



Australian Government

CPPSEC3025 Diagnose faults in advanced technology security equipment and systems

Release: 1

CPPSEC3025 Diagnose faults in advanced technology security equipment and systems

Modification History

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

Supersedes and is equivalent to CPPSEC2025A Sell security products and services. Updated to meet the Standards for Training Packages.

Application

This unit specifies the skills and knowledge required to diagnose faults in security equipment and systems that employ advanced technologies including biometrics, artificial intelligence (AI), robotics, smart technologies and video integration. It includes applying methodical diagnostic procedures, testing suspected fault scenarios, and assessing test results, historical information and operational data to diagnose faults and recommend options for rectification. This work applies in extra low voltage environments as defined in Australian Standard *AS/NZS 2201.1:2007 Intruder alarm systems – Client's premises – Design, installation, commissioning and maintenance* (AS/NZS 2201).

A person working at this level would be expected to take responsibility for organising and completing tasks assigned to them without close supervision.

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.

Pre-requisite Unit

Nil.

Unit Sector

Technical

Elements and Performance Criteria

Elements describe the essential outcomes.

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

1 Prepare to diagnose advanced technology

1.1 Review work instructions to confirm client requirements and diagnostic timeframes.

security equipment and system faults.	1.2	Review AS/NZS 2201 to understand regulatory requirements associated with diagnosing security equipment and system faults and apply to work instructions.
	1.3	Use questioning and active listening to gather information on type of security equipment and system, technologies involved and extent of fault.
	1.4	Review and follow workplace policies and procedures including work health and safety when carrying out work tasks.
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 and equipment including personal protective equipment and check for safe and correct operation.
	2.3	Arrange access to security equipment and system in consultation with relevant persons.
	2.4	Identify hazards in the work area and apply risk control measures.
3 Conduct advanced technology security equipment and system testing and diagnostic procedures.	3.1	Use safe work practices when working with electronic equipment and cables according to WHS requirements.
	3.2	Isolate security equipment and system according to workplace requirements.
	3.3	Confirm normal performance of advanced technology security equipment and system against specification schedules.
	3.4	Inspect and check advanced technology security system components and test operation according to manufacturers' instructions.
	3.5	Methodically apply diagnostic methods using measurements and estimations of system operating parameters.
	3.6	Check and test configurations and connections for equipment and system technologies following

- manufacturers' instructions.
- 3.7 Test suspected fault scenarios to identify source of system problems.
 - 3.8 Assess test data, site variables, operational and historical information to support fault diagnosis.
 - 3.9 Diagnose fault or seek assistance from relevant persons to meet work instructions.
- 4 Recommend options for fault rectification and complete documentation.
- 4.1 Document diagnosed faults and options for fault rectification that are supported by verifiable data according to workplace and regulatory requirements.
 - 4.2 Check tools and equipment for faults, wear or damage and rectify or report problems.
 - 4.3 Clean and restore work area and remove waste caused by work 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:
 - plans and specifications when locating equipment and system components
 - Australian standards and manufacturers' instructions.

Unit Mapping Information

Supersedes and not equivalent to CPPSEC3025A Identify and diagnose biometric system fault.

Links

Companion volumes to this training package are available at the VETNet website - <https://vetnet.gov.au/Pages/TrainingDocs.aspx?q=7e15fa6a-68b8-4097-b099-030a5569b1ad>

Assessment Requirements for CPPSEC3025 Diagnose faults in advanced technology security equipment and systems

Modification History

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

Supersedes and is equivalent to CPPSEC2025A Sell security products and services. Updated to meet the Standards for Training Packages.

Performance Evidence

To demonstrate competency, a candidate must meet the performance criteria of this unit by conducting testing and diagnostic procedures to identify a minimum of five faults on security equipment and systems which use at least two of the advanced technologies listed below:

- artificial intelligence (AI)
- biometrics
- robotics
- smart technologies
- video integration.

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 diagnosing faults in advanced technology security equipment and systems:
 - licensing requirements and limits of own authority
 - privacy requirements
 - reporting and documentation
 - requirements for complying with Australian Communications and Media Authority cabling rules
- work health and safety
- application of *AS/NZS 2201.1:2007 Intruder alarm systems – Client’s premises – Design, installation, commissioning and maintenance* (AS/NZS 2201) when diagnosing security equipment and system faults at client premises
- cable identification methods and techniques
- documentation to be completed when diagnosing faults in advanced technology security equipment and systems
- established threshold levels and their impact on security

- keypad and control panel types and functions for a range of advanced technology security equipment and systems
- materials, tools and equipment including personal protective equipment (PPE) used when diagnosing faults in advanced technology security equipment and systems
- methods for ensuring IP networked systems and equipment are properly secured
- operational parameters and diagnostic testing procedures for a range of advanced technology security equipment and systems:
 - AI
 - biometrics
 - robotics
 - smart technologies
 - video integration
- operational principles of data transmission networks
- types and functions of computer software associated with advanced technology security equipment and systems
- types of earthing systems used in electrical installations
- types of electrical connections and circuits encountered when diagnosing faults in advanced technology security equipment and systems, and circuit protection requirements
- typical hazards encountered when diagnosing faults in advanced technology security equipment and systems and the control measures for each:
 - confined spaces
 - electrical
 - hazardous materials and chemicals
 - people in the work area
 - power tools
 - vermin
 - work at heights.

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, advanced technology security equipment and systems, PPE, tools and materials required to achieve the performance evidence

- security equipment and system information to support diagnostic activities
- AS/NZS 2201.

Links

Companion volumes to this training package are available at the VETNet website -

<https://vetnet.gov.au/Pages/TrainingDocs.aspx?q=7e15fa6a-68b8-4097-b099-030a5569b1ad>