Australian Government

Department of Education, Employment and Workplace Relations

CPPSEC2018A Monitor electronic reporting facility

Release: 1

CPPSEC2018A Monitor electronic reporting facility

Modification History

Not Applicable

Unit Descriptor

Unit descriptor

This unit of competency specifies the outcomes required to monitor and maintain operational functions of an electronic reporting facility. It requires the ability to monitor and maintain a range of electronic security and telecommunications systems, receive, interpret and transmit information, and determine responses to security incidents.

This unit may form part of the licensing requirements for persons engaged in security operations 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 and monitoring 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 ***bold italicised*** 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 Monitor and maintain electronic security systems.	1.1 Applicable provisions of ***legislative*** and ***organisational requirements*** relevant to ***assignment instructions*** are identified and complied with. 1.2 ***Security systems*** are systematically monitored and tested to ensure performance is maintained within defined operating guidelines. 1.3 Actual or suspected ***faults*** or deficiencies in security systems are reported in accordance with organisational procedures. 1.4 Preventative and breakdown maintenance arrangements for security systems are confirmed with ***relevant persons***. 1.5 Back-up procedures to maintain security and integrity of security systems are implemented in accordance with organisational procedures. 1.6 Safe workplace practices are identified and complied with in accordance with Occupational Health and Safety (OHS) requirements.
2 Process and organise data.	2.1 Data is received, interpreted and processed in accordance with organisational procedures. 2.2 Data is entered, checked for accuracy and processed in accordance with organisational procedures. 2.2 Processed data is securely ***stored*** in accordance with organisational procedures. 2.4 Processing errors and deficiencies are identified and reported in accordance with organisational procedures.
3 Respond to incident.	3.1 Security incidents are assessed on reported information for degree of risk to persons, property and premises. 3.2 Appropriate ***response*** is formulated and implemented in accordance with organisational procedures. 3.3 Regular and systematic checks are made with field staff and situations requiring assistance are reported in accordance with organisational procedures. 3.4 ***Communication channels and processes*** are used to maintain a continual exchange of information with field staff. 3.5 Relevant ***documentation*** is accurately completed and securely maintained with due regard to confidentiality 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

- active listening
- communicate in a clear and concise manner using appropriate terminology
- communication skills to accurately enter, receive, interpret and transmit data
- communication to engage with minority groups (eg young people, old people, people with an addiction or disability, Indigenous Australians, people from Culturally and Linguistically Diverse (CALD) backgrounds)
- identify faults and errors and omissions in the operation of security systems and implement appropriate remedial action
- implement response procedures appropriate to reported security incident
- monitor and maintain basic security systems
- read and interpret technical data and specifications
- test security systems for operational performance.

Required knowledge

- approved communication terminology, codes and signals
- common security system faults
- communication channels and processes
- monitor and interpret received data
- operational and performance testing procedures for security systems
- phonetic alphabet
- range of security incident situations
- reporting and documentation procedures
- routine maintenance procedures
- security response procedures
- types, functions and operational requirements of security systems.

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 A person who demonstrates competency in this unit must be able to

assessment and evidence required to demonstrate competency in this unit	provide evidence of: • identifying monitoring functions and capabilities of electronic security systems • monitoring and maintaining security systems and carrying out routine maintenance • identifying and rectifying faults and errors • inputting data and confirming accuracy • conducting testing to confirm operational performance of security systems • determining appropriate response procedures from accurate interpretation of data.
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. Demonstration, 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:

- Australian standards and quality assurance requirements
- general 'duty of care' responsibilities
- 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.

Organisational requirements may relate to:

- 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
  - GPRS monitoring
  - GSM monitoring
  - IT monitoring
  - medical monitoring
  - radio monitoring
- incident and security risk response procedures
- monitoring centre door policy
- monitoring centre premise alarm policy
- monitoring centre time clock policy
- personal presentation requirements
- personal protection equipment
- reporting and documentation requirements
- resource and equipment requirements
- standing instructions
- subsequent or further alarms.

Security systems may include:

- alarms and signals
- access control systems
- alarm actioning sequence
- biometric devices
- break and enter reporting
- business equipment
- communications equipment
- computers and networked systems
- electronic screening equipment
- key register
- motion sensors
- patrol, static guard and foot patrols
- personal and asset tracking signals
- personal duress and hold up alarms
- shutters
- slow open or close alarms
- static alarms
- system alarms
- time management alarms
- traffic display
- video cameras and monitors.

***Faults* may include**:	• equipment and systems break-down • power failure • programming faults • reporting problems.
***Relevant persons* may include**:	• clients • colleagues • security system manufacturers • supervisors • technical personnel.
Data may be *stored*:	• by hard copies of computer generated documents • by hard copies of customer generated documents • in directories and sub-directories • on back-up systems • on CDs and DVDs • on hard and floppy disk drives.
***Response* may include**:	• dispatching field support staff • notifying emergency services • notifying relevant personnel.
Communication channels and processes may relate to:	• 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.
***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 Technical security