CIVIL AVIATION AUTHORITY
OF NEW ZEALAND
Te Mana Rererangi Tūmatanui o Aotearoa

Advisory Circular
AC139-18

Revision 0

20 April 2026

Aerodrome Security

General

Civil Aviation Authority (CAA) Advisory Circulars (ACs) contain information about standards, practices, and procedures that the Director has found to be an **acceptable means of compliance** with the associated rule.

Consideration will be given to other methods of compliance that may be presented to the Director. When new standards, practices, or procedures are found to be acceptable they will be added to the appropriate AC.

Purpose

This AC describes an acceptable means of compliance with sections of Civil Aviation Rule Part 139, *Aerodromes Certification – Operations and Use,* relating to security measures for aerodromes. It is intended for applicants and/or holders of:

- a security designated aerodrome operator certificate, and/or
- a non-security designated aerodrome operator certificate.

Operators of qualifying or non-certificated aerodromes could also refer to the sections on security advice on security measures that could benefit their aerodrome. Air Traffic Service organisations may also find this AC useful.

Related Rules

This AC relates to Part 139 – specifically Subpart D, *Aerodrome Security*.

Change Notice

This is the initial issue of this AC.

Published by
Civil Aviation Authority
PO Box 3555
Wellington 6140

Authorised by
General Manager, Strategy, Policy and International Engagement

Version History

History Log

Revision No	Effective date	Summary of changes
0	20 April 2026	Initial issue

Published by
Civil Aviation Authority
PO Box 3555
Wellington 6140

Authorised by
General Manager, Strategy, Policy and International Engagement

Table of Contents

Introduction

1. This AC contains guidance on Part 139 requirements for aerodrome security. It is intended for certificated aerodrome operators, but non-certificated aerodrome operators can also use the material as a guide to security measures they could implement. No matter how large or busy an aerodrome is, they all have a similar obligation: to prevent crimes against the Aviation Crimes Act 1972, and protect persons and property from dangers arising from such crimes, for example, an act of unlawful interference (AUI).

2. An aerodrome operator needs to create and maintain a safe and secure aerodrome environment by setting up safety and security programmes. While the aerodrome operator has this overarching responsibility, additional responsibilities for specific tasks may be shared between aerodrome operators or aviation security service providers[1], and other organisations at the aerodrome, such as government agencies, air operators, and its tenants.

3. There are many tenants on the perimeter boundary who have responsibilities. Aerodromes should work closely with their key partners to ensure principles of interoperability are applied and security outcomes for which each entity is responsible are achieved.

4. The collaborative nature of this work and the fact that anyone working at the aerodrome can notice security threats or vulnerabilities means the aerodrome operator needs to ensure open communications and good working relationships between all relevant organisations. This will ensure a robust and effective safety programme under Part 100 and security programme under Part 139.

5. Positive security culture promotes and maintains a secure environment that supports proactive and effective risk assessment and security practices.

6. New Zealand has both a 'National Aviation Safety Plan' (NASP) and a 'National Civil Aviation Security Programme' (NCASP). This AC should be read alongside the NCASP, which is designed for operators of both security-designated and non-security designated aerodromes. All certificated aerodrome operators have security responsibilities in accordance with the NCASP and should be familiar with the requirements. Aerodrome operators can request a copy of the NCASP from CAA at security.regulation@caa.govt.nz

***Note 1**: Only rules requiring compliance guidance and informative/explanatory material are included in this AC. Where a rule is self-explanatory, it is not covered in this AC.*

***Note 2:** For details of aerodrome safety programme requirements, see AC100-1, Safety Management.*

[1] AvSec, or an authorised aviation security provider certificated under Civil Aviation Rule Part 140.

Subpart A – General

Rule 139.3 Definitions

7. In addition to the definitions in rule 139.3, there are also relevant definitions in the Civil Aviation Act (CA Act) 2023, Rule Part 1, and Rule Part 12, and in the NCASP.

Abbreviations

ACE	Aerodrome certification exposition
AEP	Aerodrome emergency plan
AFM	Aircraft flight manual
AIC	Airport Identity Card
ASA	Airside security area
ASP	Aerodrome security programme
ATC	Air traffic control
AVP	Airside Vehicle Permit
AUI	Act of unlawful interference
AvSec	Aviation Security Service
CAA	Civil Aviation Authority
CCTV	Closed circuit television
IED	Improvised Explosive Device
NCASP	National Civil Aviation Security Programme
NPS	Non-passenger screening
OA	Operational area
PSR	Protective Security Requirements
SEA	Security enhanced area
SeMS	Security Management System
SMS	Safety management system

Rule 139.17 Deviations

8. To protect life or property, an aerodrome operator may deviate from certain requirements in other Part 139 rules, when this is necessary in an emergency. Aerodrome operators should, however, have processes in place to ensure that the integrity of aerodrome security measures is restored after the situation that led to the emergency being declared is over, and the emergency has been terminated.

