Australian Government

Department of Education, Employment and Workplace Relations

PSPSEC302A Respond to government security incidents

Revision Number: 2

PSPSEC302A Respond to government security incidents

Modification History

PSPSEC302A Release 2: Layout adjusted. No changes to content.
PSPSEC302A Release 1: Primary release.

Unit Descriptor

This unit covers the requirements to respond to security incidents, that may be intentional or unintentional, and that relate to people, information, property or reputation. It includes assessing and advising on security incidents and planning an incident response.
In practice, responding to security incidents may overlap with other generalist or specialist public sector work activities such as acting ethically, complying with legislation, working effectively, organising information, etc.

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. Assess and advise on security incidents	1.1 ***Security incidents*** are identified in accordance with legislation, government security policy and guidelines.
	1.2 Response is provided in accordance with organisational policy and procedures, incident management plan and reflects seriousness of the incident.
	1.3 ***Preliminary assessment*** is conducted that considers the nature of the breach, level of risk and likely consequences.
	1.4 Initial advice regarding the incident is given to ***relevant personnel*** in a timely fashion.
	1.5 Complete and accurate ***records*** relating to the incident are maintained, based on information collected in a timely fashion.
2. Plan incident response	2.1 Evidence is identified and collected in accordance with legislation, organisational policy and procedures.
	2.2 Evidence is assessed to determine risk factors.
	2.3 Action is recommended which is appropriate to the level of seriousness of the incident.
	2.4 Any changes required in security policy as a result of the incident are identified and documented.
	2.5 Appropriate agencies are advised of the incident in accordance with legislation, government security policy and procedures.
	2.6 A final report is prepared that incorporates background to the incident, action taken, interview statements, outcomes, summary of findings and recommended action.

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
- undertaking research, analysis (including trend analysis) and problem solving
- using effective communication, including interviewing tailored to a diverse stakeholder group
- responding to diversity, including gender and disability
- planning, carrying out and guiding an investigation
- recording evidence in accordance with legislation and public sector standards
- writing reports and recommendations requiring formality of language and structure, and accurate and objective content
- applying procedures relating to occupational health and safety and environment in the context of government security incident management

Knowledge requirements

Look for evidence that confirms knowledge and understanding of:

- legislation, regulations, policies, procedures and guidelines relating to government security management
- organisation's security plan
- Crimes Act 1914 and Criminal Code 1985
- powers inferred to investigate security incidents, including limitations
- referral procedures and appropriate agencies
- intelligence and analytical process
- conduct of administrative, security or criminal investigations
- equal employment opportunity, equity and diversity principles
- public sector legislation such as privacy, security, 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

PSPSEC301A Secure government assets

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)
- response to security incidents 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 related to handling security incidents
- case studies and workplace scenarios to capture the range of situations likely to be encountered when responding to security incidents

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 responding to security incidents, including coping with difficulties, irregularities and breakdowns in routine
- response to security incidents 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
- questioning
- scenarios
- simulation or role plays
- authenticated evidence from the workplace and/or training courses, such as incident reports

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 incidents may be:	• breaches • violations • contact • approach • intentional • unintentional • deliberate
Incidents may relate to:	• people • information • property • reputation
Preliminary assessment may include:	• site visit • identification of nature of the incident • collection of evidence • determination of the origin of the incident • likely cause • notification of incident to appropriate agencies
Relevant personnel may include:	• supervisors • managers • emergency services • other government departments or agencies • police • contract guarding force
Records may include:	• evidence • written • oral • files • email • Internet/intranet • electronic records • video images • graphics • notes • diary entries

- telephone messages
- pager records
- fax journals

Unit Sector(s)

Not applicable.

Competency field

Government Security Management.