Draft 0.1

This is a new unit to meet industry needs for skills and knowledge to protect networked security equipment and systems from cyber threats.

We are working with industry experts to ensure the unit:

- meets current and anticipated industry needs
- complies with current Standards for Training Packages
- is written in clear understandable English.

Information on our training package review and development process is available here: http://www.artibus.com.au/project-stage.

Summary of changes from current endorsed unit

New unit

Updates Feb 2019:
Privacy requirements included in knowledge evidence
Applied new code

Updates May 2019:
Minor updates to apply edits and incorporate feedback, eg to the licensing statement, assessment conditions info, knowledge, implementation guide links etc

Post EE:
Minor edits
Foundation skills modified to clarify requirements

Unit of Competency CPPSEC3053 Implement measures to secure IP networked security equipment and systems

Application

This unit specifies the skills and knowledge required to implement measures to secure internet protocol (IP) networked security equipment and systems to protect physical security systems from cyber threats. It includes confirming existing network arrangements, checking firewalls, network controls and protection levels, identifying vulnerabilities to cyber threats and implementing required controls to secure IP networked systems.

The unit is suitable for those with basic skills and knowledge undertaking routine work tasks under the direction of more experienced workers.

Licensing, legislative or certification requirements apply to advising on, supplying, installing, maintaining, monitoring, repairing and servicing security equipment in some states and territories. For further information, check with the relevant regulatory authority.

Prerequisite Unit

None.

Elements and Performance Criteria

1. Confirm security equipment and system network arrangements.	1.1	Review work instructions to confirm client requirements and equipment location and clarify issues with relevant persons.
	1.2	Review and comply with workplace policies and procedures and key regulatory requirements when carrying out work tasks.
	1.3	Inspect security equipment and system to clarify operational parameters and locate control panels and software.
	1.4	Obtain authorisations and information required to access IP network and system configurations.
2. Identify vulnerabilities and secure IP networked equipment and system.	2.1	Access IP network and system configurations for security equipment and system.
	2.2	Use network testing and monitoring tools and commands to check network connectivity and continuity and identify anomalies.
	2.3	Check firewalls and network controls and make required updates.
	2.4	Assess system protection levels to identify vulnerabilities to cyber threat.
	2.5	Check authentications, encryptions and supervision levels and make required changes to improve system protections.
	2.6	Perform software upgrades to install latest definitions.
	2.7	Complete work tasks and check to ensure IP networked security equipment and system is operating correctly.

3. Report results and complete documentation.	3.1	Notify work completion to relevant persons.
	3.2	Complete documentation detailing actions taken to secure IP networked security equipment and system according to workplace and regulatory requirements.
	3.3	Report identified cyber vulnerabilities and required remedial actions for specialist attention.
	3.4	Restore work area to original condition and remove waste caused by work tasks.

Foundation skills

Candidates require:

- reading skills to interpret key requirements of schematics and manufacturers' instructions for security equipment, systems and software
- numeracy skills to perform calculations in binary and hexadecimal number systems.

Unit Mapping Information

No equivalent unit.

Links

Companion Volume Implementation Guide:
https://vetnet.education.gov.au/Pages/TrainingDocs.aspx?q=6f3f9672-30e8-4835-b348-205dfcf13d9b

Assessment Requirements for CPPSEC3053 Implement measures to secure IP networked security equipment and systems

Performance Evidence

To demonstrate competency, a candidate must meet the performance criteria of this unit by implementing measures to secure two different types of internet protocol (IP) networked security equipment and systems and identifying at least two vulnerabilities to cyber threat for each system.

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 implementing measures to secure IP networked security equipment and systems:
    - licensing requirements and limits of own authority
    - privacy requirements
    - reporting
    - requirements for complying with Australian Communications Authority cabling standards
    - work health and safety
- common computer commands used to verify and manage IP and network performance
- common cyber threats attributed to IP networked security equipment and systems and solutions
- common ways that physical security systems can be breached by hackers:
    - monitoring protected areas and information through video surveillance systems
    - removing records from the security management system
    - taking control of locking and monitoring systems
    - turning off security systems
- documentation to be completed when implementing measures to secure IP networked security equipment and systems
- fundamentals of routers, switches, firewalls and wireless access points
- fundamentals of scripting language
- internet of things (IOT) devices and common security issues relating to IOT devices
- meaning of multiple form factor authentication
- principles of security system networking and integration including IP addresses and devices
- physical security system designs and configurations that offer security from cyber threats including multiple levels of protection:
    - authentication
    - encryption
    - supervision
- techniques for ensuring IP networked systems and equipment are properly secured

- types of network testing and monitoring tools and commands used to check network connectivity and continuity
- ways that physical security systems become vulnerable to cyber threats
- wireless technologies commonly found in modern security systems.

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:

- workplace policies and procedures, work instructions, documentation, IP networked security equipment, tools and software required to achieve the performance evidence.

Links

Companion Volume Implementation Guide:
https://vetnet.education.gov.au/Pages/TrainingDocs.aspx?q=6f3f9672-30e8-4835-b348-205dfcf13d9b