Australian Government

Department of Education, Employment and Workplace Relations

CPPSEC4019A Identify and diagnose security system or network fault

Release: 1

CPPSEC4019A Identify and diagnose security system or network fault

Modification History

Not Applicable

Unit Descriptor

Unit descriptor

This unit of competency specifies the outcomes required to locate, identify and diagnose systems and network faults. It requires the ability to ascertain the normal operational functions and performance of a security systems or network, conduct fault-finding inspections and checks, systematically identify and diagnose faults, and accurately report findings.

This unit may form part of the licensing requirements for persons responsible for diagnosing faults and deficiencies of networked 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 application in those work roles involving the determining networked security systems faults and deficiencies. 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 operation.	1.1 Applicable provisions of ***legislative*** and ***organisational requirements*** relevant to determining networked security systems faults are identified and complied with.
	1.2 ***Assignment instructions*** and other ***relevant information*** is obtained and reviewed.
	1.3 Extent of faults is determined from reports and consultation with ***relevant persons***.
	1.4 Normal operational functions and performance parameters of networked security system are confirmed against specifications.
	1.5 ***Tools***, ***equipment and testing devices*** 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 Occupational Health and Safety (OHS) issues are identified and appropriate ***risk*** control measures are implemented in accordance with organisational procedures.
2 Diagnose fault.	2.1 Equipment and system isolation requirements are complied with in accordance with OHS guidelines.
	2.2 Networked security system components are checked for operation in accordance with manufacturer's instructions.
	2.3 Logical diagnostic and ***systematic fault-finding methods*** are applied to diagnose faults employing measurements and estimations of system operating parameters.
	2.4 Suspected fault scenarios are tested as being the source of system problems.
	2.5 Faults are ***diagnosed*** on the basis of an accurate assessment of test results, historical information and operational data.
	2.6 Specialist advice is sought as required to assist with fault diagnosis in accordance with organisational procedures.
3 Complete and report fault 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 accuracy.

ELEMENT	PERFORMANCE CRITERIA
	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
- apply safe and efficient work practices
- coaching and mentoring to provide support to colleagues
- communicate in a clear and concise manner
- conduct testing of security systems and networks
- demonstrate basic logic and lateral thinking processes
- estimate resource requirements
- identify and correctly handle cables
- methodically prioritise and organise work tasks
- read and interpret a multimeter
- read and interpret specifications, charts and diagrams
- solve complex problems related to networking and security systems
- work in confined spaces.

Required knowledge

- building construction methods and types
- cable identification and handling requirements
- common security systems and network faults
- common testing equipment for security systems
- confined space procedures
- earthing systems arrangements and requirements
- electrical concepts (voltage, current, resistance and impedance)
- fault finding techniques
- operational principles of security systems and networks

REQUIRED SKILLS AND KNOWLEDGE

- technical terms
- tests to confirm operational performance
- types, functions and purposes of diagnostic tools
- types, functions and specifications of security systems and networks and equipment.

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:

- confirming reported faults with client and ascertaining normal performance of security systems and network against specification schedules
- accurately identifying and diagnosing faults based on an assessment of test data, site variables, operational and historical information
- clearly identifying job requirements and organising appropriate tools, equipment and materials to carry out checks and testing of security systems and networks
- conducting inspections and diagnostic tests on a range of platforms in accordance with industry preventative maintenance and diagnostic policies
- preparing and presenting reports and documentation clearly and concisely 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:

- apprehension and powers of arrest
- Australian standards and quality assurance requirements
- cabling
- 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**:

- access to site and specific site requirements
- budget allocations
- completion dates
- job requirements and tasks
- resource requirements
- specific client requirements
- warranties and service information
- work schedules.

***Relevant information* may include**:

- client questioning details
- client records
- contract documents
- details of system checks
- equipment or product manuals or guides

	• log books • networked security system fault history, trending data and current fault report • software programme • specification schedules • system configuration diagrams and site installation records • test data.
***Relevant persons* may include**:	• client • equipment and system manufacturers • other professional or technical staff • security consultants • security personnel • supervisor.
***Tools, equipment and testing devices* may include**:	• back-up disks • communications equipment • computer • hand tools • personal protective equipment • software • test equipment (multimeter).
***Site access and specific site requirements* may include**:	• access and egress points, time of access • access codes, keys, passes, security clearances • building codes and regulations • heritage listings • noise control • OHS requirements • union requirements.
***Risk* relates to**:	• the chance of something happening that will have an impact on objectives.
***Systematic fault-finding* may involve**:	• identifies fault in shortest time possible • progressively isolating fault • reviews all available information • using a methodical approach • verifies continued existence of problem.
Fault-finding *methods* may include:	• equipment program • functionality tests • visual inspections.
***Diagnoses* may identify faults or deficiencies in**:	• hardware and software • input • output • running.

***Documentation* may detail**:	• adjustments and modifications undertaken • completion of work log • costings • equipment, software and hardware faults and diagnoses • materials used • recommended repairs or disposal of equipment • testing and inspection results • warranty conditions and allowances.

Unit Sector(s)

Unit sector Security

Competency field

Competency field Security and risk management