



Australian Government

Department of Education, Employment and Workplace Relations

CPPSEC4009A Interpret information from advanced security equipment

Release: 1

CPPSEC4009A Interpret information from advanced security equipment

Modification History

Not Applicable

Unit Descriptor

Unit descriptor

This unit of competency specifies the outcomes required to operate and control advanced security systems and equipment. It requires the ability to verify and interpret received data, formulate and implement responses appropriate to situations, and maintain the operational effectiveness of security systems.

This unit may form part of the licensing requirements for persons responsible for receiving security information and implementing responses to security risk incidents in those states and territories where these are regulated activities.

Application of the Unit

Application of the unit

This unit of competency has application in those work roles involving the interpreting of security information to formulate a security response. Competency requires legal and operational knowledge applicable to relevant sectors of the security industry. The knowledge and skills described in this unit are to be applied within relevant legislative and organisational guidelines.

Licensing/Regulatory Information

Refer to Unit Descriptor

Pre-Requisites

Not Applicable

Employability Skills Information

Employability skills This unit contains employability skills.

Elements and Performance Criteria Pre-Content

Elements describe the essential outcomes of a unit of competency.	Performance criteria describe the required performance needed to demonstrate achievement of the element. Where <i>bold italicised</i> text is used, further information is detailed in the required skills and knowledge section and/or the range statement. Assessment of performance is to be consistent with the evidence guide.
---	--

Elements and Performance Criteria

ELEMENT

PERFORMANCE CRITERIA

1 Evaluate information.

- 1.1 Applicable provisions of **legislative** and **organisational requirements** relevant to receiving security information and data are identified and complied with.
- 1.2 **Security systems and equipment** are operated and monitored in accordance with manufacturer's instructions.
- 1.3 Data is received from verifiable **sources** and checked for consistency in accordance with organisational procedures.
- 1.4 Security systems are cross-checked with **companion monitoring systems** to ensure an accurate and consistent exchange of information.
- 1.5 Information conveyed by security systems is interpreted and evaluated in accordance with organisational procedures.

2 Respond to situations.

- 2.1 Potential security **risk** situations are assessed on available information and appropriate **response** is formulated and implemented in accordance with organisational procedures.
- 2.2 Contingencies and additional resources are anticipated to support a prompt and effective response.
- 2.3 Changing circumstances are identified and variations to response are determined and implemented in accordance with organisational procedures.
- 2.4 Continual exchange of information is maintained with **relevant persons**.
- 2.5 Requirements for additional support or specialist advice is promptly actioned in accordance with organisational procedures.

3 Control security systems.

- 3.1 Security systems are systematically monitored and tested to ensure performance is maintained within defined operating guidelines.
- 3.2 Preventative and breakdown maintenance arrangements for security systems are confirmed.
- 3.3 Actual or suspected faults or deficiencies in security systems are reported in accordance with organisational procedures.
- 3.4 Back-up procedures are implemented to maintain security and integrity of security systems in accordance with manufacturer's instructions.
- 3.5 Relevant **documentation** is completed and securely maintained in accordance with organisational procedures.

Required Skills and Knowledge

REQUIRED SKILLS AND KNOWLEDGE

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

Required skills

- analyse and implement response to information
- appreciate different cultural and social practices
- back up security systems
- coaching and mentoring to provide support to colleagues
- communicate in a clear and concise manner when sending and relaying information
- comply with relevant legislative and regulatory requirements
- estimate and calculate resource and equipment requirements
- evaluate and interpret information
- identify and diagnose faults or deficiencies in operation of security systems
- interpret security codes and alarm signals
- operate and maintain a range of security systems and equipment
- prepare and present written and computer-based information
- prioritise work tasks and maintain schedules.

Required knowledge

- appropriate information responses
- communication terminology (approved company greeting, call signs, codes, signals, phonetic alphabet)
- emergency procedures
- local hazards and environmental threats
- operational principles and functions of security systems and equipment
- principles of effective communication
- procedures for finding faults, maintenance and repair of equipment
- product knowledge for security systems
- relevant legislative provisions including Occupational Health and Safety (OHS) and licensing requirements, evidence, privacy, confidentiality, trespass, use of force, arrest and operational legislation (such as firearms and prohibited weapons)
- reporting, documentation requirements and processes
- roles and responsibilities of emergency and support services
- routine problem solving strategies
- security risk assessment methods
- systems back-up procedures
- verification requirements for assessing authenticity of received information.

Evidence Guide

EVIDENCE GUIDE

The evidence guide provides advice on assessment and must be read in conjunction with the performance criteria, required skills and knowledge, range statement and the Assessment Guidelines for the Training Package.

Critical aspects for assessment and evidence required to demonstrate competency in this unit

A person who demonstrates competency in this unit must be able to provide evidence of:

- formulating and implementing responses appropriate to the situation based on existing information
- varying operational plans as required to meet changing circumstances and information
- interpreting and verifying authenticity of conveyed information and carrying out consistent and accurate inputting of data using a standardised style and format
- maintaining operational efficiency and effectiveness of security systems and equipment
- promptly identifying and arranging remedial actions for actual or suspected faults and malfunctions in security systems and equipment.