9. The aerodrome operator must also write to the Director as soon as practicable, and no later than 14 days after the emergency, outlining the emergency, as well as the nature, extent and duration of the deviation, and why it was necessary.

Subpart B – Certification Requirements

Rule 139.69 Public protection

10. Aerodrome operators should ensure public protections by providing sufficient safeguards to deter the inadvertent entry of unauthorised persons, vehicles, and animals to the aerodrome's secure or operational area (i.e., airside).

11. The public protection requirement (rule 139.69) should be considered in conjunction with the security requirements in rule 139.203 and rule 139.205, below, to deter **intentional** unauthorised access. Operators must ensure that all access points, particularly in areas close to the terminals and/or passenger transport aprons remain secure, to prevent unauthorised access.

12. To support access control and reduce the risk of unauthorised access, access ways should be reduced so far as is reasonably practicable. A risk assessment can help determine whether an access way is necessary, identify any vulnerabilities it introduces to the aerodrome, and define appropriate mitigation measures to control these. Access ways from landside areas to airside security areas should be kept to a minimum.

13. Where the physical security provided by the barrier is insufficient to prevent intentional unauthorised entry, aerodromes should post signs on the barrier to deter entry, as per the examples in Appendix B. Aerodrome operators should also consider how unauthorised access is detected and enable a timely response to any intrusion.

Rule 139.75 Safety management

14. Aerodrome operators must set up and run a safety management system (SMS) which identifies hazards to aviation safety, and evaluates and manages associated risks, by putting in place mitigations to eliminate, isolate or reduce the risks to an acceptable level.

15. Operators could implement a Security Management System (SeMS), integrated with their SMS, which would address security vulnerabilities in the same way, as many of the processes and tasks are similar. The risk assessment process could then also be expanded to evaluate security risks and to focus on minimising vulnerability in the operating environment, because these risks affect the safety of an aerodrome.

Note: *There is more information about how to develop, operate and maintain an SMS in* *AC100-1,* Safety Management.

16. An aerodrome operator should start their risk evaluation and assessment processes by obtaining information about the layout and installations at the aerodrome, to identify points at which the aerodrome infrastructure and any aircraft are most vulnerable to an AUI.

17. When there is a need to conduct a risk assessment, aerodrome operators are encouraged to consider how their communication with the aerodrome community

stakeholders could relate to the risk assessment process, noting many have overlapping security responsibilities and subject matter expertise.

18. Open reporting from the aerodrome community is encouraged to ensure information sharing is free-flowing, and that suggestions and observations from members across aerodrome are sent upstream. Ways to do this could include setting up a dedicated mailbox, or team for workers on the aerodrome to contact about security concerns. Acting on these concerns, and communicating changes made, keeps people safe.

19. CAA's website has detailed advice, guidance and tools to support establishing and maintaining a positive security culture. See:

    https://www.aviation.govt.nz/safety/security-guidance/security-culture/enhancing-your-organisations-security-culture/security-culture-guidance/

Rule 139.77 Aerodrome certification exposition (ACE)

20. AC139-2, *Aerodrome certification exposition*, has guidance on drafting an ACE, in particular, a description of the security facilities and procedures that would comply with Part 139, Subpart D.

Subpart C – Aerodrome Operating Requirements

Rule 139.109 Aerodrome emergency plan (AEP)

21. Aerodrome operators are required to establish and maintain an AEP. This AC provides details on security-related emergencies, and should be read in conjunction with AC139-14*, Aerodrome Certification – Aerodrome Emergency Plan.*

22. Operators need to ensure that staff understand the requirements of the AEP and ensure it is tested regularly. ICAO guidance on security-focused exercises is for an aerodrome operator to conduct, at minimum, a full-scale security-focused exercise to test the AEP's capacity and capability to safeguard against an AUI at least every two years, with smaller-scale 'tabletop' security exercises more frequently.

23. The exercises and findings that result from debriefing sessions should be fully documented and assessed to identify additional needs or deficiencies in the AEP. These documents should be shared with relevant stakeholders involved in the exercise to elicit their feedback and ensure any issues identified during exercising are corrected.

