|  |  |
| --- | --- |
| **UNIT CODE** | CPPSEC2XXX |
| **UNIT TITLE** | Monitor electronic security equipment and respond to alarm events |
| **APPLICATION** | This unit specifies the skills and knowledge required to monitor electronic security equipment and respond to alarm events. The unit relates to work in a monitoring centre and does not include training for specific security equipment, covered by *AS 2201.2-2004 Intruder alarm systems - Monitoring centres* which specifies requirements and a grading convention for monitoring centres and the operations, equipment and staff necessary to carry out monitoring of intruder alarm systems.The unit includes: * interpreting and complying with workplace procedures, policies and legal rights and responsibilities including workplace health and safety (WHS) to receive, interpret and transmit information using a range of electronic security and telecommunications systems
* checking equipment and systems to verify correct operation and data integrity, and resolving and reporting faults
* monitoring to receive, input, process and store electronic security data following workplace procedures
* recognising and responding to different and multiple alarm events and taking appropriate response actions to verify alarm status, resolve alarm and ensure security following workplace procedures and client instructions
* using written and spoken English and communication equipment to provide clear and accurate spoken instructions

It applies to people working under general supervision as members of a security team.This unit may form part of the licensing requirements for people engaged in security operations in those states and territories where these are regulated activities. |
| **PREREQUISITE UNIT** | Nil |
| **ELEMENTS** | **PERFORMANCE CRITERIA** |
| Elements describe the essential outcomes. | Performance criteria describe what needs to be done to demonstrate achievement of the element. |
| 1. Interpret and comply with procedures and legal requirements. | 1.1 Interpret and comply with workplace procedures and policies and legal rights and responsibilities for monitoring electronic security equipment, including WHS.1.2 Clarify own understanding of legislative and workplace requirements with relevant persons. |
| 2. Check equipment for correct operation. | 2.1 Check security equipment to ensure correct operation and connections following operating instructions.2.2 Identify actual or suspected faults or deficiencies in security equipment and report to relevant persons.2.3 Confirm preventative and breakdown maintenance procedures and conduct equipment back-up to maintain security and integrity of data. |
| 3. Receive, interpret, transmit and store electronic security data. | 3.1 Receive, interpret and transmit electronic security data following workplace procedures.3.2 Input data into security equipment and check to ensure accuracy following workplace procedures.3.3 Identify processing or transmission errors and take remedial action and report issues to relevant persons.3.4 Store security data securely to meet legislative and workplace requirements. |
| 4. Respond to alarm events and report security status. | 4.1 Recognise alarm event and follow procedures to action correct response to meet client instructions.4.2 Use communication equipment and interpersonal techniques to discuss alarm status with relevant persons.4.3 Action further response to resolve alarm event and maintain security following workplace procedures and client instructions.4.4 Report security status ensuring confidentiality of security information. |
| ***FOUNDATION SKILLS***A person demonstrating competency in this unit must have the following language, literacy, numeracy and employment skills:* language skills to:
	+ provide information using security industry terminology, codes and signals
	+ communicate in English
	+ communicate in a manner that is preferred and understood by the receiver and engages minority groups
* reading skills to interpret and follow:
	+ standard operating procedures and policies that clarify legal rights and responsibilities and WHS requirements
	+ technical equipment instructions that may be in written or diagrammatic form
* speaking and listening skills to:
	+ ask questions and listen to answers to gain information or confirm understanding when clarifying work tasks and responding orally to alarm events
	+ provide clear and accurate spoken instructions when responding to alarm activations
	+ accurately interpret voice messages
* numeracy skills to calculate and enter numerical data into security equipment
* problem solving skills to:
	+ troubleshoot equipment malfunctions and select appropriate remedial actions
	+ respond to multiple simultaneous alarm events
* self-management skills to plan tasks to meet job requirements and timeframes
* technology skills to:
	+ input, manipulate, retrieve and store electronic data in a variety of formats including databases
 |
| **UNIT MAPPING INFORMATION** | Supersedes and is equivalent to CPPSEC2018A Monitor electronic reporting facility |
| **LINKS** | Companion volumes to this training package are available at the VETNet website:<https://vetnet.education.gov.au/Pages/TrainingDocs.aspx?q=6f3f9672-30e8-4835-b348-205dfcf13d9b> |

