Title	**Demonstrate knowledge of electronic security fault location and diagnostics**		
Level	**4**	**Credits**	**5**

Purpose	This unit standard is intended for the training and assessment of people working in or intending to work in the electronic security industry and covers the knowledge and application of electronic security systems. People credited with this unit standard are able to demonstrate knowledge of: – techniques to identify the location and cause of faults in security systems equipment; – diagnostic equipment used in security system fault location; – sources of additional information to assist with fault remedies; and – managing customer relationships when performing system repairs.

Classification	Electronic Engineering > Electronic Security

Available grade	Achieved

Guidance Information

1 This unit standard has been developed for learning and assessment off-job.

2 Persons working or intending to work as a security officer or in related security employment may require a Security Guards Licence or, if an employee of a Security Guard Licence holder, a Certificate of Approval to be the Responsible Employee of a Security Guard. These licences are issued by the Private Security Personnel Licensing Authority available through: www.justice.govt.nz/tribunals/licences-certificates/pspla/.

3 Definitions
Component – any device, module, part, or sub-system of any security system.
Environmental – may include sunlight, heat sources, halogen lights, pets, drafts, insects, rodents, weather, electrical interference, lightning, radio interference.
ESD – Electrostatic discharge.
Industry practice – practice used and recommended by organisations involved in the electrotechnology industry.
LAN – Local Area Network.
LED – Light Emitting Diode.
Module – bus connected system component.

Safe working practices – work practices designed to prevent personal injuries and damage to equipment and plant. This includes practices relating to personal attire and use of safety clothing and equipment, use of machinery and tools, and handling of materials and waste.

4 References
Building Act 2004;
Electricity Act 1992;
Electricity (Safety) Regulations 2010;
Health and Safety at Work Act 2015 and associated regulations;
Private Security Personnel and Private Investigators Act 2010;
Privacy Act 1993;
Telecommunications Act 2001;
AS 2201.3:1991, *Intruder alarm systems, detection devices for internal use*;
AS 2201.4:1990, *Intruder alarm systems – Wire-free systems installed in client's premises*;
AS/NZS 2201.1:2007, *Intruder alarm systems – Client's premises – Design, installation, commissioning and maintenance*;
AS/NZS 2201.5:2008, *Intruder alarm systems – Alarm transmission systems*;
AS/NZS 3000:2007, *Electrical installations (known as the Australian/New Zealand Wiring Rules)*;
New Zealand Security Association (Inc), Codes of Practice available at https://security.org.nz/;
New Zealand Telecommunications Forum Incorporated cabling requirements;
Local territorial authority requirements;
and all subsequent amendments and replacements.

5 Guidelines for connection of intruder alarm systems to telephone lines are contained in *Access Standards Newsletters* issued periodically by Spark NZ Ltd, available from www.telepermit.co.nz.

6 Where not stated, evidence for the number and type of equipment chosen is left to the discretion of the assessor, but must be sufficient to assess competence in all outcomes of the unit standard.

7 Range
- a Candidates may refer to current legislation and Standards during assessment.
- b Demonstration of safe working practices in accordance with *safe and sound practice* are essential components of assessment of this unit standard.
- c All activities and evidence presented for all outcomes and performance criteria in this unit standard must be in accordance with:
  - i legislation;
  - ii policies and procedures;
  - iii ethical codes;
  - iv Standards;
  - v applicable site, enterprise, and industry practice; and,
  - vi where appropriate, manufacturer instructions, specifications, and data sheets.

Outcomes and performance criteria

Outcome 1

Demonstrate knowledge of techniques to identify the location and cause of faults in security systems equipment.

Performance criteria

1.1 Explain techniques used to diagnose faults in security systems in terms of how they would assist to identify the fault.

Range techniques include but are not limited to – observation, simulation, measurement, identification of function loss, comparison, and previous fault data including frequency of occurrence, manufacturer documentation and diagnostic data, built-in diagnostics, alarm indications, event logs.

1.2 Explain common techniques used to identify a faulty system component.

Range systematic testing, half split, loop back, transposition.

1.3 Identify possible external causes of a given fault.

Range may include but is not limited to − mechanical versus electrical, control circuit versus power circuit, environmental influences, module versus wiring and terminations, where appropriate alternatives listed in service diagnostics book or service manual.

1.4 Explain the requirement to prevent diagnostics affecting the operation of working systems.

Outcome 2

Demonstrate knowledge of diagnostic equipment used in security system fault location.

Performance criteria

2.1 Identify built in test equipment available in a given item of equipment.

Range may include but is not limited to – display indicators, built in test modes, user controls, system logs.

2.2 Explain testing tools for a simple LAN in terms of features offered.

Range LED Indicators, wire mapping, laptop, ping, packet trace tools.

2.3 Explain testing tools in terms of features offered.

Range multimeter, tone source.

2.4 Explain storage, transport, and handling of equipment in accordance with industry practice.

Range ESD damage, physical damage, moisture damage, packaging, labelling, securing in vehicle, temperature control, shock damage.

2.5 Explain self-validation methods used for test and diagnostic tools and instrumentation.

Range evidence of three methods is required.

Outcome 3

Demonstrate knowledge of sources of additional information to assist with fault remedies.

Performance criteria

3.1 Identify potential sources of diagnostic information and describe the limitations of the sources.

Range includes but is not limited to – customer description of occurrences, on-site fault records, manufacturer manuals and technical support, on-line forums, off-site fault records.

3.2 Explain the importance of maintaining an accurate fault history for security systems.

Outcome 4

Demonstrate knowledge of managing customer relationships when performing system repairs.

Performance criteria

4.1 Explain the importance of good working practices when performing system fault diagnostics.

4.2 Identify customer behaviours that could indicate tensions, and methods that could help reduce tensions when performing fault location and diagnostics.

Range indicators may include but are not limited to – vocal indicators, body language, unrealistic expectations, disinterest, obsessive behaviours.

4.3 Explain the importance of an escalation process for situations where customer expectations cannot be met.

Planned review date	31 December 2026

Status information and last date for assessment for superseded versions

Process	Version	Date	Last Date for Assessment
Registration	1	24 January 2019	N/A
Rollover	2	26 September 2024	N/A

Consent and Moderation Requirements (CMR) reference	0003

This CMR can be accessed at http://www.nzqa.govt.nz/framework/search/index.do.

Comments on this unit standard

Please contact Waihanga Ara Rau Construction and Infrastructure Workforce Development Council qualifications@waihangaararau.nz if you wish to suggest changes to the content of this unit standard.