24. Rule 139.109(2) has the option of either a full emergency exercise every two years, or a series of tests over a three-year period, culminating in a full exercise by the end of three years. This rule provides for all types of aerodrome emergencies. Aerodromes should consider where security-related emergencies fit into testing this requirement, which scenarios are more high-risk, which are high likelihood, and the frequency in which they have been tested.

25. The purpose of the exercise is to ensure that those involved with any operational response in an emergency are aware of the systems and processes in place, and to identify weaknesses. By analysing those weaknesses, operators can change and upgrade the AEP so that it is robust enough to manage an actual security emergency.

26. When planning exercises, it is important to include security emergencies that happen in both the airside and the landside of the aerodrome. The Director may declare, by appropriate notification, that an area within an airside security area is a security enhanced area.

27. ***Note:*** *"landside" means those parts of an airport, adjacent terrain and buildings or portions that are not* airside *security areas as declared by the Director of Civil Aviation, or operational areas. A "Landside Security Area" as defined in section 125 of the CA Act 2023 is different from the "landside", which are those areas not declared as airside security areas.*

28. Security-related themes and events can be included in a safety-focused emergency exercise. This is due to the similarities in the response, process, and agencies involved in managing SMS, and safety and security programmes. When the exercises

are conducted in this way, aerodrome operators must ensure core security practices and controls[2] are included, applied, and tested, as well as safety elements.

29. Aerodrome operators are encouraged to complete regular smaller-scale exercises, in addition to the full-scale exercise, on different portions of the security requirements in the AEP. Carrying out these exercises at least once a year helps personnel who are involved to maintain their skills and knowledge and provide for continuous improvement.

30. This enables the measures and procedures tested to be re-evaluated and adjusted to remedy potential vulnerabilities. Care should be taken and thought given to the 'need to know' principle when sharing information that identifies and discusses security vulnerabilities.

[2] Core security practices and controls include, but are not limited to, impacts on searching, patrolling, and infrastructure protection affecting the ongoing security of aircraft and the aerodrome.

Subpart D Aerodrome and navigation installation security

Rule 139.203 Requirements for Tier 1 security designated aerodromes

31. A Tier 1 security designated aerodrome is one that has been designated as such by the Minister of Transport in accordance with s 120 of the CA Act 2023.

Rule 139.203 (a), (b) & (c) Barrier requirements

32. Perimeter barriers and protection should be designed to deter and deny inadvertent or intentional unauthorised access, delay intrusion, and help to detect intrusion to any airside security area or security enhanced area within the aerodrome.

33. Aerodrome operators should consider not only the visible access points, but also hidden entry points such as any ducts, drains, or tunnels that could give access to the security or security enhanced areas. Any of these entry points must have appropriate access control applied to prevent intentional or inadvertent access.

34. The aerodrome operator should ensure that the boundary of the airside security area (i.e., the boundary between the airside security area, security enhanced area, and landside area) is clearly defined.

35. Noting the ability for the Minister to declare landside security areas in accordance with s 125 of the CA Act 2023, the aerodrome operator should also understand and clearly define its landside boundary.

36. Where landside security areas are required to be declared by the Minister, this is likely to happen at pace. As such, it is critical for all relevant parties to have rapid access to the information that supports a full understanding of where the aerodrome's landside areas extend to. Refer to 'Other Requirements' for further information relating to landside security.

37. Clear signs are required, as detailed in Appendix B of this AC. It should be clear to anyone in the aerodrome, even those who are not regular visitors, which areas they can and cannot enter. The other benefit of signage is to act as a notice as referred to in s 364, *Trespass*, in the CA Act 2023. This enables an appropriately authorised person to trespass an unauthorised person found on the aerodrome, if that person does not follow directives not to enter or not to remain in the airside security area or security enhanced area.

38. ***Note***: *To align with language changes in the CA Act 2023 relating to the types of security areas at aerodromes, some references to 'security areas' have been changed to 'airside security areas' in rule 139.203.*

39. Clearly marked boundaries help operators put effective safeguards in place to protect passengers, aerodrome staff, aircraft, and facilities. The best way to do this is to use security barriers that stop people entering airside security areas or security enhanced areas except through approved access points. When installing these barriers, aerodromes must ensure they do not interfere with aircraft operations, air navigation systems, or air traffic control facilities.

