



Australian Government

Department of Education, Employment and Workplace Relations

CPPSEC3020A Monitor security from control room

Release: 1

CPPSEC3020A Monitor security from control room

Modification History

Not Applicable

Unit Descriptor

Unit descriptor This unit of competency specifies the outcomes required to monitor the security of persons and premises from a control room perspective. It requires the ability to effectively operate security systems to monitor activities, coordinate appropriate responses to security incidents and organise back-up support to field staff.

This unit may form part of the licensing requirements for persons who operate electronic security systems in those states and territories where these are regulated activities.

Application of the Unit

Application of the unit This unit of competency has wide application in the security industry in those roles which involve the operation of electronic security systems. 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 Prepare for operations.	1.1 Applicable provisions of legislative and organisational requirements relevant to assignment instructions are identified and complied with. 1.2 Assignment instructions and relevant information is obtained and verified with relevant persons.. 1.3 Security systems are checked for correct operation in accordance with manufacturer's instructions. 1.4 Faults or malfunctions in security systems are identified, corrected or reported for remedial action. 1.5 Security systems are cross-checked with companion monitoring systems to ensure accurate and consistent exchange of information. 1.6 Established communication channels and processes are verified with relevant persons.
2 Monitor security activities.	2.1 Security systems are operated and monitored in accordance with assignment instructions. 2.2 Information conveyed by security systems is received and appropriate responses implemented as required in accordance with organisational procedures. 2.3 Regular and systematic checks are made with field staff and assistance is organised as required in accordance with organisational procedures. 2.4 Irregular or non-responses from field staff are identified and promptly responded to in accordance with organisational procedures. 2.5 Incidents are risk assessed on available information and response is implemented in accordance with organisational procedures.
3 Maintain security systems and information.	3.1 Change of shift procedures are carried out and ensure system and monitoring continuity in accordance with organisational procedures. 3.2 Security database is updated in established styles and formats in accordance with organisational procedures. 3.3 Identified faults or deficiencies in security systems are corrected or reported for remedial action in accordance with organisational procedures. 3.4 Relevant documentation is completed and securely maintained with due regard to confidentiality.

Required Skills and Knowledge

REQUIRED SKILLS AND KNOWLEDGE

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

Required skills

- assess and implement appropriate response to received information
- communicate in a clear and concise manner using appropriate terminology
- estimate and calculate resource and assistance requirements
- identify and diagnose faults or deficiencies in operation of security systems
- interpret security codes and alarm signals
- monitor, evaluate and interpret data and information
- operate and maintain a range of security systems
- prepare and present written and computer-based information
- read and interpret technical data and specifications
- risk assess incidents.

Required knowledge

- approved communication terminology and codes and signals
- back-up procedures
- change of shift procedures
- common faults and malfunctions in security systems
- communication formats (high speed, contact ID etc)
- difference between local and monitored alarms
- different types of transmission methods (dialler, securitel etc)
- emergency procedures
- operational principles and functions of security systems and software and hardware
- phonetic alphabet
- problem solving strategies
- procedures for preparation of surveillance footage
- range of security risk or incident situations and appropriate response procedures implemented from a control room
- reporting and documentation procedures
- risk assessment methods
- surveillance recording systems (digital and analogue) and interfaces
- types of computer operating systems in use in a monitoring centre
- types of detectors (PIR, dual tech etc).

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:

- operating electronic systems to conduct systematic monitoring activities in compliance with legislative requirements
- diagnosing and rectifying faults or malfunctions in security systems or arranging repair or replacement
- implementing and monitoring the routine hand-over of duties and accurately completing and maintaining documentation records
- implementing appropriate contingency measures in the event of irregular or non-response from field staff
- interpreting and evaluating security alarms and communication status signals as the basis for formulating and coordinating appropriate responses
- using appropriate communication channels and techniques to accurately receive, interpret and relay information in both routine and non-routine circumstances.

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
- casinos
- counter-terrorism
- crowd control and control of persons under the influence of intoxicating substances
- force continuum, use of force guidelines
- gaming
- 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

Organisational requirements may relate to:

- equal employment opportunity
- industrial relations
- Occupational Health and Safety (OHS)
- relevant industry codes of practice
- surveillance
- telecommunications.
- 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.

Assignment instructions may include:

- assignment tasks
 - GPS monitoring
 - GSM monitoring
 - IT monitoring
 - medical monitoring
 - radio monitoring
- incident and security risk response procedures
- personal presentation requirements
- personal protection equipment
- reporting and documentation requirements
- resource and equipment requirements.

Relevant information may include:

- applicable legislation and codes of practice
- field personnel schedules
- manufacturer's specifications
- operations manuals
- organisational operating procedures and policies
- security operational plans.

Relevant persons may

- clients

include:

- emergency services personnel
- field personnel
- supervisor.

Security systems may include:

- access control systems
- acoustic sensors
- alarms and signals (local and monitored)
- analogue (VCR)
- automatic entrance and exit devices
- biometric devices
- business equipment
- closed circuit television
- communication equipment
- computers and networked systems
- digital
- electronic field detection systems
- electronic screening equipment
- infra-red sensors
- intelligent building systems
- intruder alarm systems
- motion sensors
- movement detectors
- personal duress alarms
- static alarms
- video cameras and monitors
- wide-angle cameras.

Companion monitoring systems are:

- parallel systems and may be
 - electrical monitoring systems
 - written record.

Communication channels and processes may include:

- direct line supervision paths
- established communication protocols
- formal communication pathways
- lateral supervision paths
- organisational communication networks
- verbal and non-verbal communication procedures eg pro-words, phonetic alphabet, call signs, coded messages, use of abbreviations, hand signals.

Responses may include:

- dispatching field support staff
- notifying relevant emergency services agencies
- notifying relevant personnel.

Documentation may include:

- activity logs
- radio and telephone records

- records of conversation
- running sheets
- security logs
- security systems faults and diagnosis
- situation reports
- testing and inspection results
- written and computer-based reports.

Unit Sector(s)

Unit sector Security

Competency field

Competency field Operations