, handling security classified information may overlap with other generalist or specialist public sector work activities such as working ethically, complying with legislation, applying government processes, gathering and analysing information, exercising regulatory powers.

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. **Receive security classified information**	1.1 ***Security classified information*** is ***received*** and checked to ensure transmission protocols have been adhered to. 1.2 Action is taken in accordance with security policy and procedures where protocols have not been adhered to. 1.3 Security classified information is recorded in accordance with organisational policy and procedures.
2. **Deal with security classified information**	2.1 Security classified information is ***reviewed*** to ensure classification meets the organisation's security policy for protection of information. 2.2 Aggregated security classified information is reviewed to ensure that it is classified in accordance with security requirements. 2.3 Classification requirement is checked to ensure it is warranted, and the level of protection is assigned in accordance with the consequences that might result from the compromise of the information's confidentiality, integrity and availability. 2.4 Originators of information who classify documents are contacted to discuss re-classification or de-classification where necessary. 2.5 Security classified information is ***transmitted*** in accordance with organisational security policy and procedures. 2.6 ***Expert advice*** is obtained as required in accordance with organisational policy and procedures.
3. **Maintain security classified information**	3.1 Security classified information is ***secured*** in accordance with organisational policy and procedures. 3.2 Security classified information is ***accounted for*** in accordance with organisational policy and procedures. 3.3 Security classified information is ***disposed of*** in accordance with organisational policy and procedures.

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 security classification systems
- using analysis and problem solving
- tailoring communication to the needs of a diverse range of people inside and outside the organisation who classify, transmit or advise on security classified information
- responding to diversity, including gender and disability
- undertaking recordkeeping requiring attention to detail, and adherence to standards
- 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 security classified information
- classification system for national security and non-national security information
- procedures for confirming initial security classifications
- international protocols and treaties impacting on government security management
- available sources of expert advice
- 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:
    - PSPETHC401A Uphold and support the values and principles of public service
    - PSPGOV406B Gather and analyse information
    - PSPGOV422A Apply government processes
    - PSPLEGN401A Encourage compliance with legislation in the public sector
    - PSPREG401C Exercise regulatory powers

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)
- security classified information handled 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 handling security classified information
- case studies and workplace scenarios to capture the range of situations likely to be encountered when handling security classified information

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 handling security classified information, including coping with difficulties, irregularities and breakdowns in routine
- security classified information handled 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
- demonstration
- observation
- portfolios
- projects
- questioning
- scenarios
- simulation or role plays
- authenticated evidence from the workplace and/or training courses

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.

Security classified information may include:

- hard copy
- electronic
- audio-visual
- photographic
- encrypted
- national security classified
- non-national security classified
- classified by third parties

Security classified information may be ***received*** by:

- hand
- mail
- safe hand mail
- courier
- electronic means

Reviewed information may include:

- single or aggregated information

Transmission may be by:

- hand
- mail
- courier
- electronic means

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

Securing practices may include:

- correct filing
- clean desk

	• quitting all electronic systems and networks • checking environment including: • desks • whiteboards • waste bins • computer drives • containers • cabinets • safes • vaults • windows • doors • safe carriage of keys
Accounting for security classified information may include:	• audit • spot checks • correct notation or markings • file records • transmission records • receipts
Methods of ***disposal*** may include:	• pulping • burning • pulverisation • shredding • overwriting • degaussing • destruction • archiving

Unit Sector(s)

Not applicable.

Competency field

Government Security Management.