40. Barriers that delay, deter and/or deny access to the airside security area and security enhanced areas should:

- define the area to be protected, e.g., a perimeter fence which clearly divides the landside area from the security or airside area
- create a physical and psychological deterrent to persons attempting or contemplating unauthorised entry
- slow down intruders and enable operational and security staff time to detect, challenge and, if necessary, apprehend them
- provide designated and clearly identified entry points for people and vehicles, and
- keep the number of entry points to a minimum and secured or have positive access controls in place. Gates should be built to the same standard as perimeter fences.

41. Aerodrome operators may use buildings or other permanent structures as part of the physical security barrier where this is practical. When a building forms part of that barrier, the operator must ensure that any access through the building is properly controlled.

42. This includes making sure that doors, windows, roofs, ventilation openings, ducts etc remain securely locked or protected with bars, grilles, screens or other equivalent means. These protections are required when any such opening is less than three metres above ground level, or within three metres of any structure outside the security barrier.

43. The aerodrome operator should ensure barriers are regularly inspected and maintained, to make sure they are still effective. Issues that could weaken or compromise the barrier (such as environmental corrosion, which can be common in New Zealand) must be promptly addressed.

44. In addition to barriers, aerodrome operators may use extra security measures to better deter, delay, prevent, and detect unauthorised access. These measures can include barbed or razor-wire topping, perimeter intrusion detection systems, adequate lighting, and CCTV.

45. Security fences and other barriers should be designed and placed to deter and/or prevent people from climbing them, or from throwing sabotage devices, banned substances, or other unauthorised items onto or near an aerodrome. To ensure they are high and strong enough, barriers should be:

- at least 2.44 m high
- designed to be very difficult to climb, by using inclined barbed wire or razor-taped wire (subject to New Zealand's fencing regulations)
- made from material that resists bending, and
- constructed to prevent anyone lifting the barrier at the bottom to crawl or dig underneath; for example, by anchoring fence posts into the ground or securing the fence to a concrete base or sill.

46. Aerodrome operators must ensure that barriers to airside security areas always prevent inadvertent unauthorised access. These barriers should be:

- inspected regularly, based on a risk assessment that considers the local topography, surrounding environment, and any nearby activity, and
- maintained so they remain effective and in good condition.

47. Aerodrome operators may also take the natural environment into account when assessing security. In some locations, natural features can act as effective barriers and provide a comparable level of protection against unauthorised entry.

48. Natural barriers, such as cliffs, water or swamp, should be considered as part of the security design. Their use must be supported by a risk assessment. If these natural features do not provide an equivalent level of security, additional structural security measures are required.

49. ***Note***: *Further information can be found in the section on rule 139.207 concerning prohibited actions affecting security.*

Rule 139.203(d) - Other requirements for Tier 1 security designated aerodromes

Rule 139.203(d)(1) Isolated area for aircraft subject to unlawful interference

50. The aerodrome operator must identify an isolated parking area for any aircraft that is known or suspected to be subject to unlawful interference, or that needs to be separated from normal aerodrome activities for other safety or security reasons. This area should be chosen to minimise disruption to normal operations and to reduce the risk of harm to people, infrastructure, facilities, and other aircraft if there is a suspected IED or other threat on board.

51. When choosing the predetermined isolated area, operators should select a site that allows passengers to be evacuated quickly and safely, enables law enforcement officers and security personnel to carry out their duties effectively, and supports, so far as is reasonably practicable, the continuation of normal air traffic movements or the rapid return to normal operations once the incident is resolved. Operators should also identify a second isolated area in case the primary area cannot be used.

52. Isolated aircraft parking positions should be at least 100 metres from other aircraft parking positions, buildings, public areas, and similar locations, or as far away as practicable. The aerodrome operator should also ensure that these positions are not located above underground utilities such as gas lines, aviation fuel lines, or, where feasible, electrical or communication cables, or near storage facilities that may introduce additional risks. Floodlighting should be provided for any isolated parking position intended for use at night.

Rule 139.203(d)(2) & (3) Lighting and emergency lighting

53. Sufficient lighting deters potential intruders, since well-lit areas make intruders more noticeable and make it harder for any unauthorised person to access an aircraft without being detected.

54. To ensure lighting supports good security outcomes, aerodrome operators should refer to the lighting requirements specified in AC139-6, *Aerodrome Design Requirements (All Aeroplanes Conducting Air Transport Operations, All Aeroplanes above 5700 kg MCTOW)* and consider:

- whether the lighting is powerful enough to make any person approaching the aircraft clearly visible from a distance of 200 m with the naked eye
- whether lighting ensures that security enhanced areas and areas of potential security vulnerability are well-lit, with even lighting coverage so that there are no dark or blind spots, and
- if sensor-activated lighting is used, when any aircraft within the area is approached:
    - all approaches to the affected aircraft are covered by the sensors
    - the sensors are tamper-proof and provide instant lighting, and
    - vapour-filled lights requiring a warm-up period are not used, since they are not suitable in such situations.

