Australian Government

Department of Education, Employment and Workplace Relations

CPPSEC3039A Identify and diagnose electronic security equipment and system fault

Release: 1

CPPSEC3039A Identify and diagnose electronic security equipment and system fault

Modification History

Not Applicable

Unit Descriptor

Unit descriptor	This unit of competency specifies the outcomes required to identify and diagnose faults in electronic security equipment and systems. It requires the ability to conduct fault-finding inspections and checks against normal operational performance and identify and diagnose faults. This work applies in extra low voltage as defined through the Australian Standards AS 2201 (1986) environments. This unit may form part of the licensing requirements for persons responsible for inspecting and testing security systems and equipment 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 inspection and testing of security equipment and 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 Prepare for diagnosis of faults.	1.1 Applicable provisions of ***legislative*** and ***organisational requirements*** relevant to ***assignment instructions*** are identified and complied with. 1.2 Assignment instructions and other ***relevant information*** is obtained and reviewed. 1.3 Appropriate ***interpersonal techniques*** are used to consult with ***relevant persons*** to determine extent of ***faults***. 1.4 Normal operational functions and performance parameters of ***security equipment and system*** are confirmed against specifications. 1.5 ***Tools***, ***equipment and materials*** are organised and checked for correct operation and safety. 1.6 ***Site access and specific site requirements*** are identified and confirmed with relevant persons in accordance with organisational procedures. 1.7 Potential and existing ***risks and hazards*** in the work area are identified and controlled in accordance with ***Occupational Health and Safety*** (***OHS***) requirements and own role, competence and authority.
2 Diagnose faults.	2.1 Suitable ***personal protection equipment*** is selected, used and maintained in accordance with OHS and organisational requirements 2.2 Equipment and system isolation requirements are complied with in accordance with OHS guidelines. 2.3 Networked security system components are checked and tested for operational performance in accordance with manufacturer's instructions. 2.4 Logical diagnostic and ***systematic fault-finding methods*** are applied to diagnose faults employing measurements and estimations of system operating parameters. 2.5 Suspected fault scenarios are tested as being the source of system problems. 2.6 Faults are diagnosed on the basis of an accurate assessment of test results, historical information and ***operational data***. 2.7 Specialist advice is sought as required to assist with fault diagnosis in accordance with organisational procedures.
3 Complete and report diagnosis.	3.1 Findings of fault diagnosis are documented and presented to relevant persons in accordance with organisational procedures. 3.2 Recommendations include options for fault rectification and are supported by verifiable data. 3.3 Presented information uses clear and concise language and meets organisational standards for style, format and

ELEMENT	PERFORMANCE CRITERIA
	accuracy. 3.4 Complex faults are referred for specialist advice in accordance with organisational procedures. 3.5 Work area is cleaned and restored in accordance with organisational procedures. 3.6 Waste is collected, treated and disposed of in accordance with organisational procedures. 3.7 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

- accurately identify and diagnose faults
- accurately identify and handle cables
- communicate in a clear and concise manner
- complete documentation
- demonstrate basic logic and lateral thinking processes
- download and upload digital information
- estimate and organise materials, tools and equipment requirements
- evaluate test results
- identify and comply with applicable legislative requirements including licensing
- identify and control workplace hazards
- identify and follow routine workplace safety procedures
- identify and report faulty equipment
- operate security equipment and systems
- organise and prioritise work tasks
- read a multimeter
- read and interpret plans and specifications
- solve routine problems
- test security equipment and systems
- use keypads and control panels
- use suitable tools and equipment, including hand and power tools and testing devices
- work in confined spaces.

Required knowledge

REQUIRED SKILLS AND KNOWLEDGE

- applicable legislative requirements including licensing and client confidentiality
- basics of circuit diagrams
- building construction methods and types
- cable identification methods and techniques
- circuit protection requirements
- common equipment and system faults
- earthing systems arrangements and requirements
- electrical concepts
- emergency procedures
- fault-finding techniques
- isolating and testing procedures
- keypad and control panel types and functions
- operational principles of data transmission networks
- procedures for accessing and storing tools, equipment and materials
- procedures for reporting malfunctioning or faulty tools and equipment
- reporting and documentation requirements
- requirements for compliance with Australian building codes and regulations and Australian Communications Authority cabling standards
- requirements for working at height and in a confined space
- risks and hazards associated with working with security equipment and systems
- safe workplace procedures
- technical terminology
- tests to confirm equipment and system operation
- types and functions of computer software
- types of security equipment and system configurations
- types, functions and features of security equipment and systems
- types, functions and features of tools and equipment including testing devices
- waste disposal procedures.

