



Australian Government

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

Release: 1

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

Modification History

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

New unit.

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