55. At Tier 1 security designated aerodromes, all lighting should be:

- checked daily for damage with spare parts kept readily available
- powered by mains with a secondary supply should the mains power fail, and
- protected against unlawful interference.

56. For designated isolated parking areas, aerodrome operators must arrange for permanent and/or portable high intensity lighting for aircraft under threat of unlawful interference.

57. Where the areas are used at night, the lighting should be turned on within 30 minutes of the aircraft being brought to the area. If permanent lighting is not available, light from an alternative power supply or portable floodlights must be available within 30 minutes.

Rule 139.203(d)(4) and (4A) Areas for searching

58. Searching passengers and their cabin baggage is one of the most important measures for preventing threat items from being taken onto an aircraft. A core aviation security principle is that searching and sterile areas must be established and controlled so that searched and unsearched people, baggage, and items cannot mix.

59. Aerodrome operators should understand the threats and risks (including vulnerabilities) to the sterile area. Measures to ensure the integrity of the sterile area should include sufficient barriers, access controls, procedures, pathways and any signage necessary to prevent the mixing of searched and unsearched passengers, crew and things. This includes transit and transfer passengers, crew and their things.

60. As part of aerodrome development and planning, aerodrome operators should collaborate with other airport agencies and stakeholders. Aerodrome operators should establish and design areas in the aerodrome that support other organisations operating in the aerodrome to carry out their operations that achieve the security outcomes required by the rule.

61. Sections 232 and 241 of the CA Act 2023 require that airport operators consult substantial customers and relevant government agencies on spatial plans and put an obligation on the airport to provide a regulatory airport spatial undertaking (RASU) to the Secretary for Transport. This process is managed by the Ministry of Transport.

62. Aerodrome operators must make space available for the searching of passengers, crew and baggage. When providing areas for searching, the aerodrome operator should consider several factors, in collaboration with an aviation security service provider and other critical stakeholders. These include, but are not not limited to):

- the physical security searching equipment, surveillance equipment and supporting infrastructure necessary to achieve the desired aviation security outcomes. This can include x-ray machines, walk-through metal detectors, body-scanners, explosive trace detection systems, CCTV etc.
- any facilities before and after the screening point that would support persons subject to searching with any unpacking or packing of things, so that passenger flow is not unduly impacted. For example, benches are commonly installed at many airports after the screening points to enable passengers to clear the screening point and repack their things so as not to unduly delay the searching process.
- any facilities necessary to support and respectfully search passengers in sensitive situations. This could include passengers who need to adjust clothing for the purposes of a pat-down search, those with sensitive medical issues, situations where religious or cultural etiquette may need to be considered, or any other sensitive situation.
- flight scheduling, expected passenger volume and any impacts that may have on queues, ponding areas or crowded spaces and sterile area capacity etc.

63. The spatial requirements for aviation security delivery should be regularly reviewed to ensure they continue to be suitable.

64. Aerodrome operators are encouraged to consult CAA at security.regulation@caa.govt.nz when sterile areas and security enhanced areas are

being planned as early as practicable to ensure that necessary regulatory requirements are considered and integrated throughout the design process.

Rule 139.203(d)(5) Searching areas for domestic passengers

65. There may be cases where the Minister of Transport, or the Director of Civil Aviation, requires searching to occur for domestic passengers. When this is required, aerodrome operators must provide the space to enable the activities outlined in rules 139.203(d)(4) and (4A) and (5) to occur. This includes provision for screening points, sterile areas, and the separation of arriving passengers and crew from departing passengers and crew. This may include persons currently subject to domestic searching requirements, and/or passengers not currently subject to searching, depending on the nature of the security threat being responded to.

66. Aerodrome operators are expected to establish a contingency plan for how they would do this. There is no set standard for how fast aerodrome operators would need to set up a domestic searching area. However, security threats can move at an exceptionally high pace and without notice.

67. Changes to the threat environment may lead to almost immediate additional security requirements that could last for either an extended period or be reduced more gradually and over time. A contingency plan for enhanced domestic searching requirement(s) should be developed collaboratively with all critical stakeholders and include details of:

- where any required searching area(s) and security areas would be
- how these areas would be identified, designated, secured and controlled
- the necessary people and resources to implement and maintain any additional searching and security controls
- any additional technology, communications or infrastructure support that would be required, including how this would be implemented and notified
- any procedures necessary to support the contingency plan.

