Title	Control access to the security designated areas of an airport using access control devices
Level	4	Credits	10

Purpose	This unit standard is intended for people who operate airport access control systems.
	People credited with this unit standard are able to: issue, enable, and disable access control devices for security designated areas of an airport; reconcile the enablement and disablement of access devices with an airport security database; and respond to unsuccessful attempts to gain access to security designated areas of an airport.

Classification	Aviation > Airport Operations

Available grade	Achieved

Guidance Information

1   Definition
      The term *airport* refers to aerodrome as per Civil Aviation Rules.

2   Reference to *enterprise procedures* means that all activities must comply with the requirements contained in the current airport exposition, current airport company manuals and procedures, and any relevant legislative and/or regulatory requirements, which may include but are not limited to: Civil Aviation Act 1990, relevant Civil Aviation Rules, New Zealand Defence Force (NZDF) Policy.

3   This unit standard may be assessed against in an aviation workplace in real or simulated situations, or in a training environment if simulated workplace conditions are able to be provided that reflect the standards of an aviation workplace.

Outcomes and performance criteria

Outcome 1

Issue, enable, and disable access control devices for security designated areas of an airport.

Range   duration of validity may include but is not limited to – temporary, permanent; devices may include but are not limited to – swipe cards, remotes, keys, key-in pads.

Performance criteria

1.1   Access control devices are issued in accordance with enterprise procedures.

1.2   Access control devices' enablement is in accordance with enterprise procedures.

1.3   Access control devices' disablement is in accordance with enterprise procedures.

Outcome 2

Reconcile the enablement and disablement of access devices with an airport security database.

Range   duration of validity may include but is not limited to – temporary, permanent; devices may include but are not limited to – swipe cards, remotes, keys, key-in pads.

Performance criteria

2.1   Variations between security database records and access control device status are detected in accordance with enterprise procedures.

2.2   Variations between security database records and access control device status are responded to in accordance with enterprise procedures.

Outcome 3

Respond to unsuccessful attempts to gain access to security designated areas of an airport.

Performance criteria

3.1   Security breaches are identified and responded to in accordance with enterprise procedures.

Range   response activity may include but is not limited to – notification to relevant airport staff.

3.2   Maintenance call-out in the event of a fault conforms to enterprise procedures.

Range   maintenance call-out may include but is not limited to – security system maintenance called.

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	17 December 1996	31 December 2016
Review	2	27 April 2000	31 December 2016
Revision	3	22 July 2005	31 December 2016
Review	4	21 November 2008	31 December 2016
Review	5	24 October 2014	31 December 2023
Review	6	29 July 2021	N/A

Consent and Moderation Requirements (CMR) reference	0028

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

Comments on this unit standard

Please contact ServiceIQ qualifications@serviceiq.org.nz if you wish to suggest changes to the content of this unit standard.