|  |  |
| --- | --- |
| **TITLE** | CPPSEC2XXX Monitor electronic security equipment and respond to alarm events |
| **PERFORMANCE EVIDENCE** |
| A person who demonstrates competency in this unit must on two (2) separate occasions, monitor electronic security equipment and respond to four (4) different alarm events on each occasion. In doing this, the person must meet the performance criteria for this unit. |
| **KNOWLEDGE EVIDENCE** |
| To be competent in this unit, a person must demonstrate knowledge of:* standard operating procedures and workplace policies that ensure compliance with legislative and regulatory requirements including:
	+ duty of care
	+ licensing requirements and limits of own authority
	+ workplace health and safety (WHS)
* approved communication terminology, call signs and radio channels used in the security industry
* categories of alarm events and procedures for responding to each category
* customer service standards
* methods for verifying polling connections
* operational functions of electronic security equipment
* own competence to operate electronic security system as required by *AS 2201.2-2004 Intruder alarm systems, Part 2: Monitoring centres*
* procedures for door, alarms, time clock, subsequent and further alarms and monitoring
* procedures to back-up and protect security data
* the phonetic alphabet and how it is used
* types of alarm events that may require response such as duress alarms, intrusion alarms, air conditioning alarms, smoke alarms, vehicle global positioning system (GPS) and satellite tracking
* types of alarm transmission technologies including wireless and internet protocol (IP) monitoring and dialler monitoring
 |
| **ASSESSMENT CONDITIONS**  |
| Assessors must satisfy the requirements for assessors contained in the Standards for Registered Training Organisations. Assessment of performance must be undertaken in a simulated workplace or environment that reflects workplace conditions. Tasks are to be performed to the level of proficiency and within the time limits that would be expected in a workplace.Assessors are responsible for ensuring that the person demonstrating competency has access to:* specifications of assessment tasks to monitor electronic security equipment and respond to alarm events
* electronic security equipment in a monitoring centre environment
* standard operating procedures and workplace policies related to the security work role and which specify requirements for complying with industry legislation and regulations
 |
| **LINKS** | Companion volumes to this training package are available at the VETNet website:<https://vetnet.education.gov.au/Pages/TrainingDocs.aspx?q=6f3f9672-30e8-4835-b348-205dfcf13d9b> |

For inclusion in separate Companion Volume: Range Statements

|  |  |
| --- | --- |
| ***Workplace procedures, policies and legal rights and responsibilities*** may relate to: | * anti-discrimination and diversity
* *AS 2201.2-2004 Intruder alarm systems - Monitoring centres*
* client service standards
* code of conduct and ethics
* communication and reporting procedures
* duty of care
* industry codes of practice
* licensing requirements
* monitoring centre policies and procedures relating to:
* alarms
* door
* monitoring: e.g. GPRS, GSM, IT, medical and radio
* subsequent and further alarms
* time clock
* own role, responsibilities and authority
* personal presentation and grooming
* privacy and confidentiality
* telecommunications
* workplace health and safety (WHS) policies and procedures
 |
| ***Relevant persons*** may include: | * clients
* colleagues
* security personnel
* supervisors
 |
| ***Security equipment*** may monitor: | * alarms and signals
* access control systems
* alarm actioning sequences
* 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 relate to: | * connection or polling problems
* equipment and systems break-downs
* power failure
* programming faults
* reporting problems
 |
| Data may be ***received*** through: | * colours, lights and sounds
* devices
* electronic or numerical data
* electronic messages
* electronic signals
* telephone calls
* voice messages
 |
| 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 drives
* on secure internet servers
 |
| ***Security response*** may involve: | * communicating with clients
* communicating with relevant personnel
* inputting data into the security system
* notifying emergency services
* transmitting data or messages
 |
| Documentation may include: | * activity logs
* incident reports
* request for assistance forms
* security risk and incident details
* vehicle and personnel movements
* written and electronic reports
 |