68. ***Note:*** *Further information on additional and scalable contingency measures that may be required in the event of threat level changes can be found in Appendix J of the NCASP. There is more guidance on AEPs in AC139-14, Aerodrome Certification – Aerodrome Emergency Plan.*

Rule 139.203(d)(7) Design of areas and access control

69. Aerodrome operators are responsible for controlling access to their aerodromes, particularly access to airside security areas. This requires collaboration with aviation security service providers, air operators and any other party with access control responsibilities and/or duties.

70. The aerodrome operator may agree that tenants or occupiers can manage access control for their concession or facility, where these form part of the landside and airside security area of any aerodrome, or through which access can be gained from landside to airside . The tenant or occupier should ensure that security controls are applied with respect to access through their concession or facility and that security controls are applied with respect to personnel, goods, supplies, equipment or vehicles.

71. Where this occurs, formal interoperability agreements should be established and overseen by the aerodrome operator. These agreements will ensure effective security controls are established and maintained, risks managed and that the aerodrome's requirements for access control continue to be met. This is also reinforced in rule parts 108.53 and 108.55.

72. Tenants or occupiers need to ensure that:

- access is restricted to only those persons with a legitimate operational need or requirement to enter the airside security area
- no unauthorised access of persons or vehicles is permitted
- no goods, supplies, items or things that could be used to compromise security are transferred from landside to airside, and
- access control measures are closely monitored to prevent unauthorised entry. Where methods such as lock-and-key systems are used, these need to be subject to strict controls.

73. The access controls for areas used for screening and sterile areas must be designed so that only authorised persons and things are allowed access. Any person entering these areas must be security searched through a screening point.

74. Where access control cards are provided by the aerodrome operator to authorised persons requiring access (or by a third party subject to any formal agreement with the aerodrome operator), the aerodrome operator should ensure that systems and processes are in place which positively link these access cards to the individual to whom they are issued, and prevent any unauthorised use, so far as is reasonably practicable.

75. This may include issuing access control cards which contain pertinent information such as the photograph and the name of the bearer, as well as the position, company and the expiry date of the card. So far as practicable, the expiry date for these access cards should be linked to the expiry date for an Airport Identity Card (AIC).

Rule 139.203(d)(8) Training

76. Aerodrome operators must ensure appropriate security training is provided to all aerodrome personnel, including those responsible for the implementation of landside security measures. Training methods can be varied, such as classroom-based sessions or online learning, complete with a competence assessment such as a quiz or a questionnaire.

77. Training must be tailored to different levels appropriate to the functions a specific person performs and must include training on security awareness, and where persons are responsible for implementing security controls (including landside security controls), the level of training necessary to support effective implementation of those controls. Airside workers will necessarily be required to complete more detailed training on their security requirements and responsibilities given their role requires access to airside security areas and security enhanced areas.

78. Aerodrome operators must ensure all organisations operating at the aerodrome receive appropriate security training from the aerodrome or have an approved

security training programme. One way to ensure this is for an aerodrome operator to make its in-house security training part of the application for aerodrome access, as it ensures everyone granted access by the aerodrome has been trained and assessed on their security responsibilities to a level that meets the standards required.

79. An organisation (including organisations only operating landside), may also, as part of its approval to operate at the aerodrome, supply its security training programme to the aerodrome operator for approval. Agreements for organisations to provide their own training should be recorded, and organisations need to be made aware that they must provide any updates to the security training to the aerodrome operator.

80. ***Note:*** More advice about training is contained in Appendix A of this AC.

Rule 139.203(d)(9) Identifying and reporting breaches and deficiencies in security procedures

81. Identifying and managing an aerodrome's security vulnerabilities and risks is a key part of an aerodrome's security management. Because it involves similar ongoing monitoring and assessment processes to managing an aerodrome's SMS, it may be possible to monitor risks to security along with risks to safety. Pro-active identification of system vulnerabilities is vital, to ensure available security resources can be focused on the highest priority risk areas.

82. The rule requires any breach of security procedures or deficiency in security at the aerodrome to be reported to the Director. This enables and supports the Director's requirement to maintain an awareness of threats and risks to aviation security, including vulnerabilities, that may be exploited to facilitate an attack. This rule is distinctly different to Part 12 requirements that have a higher threshold of security incident reporting.

83. Aerodromes must have procedures in place that are sufficient to identify breaches or deficiencies and report them to the Director. CAA encourages aerodromes to follow the 'Aviation Related Concern' process provided for here: Aviation concerns | aviation.govt.nz, and also forward information directly to security.regulation@caa.govt.nz.

