Title	Develop data networking solutions to support electronic security systems		
Level	4	Credits	10

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 planning and installation of electronic security intruder alarm systems.
	People credited with this unit are able to:
	– confirm client's data networking support system requirements;
	– select data networking system type to support electronic security systems;
	– select components for data networking systems to support electronic security systems; and
	– lead the installation, commissioning, and handover of data networking system.

Classification	Electronic Engineering > Electronic Security

Available grade	Achieved

Guidance Information

1   This unit standard has been developed for learning and assessment on-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   References
Building Act 2004;
Electricity (Safety) Regulations 2010;
Health and Safety at Work Act 2015;
Health and Safety in Employment Regulations 1995;
Private Security Personnel and Private Investigators Act 2010;
Privacy Act 1993;
Telecommunications Act 2001;
AS 2201.2-2004, *Intruder alarm systems – Monitoring centres*;
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)*;
IEEE 802.11-2016, *standard for Information Technology —Telecommunications and information exchange between systems Local and metropolitan area networks— Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications;*
NZS 4512:2010, *Fire detection and alarm systems in buildings*;
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.

4   Definitions
Industry practice – practice used and recommended by organisations involved in the electrotechnology industry.
POE – power over ethernet.
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.
Structured cabling system – Cat 6, Cat 7 cabling or subsequent replacements.
UPS – uninterruptible power supply.
WAP – wireless application protocol.

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   The networking solutions may include several small network solutions, or one or more large network solutions, depending on the complexity of the network. The number and type of networking solutions is left to the discretion of the assessor, but must be sufficient to assess competence in all outcomes of the unit standard. To allow for sufficient evidence, it is expected that evidence will be collected over a period of time, typically one month or more.

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, drawings, and data sheets.

Outcomes and performance criteria

Outcome 1

Confirm client's data networking support system requirements.

Performance criteria

1.1   Identify the client's objectives and budget.

1.2   Use supplied job/project documentation to confirm with the client that the planned data networking system will support all requirements of the electronic security system(s).

1.3   Review the specification to identify and document specific system programming requirements.

1.4   Agree the installation timeframe and milestones with the customer, installation team, and any other trades.

Outcome 2

Select data networking system type to support electronic security systems.

Range   system types may include but are not limited to – fibre optic system, copper structured cabling system, wireless system;
evidence of two different system types is required.

Performance criteria

2.1   Select data networking system type to meet all installation requirements and ensure that it meets customer and electronic security system requirements.

2.2   Position or route the selected system type to maximise electronic security system effectiveness and reliability.

Outcome 3

Select components for data networking systems to support electronic security systems.

Performance criteria

3.1   Select data networking system components to meet all installation requirements and ensure that they are compatible and meet customer requirements.

Range   may include but is not limited to – router, modem, switch, hub, WAP, telecommunication outlets, rack/frame, patch panels, media converter, repeater, ethernet over power.

3.2   Establish connection requirements for the data networking system components.

3.3 Confirm power arrangements or POE for powered equipment are available and suitable.

Range includes but is not limited to – POE capacity, UPS.

3.4 Position selected components to maximise electronic security system effectiveness and reliability.

Range may include but is not limited to – environment, radio frequency interference, damp situations, segregation of services, monitoring link disconnect.

Outcome 4

Lead the installation, commissioning, and handover of data networking system.

Performance criteria

4.1 Explain installation requirements to supervised persons and any other trades.

Range may include but is not limited to – methodology, regulatory requirements, timeframes, health and safety, customer expectations, waste management, workflow, team roles, tool box meetings, tailgate meeting.

4.2 Ensure appropriate installation of cabling and cable support systems.

Range includes but is not limited to – penetrations sealed, weatherproofed, fire cell integrity, segregation of services.

4.3 Ensure appropriate installation of selected components and devices, and all operational software is current.

4.4 Power up and test system for initial operation.

4.5 Ensure system programming meets client's operational requirements and electronic security system requirements.

Range may include but is not limited to – firewall, modem, router, WAP, repeaters, managed switches.

4.6 Commission the system and prepare for handover to client.

Range includes but is not limited to – waste and unused materials removed, site left clean and tidy, system operational tests, site restored to client expectations.

4.7 Communicate equipment operation, warranty, test and maintenance schedule, and service options to the customer.

4.8   Complete the handover process and documentation in the agreed format and in accordance with customer and industry requirements.

4.9   Provide feedback to staff and management on project and performance of supervised staff.

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.