Title	**Develop solutions for electronic security access control 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 access control systems. People credited with this unit standard are able to: – confirm client's electronic security access control systems requirements; – select system components for electronic security access control systems; – select electronic security access control system peripheral devices; and – lead the installation, commissioning, and handover electronic security access control 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/NZS 3000:2007, *Electrical installations (known as the Australian/New Zealand Wiring Rules)*;
IEC 60839-11-1, *Electronic access control systems - System and components requirements*;

IEC 60839-11-2, *Electronic access control systems - Application guidelines*;
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 Definition
Component – any device, module, part, or sub-system of any security system.
Industry practice – practice used and recommended by organisations involved in the electrotechnology industry.
REX – request to exit.
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.

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

6 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.
d Three separate access control systems with three or more doors, at least one of which will have a two or more controllers in an integrated system.

Outcomes and performance criteria

Outcome 1

Confirm client's electronic security access control systems 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 all electronic security access control systems objectives have been identified.

1.3 Review the specification, 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 system components for electronic security access control systems.

Performance criteria

2.1 Select the system components to meet all installation requirements and ensure they are compatible.

Range may include but is not limited to – control modules, input modules, output modules, code pads, communications modules, network interface, anti-tamper devices, power supply and battery.

2.2 Establish connection requirements for the system components.

2.3 Confirm power supply capacity and cabling are suitable for the specified load.

Outcome 3

Select electronic security access control system peripheral devices.

Range peripheral devices may include but are not limited to – electric strikes, electric mortise locks, electromagnetic locks, V-Locks, power bolts, cable transfer hinges, door furniture, egress switches, point-to-point beam, vehicle detection loop, credential reader (key, card, tag), radio and infra-red transmitters, vehicle barrier, REX device, emergency release device;
evidence of five different devices across the three systems is required.

Performance criteria

3.1 Select devices to meet all installation requirements and ensure that they meet customer requirements.

3.2 Position selected devices to maximise system effectiveness and reliability.

Range may include but is not limited to – environment, pets, radio frequency interference, audible interference, vibrations, running water, monitoring link disconnect.

Outcome 4

Lead the installation, commissioning, and handover of electronic security access control system.

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.

Performance criteria

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

4.2 Ensure appropriate installation of cabling and cable support systems.

4.3 Ensure appropriate installation of selected components and devices.

4.4 Power up and test system for initial operation.

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

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, as-built documentation.

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.

Range includes but is not limited to – administration login and password, technician password, service and support details, backup management and system restoration, data archiving.

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

Replacement information	This unit standard replaced unit standard 5896.

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.