84. Active reporting is a key part of managing security risks and vulnerabilities effectively. Further information and guidance on the importance of reporting systems can be found here: Reporting systems and incident response. The New Zealand Security Intelligence Service has also produced useful guidance to help identify signs of violent extremism, and New Zealand Police maintains guidance for detecting and responding to hostile reconnaissance.

Rule 139.203(d)(10) Security of services

85. When assessing security risks, aerodromes and operators of air traffic control facilities should consider services essential to the operation of the aerodrome or facility and support infrastructure. These services include suppliers or contractors coming to an aerodrome to make deliveries or undertake construction, maintenance and repairs.

86. International trends have highlighted increased awareness amongst terrorists of security weaknesses in aerodromes. These weaknesses leave aerodromes vulnerable to attack through energy, communications, cyber systems, water, sewerage and

access road systems. The threats posed by deliberate cyber-attacks on civil aviation also continue to rapidly evolve.

87. Aerodrome operators should:

- consider the potential for major civil disorder or sabotage to destroy or severely disrupt services essential to aviation operations, and
- consider their critical information and communication systems and, in accordance with a risk assessment, protect these from cyber-threats and risks that could lead to an AUI, and
- develop realistic contingency plans to keep people at the aerodrome safe and ensure essential operations can continue.

88. As the security environment changes, aerodromes may need to implement improvements in their security and cyber-security systems and further develop contingency plans. This is particularly relevant for infrastructure changes, which should be assessed through a security lens. The responsible organisations are encouraged to review aspects of security and cyber-security at least annually.

139.203(d)(11) Security perimeter signage

89. The Director may declare, by signs affixed to the perimeter of an area, that an area within a security designated aerodrome is an airside security area, and that an area within the airside security area is a security enhanced area.

90. Approved security signs must be displayed at security designated aerodromes and security designated navigation installations. These signs legally define the boundary or perimeter of the area and the protections afforded to the security areas of an aerodrome. In addition, they act as a form of deterrence.

91. The standards and specification of the security perimeter signage are outlined in Appendix B of this AC. For further information relating to airport signage, please contact signs@caa.govt.nz or visit the CAA website: Aviation security | aviation.govt.nz.

Rule 139.203(d)(12) Vehicle control

92. Operators of security designated aerodromes must ensure that unauthorised vehicles (and their occupants and things) are not granted access to airside security areas and security enhanced areas.

93. Vehicle control procedures should clearly state that only authorised vehicles and occupants may enter airside security areas and security enhanced areas. No prohibited items are allowed in these areas without lawful excuse. All occupants must carry a valid AIC in accordance with rule 139.209 and complete appropriate training such as the standard aerodrome security training outlined under rule 139.203(d)(8).

94. Non-service vehicles, i.e. vehicles not in aircraft service, such as tugs, are permitted to enter the aerodrome only if they require regular access. Aerodrome operators may require these vehicles to remain airside when not in use to minimise traffic at access points. An escort may be required to prevent entry into dangerous zones and mitigate against any risks to security.

95. The owner or operator of each authorised vehicle, along with their contact details and the vehicle registration, must be recorded. Approved drivers should also be

listed where possible. If this is not feasible, the aerodrome operator should require the vehicle owner to establish a procedure for identifying the driver at any given time.

96. Aerodrome operators should provide clear directions regarding the areas an authorised vehicle may enter and remain, the purpose of entry, and any restrictions on access points or conditions of entry. Vehicle operators should ensure these restrictions are documented and readily available to drivers and occupants during inspections.

97. Authorisation records for vehicles (also called AVPs) must have a clearly defined validity period based on the purpose and timeframe of access. These records should:

- Be displayed prominently at the front of the vehicle while in security areas.
- Be unique to the vehicle, showing the registration and authorisation expiry date.

98. Vehicle occupants' AICs and vehicle passes may be checked at entry points or while airside. Authorisation records should be retained for two years after expiry and stored so they can be retrieved when needed.

99. Any vehicles, occupants, or items entering, or within, security enhanced areas may be subject to non-passenger screening (NPS). Unattended, unidentifiable vehicles found in airside security areas should be treated as suspicious.

100. When an unattended or unidentified vehicle is found, aerodrome operators should determine how and when it entered, assess any related activities, and identify potential security risks. Appropriate actions must then be taken to mitigate those risks. If no concerns are identified, operators should attempt to locate the vehicle's owner or driver and address any vulnerabilities that enabled the entry. The vehicle may remain only if it presents no security risk and proper vehicle control procedures are in place.

