



Australian Government

Department of Education, Employment and Workplace Relations

CPPSEC4015A Maintain networked security system

Release: 1

CPPSEC4015A Maintain networked security system

Modification History

Not Applicable

Unit Descriptor

Unit descriptor This unit of competency specifies the outcomes required to manage the security and integrity of a networked security system. It requires the ability to develop a maintenance plan, monitor the performance and effectiveness of a system or network, and undertake preventative maintenance and repairs of equipment, software, hardware and components.

This unit may form part of the licensing requirements for persons responsible for maintaining 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 maintenance of networked 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 <i>bold italicised</i> 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 Formulate maintenance strategy.	1.1 Applicable provisions of legislative and organisational requirements relevant to maintaining networked security systems are identified and complied with. 1.2 Networked security system architecture and configuration documentation is obtained and reviewed. 1.3 Networked security system warranty status of components, software and hardware is determined. 1.4 Networked security system requirements to maintain operational effectiveness are determined. 1.5 Maintenance options are examined against budgetary constraints and assessed risk to business continuity. 1.6 Preventative and breakdown maintenance arrangements for networked security systems are determined and confirmed.
2 Monitor and maintain effectiveness of networked security system.	2.1 Occupational Health and Safety issues are identified and appropriate risk control measures implemented in accordance with organisational procedures. 2.2 Networked security system performance is monitored on a systematic basis and evaluated for operational effectiveness. 2.3 Security and access features of the networked security system are monitored to ensure security and integrity of information is maintained. 2.4 Operational irregularities or faults are identified, diagnosed and rectified in accordance with organisational procedures. 2.5 Performance and audit reports are reviewed on a regular basis and maintained in accordance with organisational procedures.
3 Implement preventative maintenance procedures.	3.1 Networked security system back-up procedures are implemented on a routine basis in accordance with manufacturer's instructions. 3.2 Anti-virus software is updated and maintained on a routine basis in accordance with organisational procedures. 3.3 Networked security system maintenance is scheduled and carried out with minimal disruption to surrounding environment and services. 3.4 Repairs or adjustments are undertaken in accordance with manufacturer's instructions and within scope of own competence.

ELEMENT**PERFORMANCE CRITERIA**

- 3.5 Complex faults or repair requirements outside area of competence are referred for specialist advice.
- 3.6 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

- apply best practice in the implementation of maintenance and preventative maintenance strategies
- apply safe and effective ergonomic workplace practices
- assess and analyse risk to client core business functions
- coaching and mentoring to provide support to colleagues
- conduct and interpret tests
- conduct technical diagnosis
- identify and rectify common network problems
- identify systems and network maintenance requirements
- interpret and evaluate the purposes and objectives of various features of systems and networks
- read and interpret technical information.

Required knowledge

- anti-discrimination
- back-up and security procedures, maintenance and diagnostic procedures, licensing and installation and purchasing procedures
- common systems and network performance problems
- data analysis techniques
- energy and resource conservation
- environmental protection
- equal opportunity
- industrial relations
- Occupational Health and Safety (OHS)
- organisational operating systems and networks
- principles of developing a maintenance schedule for a network
- relevant legislation from all levels of government that affects business operation
- systems and network administration, security and storage requirements

REQUIRED SKILLS AND KNOWLEDGE

- systems and network diagnostic tools and their functions
- types of equipment, software and hardware and their applications.

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 diagnosing and rectifying system irregularities and referring complex faults for specialist advice
- determining maintenance strategies and support processes to maintain the continuity of operations directly related to the core business functions of the client
- efficiently and effectively protecting, securing and maintaining networked client server environments and operating systems
- implementing an efficient and responsive maintenance strategy to ensure optimal operational performance of equipment and software
- monitoring and assessing comprehensive performance indicators to determine system performance and reliability in relation to both hardware and software.

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.
Networked security systems maintenance requirements may relate to:	• back-up procedures • maintenance of customised software • storage retrieval • updating of virus protection systems.
Maintenance options may include:	• 24 x 7 hours support • business hours only support • on-site response • remote diagnostics • return to depot • second level support • telephone support.
Risk relates to:	• the chance of something happening that will have an impact on objectives.
Security and access procedures may relate to:	• data inputting • search and browse authorities • viewing and operation • write permission.

Irregularities may include:

- intrusion attempts
- security intrusions
- systems and network malfunctions.

Diagnoses may identify faults or deficiencies in:

- hardware and software
- input
- output
- running.

Documentation may detail:

- costings
- equipment faults and diagnoses
- materials used, parts and components replaced
- operational details
- recommended repairs or disposal of equipment
- repairs and servicing undertaken
- testing and inspection results.

Unit Sector(s)

Unit sector Security

Competency field

Competency field Security and risk management