



Australian Government

CPPSEC4015 Maintain networked security systems

Release: 1

CPPSEC4015 Maintain networked security systems

Modification History

Release 1 This version first released with CPP Property Services Training Package Release 9.0.

Supersedes and is equivalent to CPPSEC4015A Maintain networked security system. Updated to meet the Standards for Training Packages.

Application

This unit specifies the skills and knowledge required to maintain a range of networked security systems. It includes assessing system architecture and configurations and formulating suitable maintenance strategies against budgetary constraints and risks to continuity of client operations. It also includes monitoring system performance, performing back-ups and hardware and software updates, identifying operational irregularities and faults, and implementing required repairs and maintenance.

This unit is suitable for those using specialised knowledge to complete routine and non-routine tasks and using their own judgement to deal with predictable and sometimes unpredictable problems.

Legislative, regulatory or certification requirements apply in some states and territories to the provision of advice on security solutions, strategies, protocols and procedures. For further information, check with the relevant regulatory authority.

Pre-requisite Unit

None.

Unit Sector

Security/Risk management

Elements and Performance Criteria

Elements describe the essential outcomes.

Performance criteria describe what needs to be done to demonstrate achievement of the element.

1 Formulate maintenance strategy for networked security system.

1.1 Access and interpret key requirements of legislation, regulations and workplace policies and procedures, including work health and safety (WHS), and apply to work instructions to ensure compliance.

- 1.2 Review work instructions to confirm client and site requirements and work timeframes.
 - 1.3 Review *AS/NZS 2201.1:2007 Intruder alarm systems – Client’s premises – Design, installation, commissioning and maintenance* (AS/NZS 2201) to understand requirements associated with maintaining networked security systems and apply to work instructions.
 - 1.4 Review networked security system architecture and configuration documentation to confirm requirements to maintain operational effectiveness.
 - 1.5 Confirm warranty status of networked security system components, software and hardware.
 - 1.6 Assess maintenance options against budgetary constraints and risk to continuity of client operations.
 - 1.7 Finalise and schedule maintenance strategy that ensures optimal operational performance of networked security system and software.
- 2 Plan and organise work tasks.
 - 2.1 Plan and prioritise work tasks allowing sufficient time to meet work instructions.
 - 2.2 Select and organise required materials, tools, testing devices and equipment including personal protective equipment and check for safe and correct operation.
 - 2.3 Arrange access to networked security system in consultation with relevant persons.
 - 2.4 Identify hazards in the work area and apply risk control measures.
 - 2.5 Use safe work practices when working with electronic equipment and cables according to WHS requirements.
- 3 Monitor effectiveness of networked security system.
 - 3.1 Access networked security system with minimal disruption to services and others in the work area.
 - 3.2 Systematically monitor and assess networked security system operation against performance indicators to determine hardware and software performance and

		reliability.
	3.3	Monitor security and access features of networked security system to confirm information security and integrity.
	3.4	Review and maintain system performance and audit reports according to workplace requirements.
4	Implement preventative maintenance procedures.	
	4.1	Routinely implement networked security system back-up procedures.
	4.2	Routinely update and maintain anti-virus software and mechanisms to secure internet protocol networks.
	4.3	Carry out repairs or adjustments to networked security system within scope of own competence and according to maintenance strategy and manufacturers' instructions.
	4.4	Identify, diagnose and rectify system irregularities or faults and refer complex faults for specialist attention according to manufacturers' instructions.
5	Finalise maintenance and complete documentation.	
	5.1	Reinstate networked security system and confirm correct operation and connections.
	5.2	Notify completion of work to relevant persons.
	5.3	Complete maintenance documentation detailing repairs undertaken and identified faults according to workplace and regulatory requirements.
	5.4	Check tools and equipment for faults, wear or damage and rectify or report problems.
	5.5	Restore work area to original condition and remove waste caused by maintenance tasks.

Foundation Skills

As well as the foundation skills explicit in the performance criteria of this unit, candidates require:

- reading skills to interpret key requirements of:

- specifications for networked system architecture and configuration
- plans and specifications when locating networked security system and components for maintenance
- Australian standards and manufacturers' instructions
- numeracy skills to interpret multimeter readings when maintaining networked systems.

Unit Mapping Information

Supersedes and is equivalent to CPPSEC4015A Maintain networked security system.

Links

Companion volumes to this training package are available at the VETNet website -
<https://vetnet.gov.au/Pages/TrainingDocs.aspx?q=6f3f9672-30e8-4835-b348-205dfcf13d9b>

Assessment Requirements for CPPSEC4015 Maintain networked security systems

Modification History

Release 1 This version first released with CPP Property Services Training Package Release 9.0.

Supersedes and is equivalent to CPPSEC4015A Maintain networked security system. Updated to meet the Standards for Training Packages.

Performance Evidence

To demonstrate competency, a candidate must meet the performance criteria of this unit by maintaining three different networked security systems.

Knowledge Evidence

To be competent in this unit, a candidate must demonstrate knowledge of:

- workplace policies and procedures that ensure compliance with legislative and regulatory requirements when maintaining security systems:
 - licensing requirements and limits of own authority
 - requirements for complying with Australian Communications and Media Authority cabling rules
 - regulatory requirements in the jurisdiction of operation
 - work health and safety
- cable identification, termination and connection procedures associated with repairing networked security systems
- common computer commands used to verify and manage internet protocol and network performance
- documentation to be completed when maintaining security systems to ensure compliance with licensing and warranty requirements
- fundamentals of routers, switches, firewalls and wireless access points
- fundamentals of scripting language
- keypad and control panel types and functions for a range of security equipment and systems
- local area network and wide area network capabilities
- meaning of multiple form factor authentication
- principles of security system networking and integration including IP addresses and devices
- methods for ensuring IP networked systems and equipment are properly secured

- maintenance procedures for a range of networked security systems and repairs permitted within scope of own role, authority and competence
- maintenance strategies for networked security systems
- methods for reinstating networked systems and equipment and ensuring they are properly secured over IP networks
- security equipment calibration requirements
- techniques for recognising routine and complex faults in networked security systems
- tests to confirm security system functionality
- tools and equipment including personal protective equipment (PPE) used when maintaining networked security systems
- types, functions and features of a range of networked security systems and components:
 - access control systems
 - audible and visual warning devices
 - cameras and monitors
 - commercial and residential alarm systems
 - detection devices
 - electronic 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
- types of earthing systems used in electrical installations
- typical hazards encountered when maintaining networked security systems and the control measures for each:
 - confined spaces
 - electrical
 - hazardous materials and chemicals
 - hidden utilities
 - people in the work area
 - power tools
 - vermin.

Assessment Conditions

Assessors must meet the requirements for assessors contained in the Standards for Registered Training Organisations.

All individuals engaged by a licensed RTO for security licensing purposes must hold both a security trainers licence (where such a licence exists within the relevant jurisdiction) and the licence for performing the security activities for which the individual is providing training or assessment. Regulators may impose other assessor conditions to meet jurisdictional assessment requirements.

Assessment must be conducted in the workplace or in a simulated workplace environment. Candidates must have access to:

- legislation and licensing requirements that apply to maintaining networked security systems in the jurisdiction of operation
- work instructions, documentation, networked security equipment and systems, manufacturers' instructions, PPE and tools required to achieve the performance evidence.

Links

Companion volumes to this training package are available at the VETNet website - <https://vetnet.gov.au/Pages/TrainingDocs.aspx?q=6f3f9672-30e8-4835-b348-205dfcf13d9b>