



Australian Government

Department of Education, Employment and Workplace Relations

CPPSEC4016A Install networked security system

Release: 1

CPPSEC4016A Install networked security system

Modification History

Not Applicable

Unit Descriptor

Unit descriptor This unit of competency specifies the outcomes required to coordinate and install a networked security system. It requires the ability to plan and manage the installation of a range of software, hardware and new components in a network, conduct appropriate testing to determine operational effectiveness and accurately identify faults and malfunctions.

This unit may form part of the licensing requirements for persons responsible for installing 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 installation 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 Prepare for installation.	1.1 Applicable provisions of legislative and organisational requirements relevant to installing networked security systems are identified and complied with. 1.2 Assignment instructions and networked security system parameters, specifications and performance requirements are obtained and reviewed. 1.3 Location and availability of networked security system components are confirmed in accordance with organisational procedures. 1.4 Site access and specific site requirements are identified and appropriate arrangements made with relevant persons in accordance with organisational procedures. 1.5 Relevant persons are consulted to ensure installation work is coordinated effectively with others in the work area. 1.6 Tools, equipment and testing devices are selected and checked for correct operation and safety. 1.7 Occupational Health and Safety (OHS) issues are identified and appropriate risk control measures implemented in accordance with organisational procedures.
2 Install networked security system.	2.1 Installation work is conducted using safe operating practices in accordance with OHS guidelines. 2.2 Relevant circuits are checked as being isolated where necessary in accordance with OHS guidelines. 2.3 Installation of cabling and associated components is completed and checked for compliance with relevant standards and building requirements. 2.4 Networked security system hardware, software and related components are installed in accordance with manufacturer's instructions. 2.5 Configuration of software and hardware is completed in accordance with manufacturer's instructions and assignment instructions. 2.6 Testing of networked security system is undertaken in accordance with manufacturer's instructions. 2.7 Test data is measured and assessed against performance parameters of networked security system.
3 Complete installation.	3.1 Work is completed in an efficient and effective manner within designated timeframes. 3.2 Notification of work completion is made in accordance with organisational procedures.

ELEMENT**PERFORMANCE CRITERIA**

- 3.3 Work area is cleaned and restored in accordance with organisational procedures.
- 3.4 Waste from installation procedures is collected, treated and disposed of in accordance with organisational procedures.
- 3.5 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 safe and environmentally aware work practices
- conduct systems and network performance testing
- drill, solder and weld
- identify faults and malfunctions
- methodically organise and prioritise work tasks
- read and interpret technical systems and network installation specifications
- solve routine problems
- use suitable tools and equipment, including hand and power tools
- work in confined spaces.

Required knowledge

- cable termination and connection procedures
- coaching and mentoring to provide support to colleagues
- confined space procedures
- electrical concepts
- installation hazards
- LAN capabilities
- OHS requirements and safe work practices
- operational principles of a range of systems and networks
- organisational and client confidentiality requirements
- requirements for compliance with Australian building codes and regulations and Australian Communications Authority cabling standards
- systems and networks installation procedures
- technical terminology
- types and functions of industry accepted network hardware and software

REQUIRED SKILLS AND KNOWLEDGE

- types of industry security products, devices and procedures
- types, functions and specifications of systems and networks.

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:

- interpreting and complying with all applicable statutory and legislative guidelines for installation of security systems and accurately completing all relevant documentation
- methodically organising installation tasks, and safely and efficiently following installation procedures
- carrying out checks to ensure integrity, security and safety of security systems or network
- organising correct tools and equipment and applying appropriate methods and safe operating practices to install a range of security system 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.

<i>Legislative requirements may relate to:</i>	• 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
---	---

- Organisational requirements may relate to:***
- relevant industry codes of practice
 - telecommunications
 - trespass and the removal of persons.
 - 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.
- Site access and specific site requirements may relate to:***
- 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.
- 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:

- communications equipment
- hand tools
- multimeter
- personal protective equipment
- power tools
- soldering iron
- terminating tools
- welder.

Risk relates to:

- the chance of something happening that will have an impact on objectives.

Hardware may be based on:

- micro, mainframe or mid-range platforms

Hardware may include:

- cables
- CD
- client servers (LAN)
- disk drives
- monitors
- peer to peer networks
- personal computers
- print servers
- printers
- routers
- scanners.

Software may include:

- in-house development or out-sourced development
- packaged software.

Documentation may detail:

- costings
- records of any adjustments to original installation plan
- records of equipment and system positioning
- records of faulty or malfunctioning tools and equipment
- records of materials used
- testing and inspection results.

Unit Sector(s)**Unit sector**

Security

Competency field

Competency field Security and risk management