Context of and specific resources for assessment

Context of assessment includes:

- a setting in the workplace or environment that simulates the conditions of performance described in the elements, performance criteria and range statement.

Resource implications for assessment include:

- access to plain English version of relevant statutes and procedures
- access to a registered provider of assessment services
- access to a suitable venue and equipment
- assessment instruments including personal planner and assessment record book
- work schedules, organisational policies and duty statements.

Reasonable adjustments must be made to assessment processes where required for people with disabilities. This could include access to modified equipment and other physical resources, and the provision of appropriate assessment support.

Method of assessment

This unit of competency could be assessed using the following methods of assessment:

- observation of processes and procedures

- questioning of underpinning knowledge and skills.

Guidance information for assessment

Assessment processes and techniques must be culturally appropriate and suitable to the language, literacy and numeracy capacity of the candidate and the competency being assessed. In all cases where practical assessment is used, it should be combined with targeted questioning to assess the underpinning knowledge.

Oral questioning or written assessment may be used to assess underpinning knowledge. In assessment situations where the candidate is offered a choice between oral questioning and written assessment, questions are to be identical.

Supplementary evidence may be obtained from relevant authenticated correspondence from existing supervisors, team leaders or specialist training staff.

Range Statement

RANGE STATEMENT

The range statement relates to the unit of competency as a whole. It allows for different work environments and situations that may affect performance. Bold italicised wording, if used in the performance criteria, is detailed below. Essential operating conditions that may be present with training and assessment (depending on the work situation, needs of the candidate, accessibility of the item, and local industry and regional contexts) may also be included.

Legislative requirements may relate to:

- apprehension and powers of arrest
- Australian standards and quality assurance requirements
- crowd control and control of persons under the influence of intoxicating substances
- force continuum, use of force guidelines
- general 'duty of care' responsibilities
- inspection of people and property, and search and seizure of goods
- licensing or certification requirements
- privacy and confidentiality
- relevant commonwealth, state and territory legislation, codes and national standards for:
 - anti-discrimination
 - cultural and ethnic diversity
 - environmental issues
 - equal employment opportunity
 - industrial relations

- OHS
- relevant industry codes of practice
- telecommunications
- trespass and the removal of persons
- use of listening and recording devices
- use of restraints and weapons:
 - batons
 - firearms
 - handcuffs
 - spray.
- access and equity policies, principles and practices
- business and performance plans
- client service standards
- code of conduct, code of ethics
- communication and reporting procedures
- complaint and dispute resolution procedures
- emergency and evacuation procedures
- employer and employee rights and responsibilities
- OHS policies, procedures and programs
- own role, responsibility and authority
- personal and professional development
- privacy and confidentiality of information
- quality assurance and continuous improvement processes and standards
- resource parameters and procedures
- roles, functions and responsibilities of security personnel
- storage and disposal of information.

Organisational requirements may relate to:

Security systems may include:

- acoustic sensors
- automatic entrance and exit devices
- closed circuit television
- electronic field detection systems
- fire alarms
- infra-red sensors
- intelligent building systems
- movement detectors
- other access control systems
- other intruder alarm systems
- weighbridge operation
- wide angle cameras.

Sources may include:

- audio, visual, or digital recording devices
- computer data files

- local, state and commonwealth government documents and registers
 - policy statements and media reports
 - statistical summaries
 - statutes.
- Companion monitoring systems may include:***
- audio, visual, or digital backup recording systems
 - parallel systems and may be a written record or electrical monitoring systems.
- Responses may involve:***
- disciplinary action according to organisational requirements
 - dispatching field support staff
 - execution of standard operating procedures for the occurrence of particular events
 - notifying emergency services
 - notifying relevant personnel.
- Risk relates to:***
- the chance of something happening that will have an impact on objectives.
- Security risks may relate to:***
- biological hazards
 - chemical spills
 - client contact
 - electrical faults
 - explosives
 - financial viability
 - injury to personnel
 - noise, light, heat, smoke
 - persons carrying weapons
 - persons causing a public nuisance
 - persons demonstrating suspicious behaviour
 - persons suffering from emotional or physical distress
 - persons under the influence of intoxicating substances
 - persons with criminal intent
 - persons, vehicles and equipment in unsuitable locations
 - property or people
 - security systems
 - suspicious packages or substances
 - systems or process failures
 - terrorism
 - violence or physical threats.
- Relevant persons may include:***
- clients
 - colleagues
 - emergency services personnel
 - employer

Documentation may include:

- equipment manufacturer
- field staff
- supervisor.
- activity reports
- field notes and security notebooks
- incident and accident reports
- radio and telephone records
- records of conversation
- request for assistance forms
- running sheets
- situation reports
- task allocation sheets
- written and computer-based information.

Unit Sector(s)

Unit sector Security

Competency field

Competency field Security and risk management