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	A person who demonstrates competency in this unit must be able to provide evidence of: • ascertaining normal performance of security equipment and

demonstrate competency in this unit	systems against specification schedules • cleaning and storing tools and equipment, reinstating work area in a clear and safe condition, and updating and submitting all required documentation in an accurate and prompt manner • conducting inspections and tests of security equipment and systems in a methodical manner and accurately identifying and diagnosing faults based on an assessment of test data, site variables, operational and historical information • following safe and efficient work practices in the use of tools and equipment and effectively managing risks and hazards in the work area • organising appropriate tools, equipment and materials to carry out checks and testing of a range of security equipment and systems • preparing and presenting accurate and concise documentation detailing fault diagnosis and repair recommendations based on verifiable 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. 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**:	• access to site and specific site requirements
	• equipment and system location information
	• equipment, tools and material requirements
	• personal protection clothing and equipment requirements
	• reporting requirements
	• security equipment and system information:
	  • features, functions and capabilities
	  • installation procedures
	  • manufacturer's instructions
	  • service and maintenance requirements
	  • type
	  • warranties and guarantees
	• specific client requirements
	• timeframes
	• work schedules
	• work tasks and procedures.

***Relevant information* may relate to**:	• historical performance information
	• operational data
	• site variables:
	  • equipment and system usage
	  • environmental conditions
	  • building structures
	  • client habits.

Interpersonal techniques may involve:	• active listening • being non-judgemental • being respectful and non-discriminatory • constructive feedback • control of tone of voice and body language • culturally aware and sensitive use of language and concepts • demonstrating flexibility and willingness to negotiate • effective verbal and non-verbal communication • maintaining professionalism • providing sufficient time for questions and responses • reflection and summarising • two-way interaction • use of plain English • use of positive, confident and cooperative language.
***Relevant persons* may include**:	• clients • colleagues • engineers and technicians

- equipment and systems manufacturers
- security consultants
- security personnel
- site managers or project managers
- supervisor.

***Faults* may be**:	• due to operational misuse • due to previous installation • electronic • environmental • mechanical • procedural • software-related.
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.
Security systems may be:	• computerised • electronic • mechanical • procedural.
***Tools, equipment and materials* may include**:	• cable testing equipment • circuit board cleaner • communications equipment • computer cables and leads • computers and computer software including back-up disks • crimp tools • drop sheet • file • glass break tester • hand tools • interface PCBs • ladder • multimeter • personal protection equipment • power tools • routers • spirit level.

***Site access and specific site requirements* may relate to**:

- access and egress points
- access codes, keys or passes
- building codes and regulations
- heritage requirements
- noise control
- obtaining security clearance
- OHS requirements
- time of access to site
- union requirements.

***Risks and hazards* may relate to**:

- chemical hazards eg battery corrosion
- exposed electrical wiring
- exposure to:
  - asbestos
  - building debris
  - dust
  - glass fibre
  - live power
  - natural and other gas build-up
  - noise
  - vermin
  - water
- manual handling
- non-compliance with building codes and regulations.

***Occupational Health and Safety* (*OHS*) *requirements* may relate to**:

- emergency procedures
- following confined spaces procedures
- implementation of safety policies and procedures:
  - chemicals, gas and vapour
  - isolation procedures
  - monitoring and testing procedures
  - use of personal protection equipment and clothing
  - work clearance procedures
- risk and hazard recognition
- safety training
- working with electrical wiring and cables
- working with tools and equipment.

***Personal protection equipment* may include**:

- breathing apparatus
- fire extinguisher
- first aid kit
- gloves
- head protection

- hearing protection
- knee pads
- masks
- safety boots
- safety glasses
- warning signs and tapes
- witches hats.

***Systematic fault-finding* methods may involve**:	• identifying fault in shortest time possible • progressively isolating fault • reviewing all available information • using a methodical approach • using testing equipment • verifying continued existence of problem.
Operational data may be found in:	• back-up information • central monitoring station records • maintenance documentation • manufacturer's instructions • software records • visual inspections.
***Documentation* may include**:	• faulty or malfunctioning tools and equipment • location of security equipment and system • materials used • recommendations for repair • security equipment and system faults • testing and inspection results • warranty conditions • work activity report • written and electronic reports.

Unit Sector(s)

Unit sector Security

Competency field

Competency field Technical security