Australian Government
Department of Education, Employment and Workplace Relations

CPPSEC2024A Implement electronic monitoring procedures

Release: 1

INDUSTRY SKILLS COUNCILS
Creating Australia's Future

CPPSEC2024A Implement electronic monitoring procedures

Modification History

Not Applicable

Unit Descriptor

Unit descriptor	This unit of competency specifies the outcomes required to monitor and respond to information received from security equipment and systems. It requires the ability to accurately interpret information and implement appropriate responses to a range of security situations. Work is usually conducted from a secure electronic reporting facility, monitoring centre or control room. This unit may form part of the licensing requirements for persons engaged in monitoring information received from 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 involving the monitoring 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 ***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 data and information**.	1.1 Applicable provisions of ***legislative*** and ***organisational requirements*** relevant to ***assignment instructions*** are identified and complied with.
	1.2 ***Security equipment and systems*** are continually monitored for correct operation in accordance with manufacturer's instructions.
	1.3 ***Monitoring parameters*** of security equipment and systems are identified and complied with.
	1.4 ***Data and information*** is monitored on a systematic basis in accordance with assignment instructions.
	1.5 Security systems are routinely cross-checked with companion ***monitoring systems*** to ensure an accurate and reliable exchange of information.
	1.6 Faults or malfunctions in security systems are identified, corrected or reported for remedial action.
2 **Respond to data and information**.	2.1 Established ***communication channels and processes*** are verified with ***relevant persons***.
	2.2 Received information is identified and verified for reliability and accuracy in accordance with organisational procedures.
	2.3 Information is received and appropriate ***response*** determined and implemented in accordance with organisational procedures.
	2.4 Responses are prioritised and comply with established monitoring parameters.
	2.5 Changing circumstances are identified and variations to response procedures are implemented in accordance with organisational procedures.
	2.6 Personal limitations in carrying out response procedures are identified and assistance is sought relevant persons in accordance with organisational procedures.
3 **Complete monitoring activities**.	3.1 Change of shift procedures are carried out and ensure system and monitoring continuity in accordance with organisational procedures.
	3.2 Responses are accurately documented and presented for review in accordance with organisational procedures.
	3.3 Identified faults or deficiencies in security systems are 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

- apply safe and efficient work practices
- back-up security systems
- carry out basic data entry and keyboarding
- communicate in a clear and concise manner using appropriate terminology
- comply with relevant legislative requirements including licensing
- demonstrate understanding of basic numeracy
- determine and implement appropriate response to received information
- identify basic faults or malfunctions in operation of security systems
- interpret security codes and alarm signals
- monitor, evaluate and interpret data and information
- operate a range of electronic security alarm monitoring management software relating to electronic security systems and tracking equipment
- prepare and present written and computer-based information
- prioritise responses
- read and interpret data, information and instructions
- solve routine problems and make decisions according to set procedures
- use keypads and control panels.

Required knowledge

- approved communication terminology and codes and signals
- back-up procedures
- change of shift procedures
- client confidentiality requirements
- common faults and malfunctions in security systems
- computer software used for monitoring functions
- electronic equipment and system configurations and programs
- emergency procedures
- keypad and control panel types and functions
- monitoring and response requirements
- operational principles and functions of electronic security systems and equipment
- relevant legislative provisions including Occupational Health and Safety (OHS) and licensing requirements
- reporting, documentation requirements and processes

REQUIRED SKILLS AND KNOWLEDGE

- roles and responsibilities of emergency services
- routine problem solving strategies
- software templates for electronic security equipment and systems
- technical terminology
- verification procedures and requirements for confirming 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: • accurately completing and processing documentation relating to monitoring • carrying out monitoring activities in a systematic manner in compliance with legislative requirements • implementing procedures to verify accuracy and reliability of received information • interpreting security data and information and determining appropriate responses based on the information available • prioritising and responding promptly to data and information in compliance with monitoring parameters • recognising faults or malfunctions in security systems and telecommunications • using appropriate communication channels and processes to accurately receive and convey 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:

- applicable commonwealth, state and territory legislation which affects work such as:
  - workplace safety
  - environmental issues
  - equal employment opportunity

  - industrial relations
  - anti-discrimination and diversity
- Australian building codes and regulations
- Australian Communications Authority cabling standards
- Australian standards and quality assurance requirements
- award and enterprise agreements
- evidence collection
- freedom of information
- licensing arrangements and certification requirements
- privacy requirements
- relevant industry codes of practice
- telecommunications
- trade practices.

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**:

- change of shift procedures
- equipment, tools and material information:
  - features, functions and capabilities
  - manufacturer's instructions
  - warranties and guarantees
- personal protection clothing and equipment requirements
- reporting requirements
- response procedures
- security equipment and system information
- specific client requirements
- work schedules
- work tasks and procedures.

Security equipment and systems may include:

- access control systems
- audible and visual warning devices
- cameras and monitors
- commercial and residential alarm systems
- detection devices
- electric and mechanical fire safety and fire locking systems
- electronic locks and locking systems
- electronic readers
- electronic screen equipment
- intercoms and control panels
- security doors and door controls
- specialised access control systems eg biometrics.

Monitoring parameters may relate to:

- functions monitored
  - alarms
  - access times
  - levels of access
  - identity of person gaining access
- levels of integrity of systems
- passwords and codes
- recording functions
- response requirements
  - people to contact
  - emergency services to contact
  - armed guard or patrol send out
  - no action
- testing and report functions.

Data and information **may relate to**:

- AC power fail or low battery
- alarms
  - medical
  - fire
  - duress
  - access
  - hold-up
  - intruder
- isolations
- late to close or late to open
- plant and systems
- system messages
- tampering
- test signals

	• verbal and visual information
***Monitoring systems* may include**:	• audio equipment • computer terminal, screen and software • digital receivers • instrument panels • intercoms • monitors • printouts • radios • telephones • video cameras • video receivers.
***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.
***Relevant persons* may include**:	• clients • colleagues • equipment and systems manufacturers • maintenance technician • security consultants • security personnel • supervisor.
***Response* may involve**:	• dispatching field support staff • notifying emergency services • notifying relevant personnel.
***Documentation* may include**:	• activity reports • computer databases • faulty or malfunctioning systems and equipment • response reports • voice and video recordings • written and electronic reports.

Unit Sector(s)

Unit sector Security

Competency field

Competency field Technical security