101. Ambulances completing patient transfers to Air Ambulance flights will not be subject to the above requirements. Where the vehicle is transferring a patient, essential medical crew (including nurses, doctors, ICU specialists, midwives, etc.), and patient support persons directly to or from the aircraft, these vehicles should have the same priority as other emergency response vehicles to prevent operational delays.

102. Aerodrome operators are encouraged to promote a strong security culture in which vehicles are routinely kept locked or supervised, have their keys removed when left unattended, and remain locked whenever they are outside security or security enhanced areas.

Rule 139.205 Requirements for non-security designated aerodromes

Rule 139.205 (a)(1) Contingency planning

103. To ensure continuity of operations, aerodrome operators must maintain a contingency plan for implementing passenger, crew, and baggage screening and additional security

controls, when directed by the Director. An acceptable plan should be developed with reference to the guidance in rule 139.203, outlining the following:

- designated areas for screening passengers, crew, and baggage
- areas for non-passenger screening
- sterile areas that prevent screened persons from accessing unauthorised articles or unscreened individuals, and
- zones that allow for effective separation of screened and unscreened passengers and crew, including those in transit or transfer.

104. There is no prescribed timeframe for how quickly aerodrome operators must establish a domestic searching area; however, security threats can escalate rapidly and without warning. Shifts in the threat environment may require the immediate introduction of additional security measures, which could remain in place for an extended period or be scaled back gradually as circumstances allow.

105. A contingency plan for enhanced domestic searching requirement(s) should be developed collaboratively with all relevant stakeholders, to ensure areas provided would be effective in ensuring the security outcome required. The contingency plan should be regularly reviewed and amended to ensure it remains suitable.

Rule 139.205(2) Other security requirements

106. For information on lighting and emergency lighting requirements, refer to the section on rule 139.203(d)(2) and (3). For information on identification, reporting breaches and deficiencies in security procedures, refer to the section on rule 139.203(d)(9).

Rule 139.205(b)(1) and (2) Security awareness group

107. The purpose of a security awareness group is to promote understanding of security issues, methods, and practices at non-security designated aerodromes. This encourages a proactive and collaborative approach to implementing practical and effective security measures in the domestic aviation environment. It maintains an effective means of sharing security information among group members, typically representatives of organisations that operate at the aerodrome or hold related responsibilities, such as city or regional councils.

108. The aerodrome operator should hold security awareness group meetings at regular intervals, noting that the rule requires the gap between meetings to be no more than 12 months. Operators are encouraged to consider the intent behind this requirement and adopt a more frequent meeting schedule that supports proactive management of security awareness and the overall security culture.

109. The key functions of the security awareness group include reviewing the security of vulnerable points, such as essential equipment and facilities, assessing existing security measures to ensure they remain sufficient, evaluating current security risks and the effectiveness of controls, and considering the provision of security awareness training for those not employed, engaged, or contracted by the aerodrome operator.

110. The group is also responsible for recommending improvements to aviation security and ensuring that any proposals, recommendations, or initiatives arising from its work are communicated to all organisations operating at the aerodrome.

Rule 139.205 (c) and (d) Security training

111. Refer to the information contained above in the section on 139.203(d)(8) and Appendix A for further guidance.

Rule 139.207 Prohibited actions affecting security

112. This rule establishes prohibitions in relation to fences, gates and access controls; namely, that they must not be left open or insecure, and that any article which could be used to evade security controls must not be left in the vicinity.

113. To meet this requirement in practice, aerodrome operators should ensure that security fence lines are kept clear of any article, vehicle, stored equipment, or other material for at least 1.5 metres on both sides of the fence or barrier. This clearance should be measured on the outside, or landside, from a vertical line extending down from the extreme outer edge of the fencing structure, including any outriggers, and on the inside, or airside, from the outer edge of any post, brace, or other fencing support.

114. In situations where the area outside the fence cannot be kept fully clear because of a fixed obstruction, piece of equipment, or other object, the fence or barrier must still achieve the required level of security. This may include extending the barrier upward so that its height is at least 2.44 metres above the top of the obstruction.

Appendix A – Training

Any security training programme should ensure personnel at the aerodrome, whether landside or airside:

- are trained in good security practices and culture
- understand the principles and implementation of security awareness, and
- understand their responsibilities for aerodrome security.

Any training required under rule 139.203(d)(8) and/or 139.205(c)[3] is to be carried out by a person with the required knowledge, experience and competency in the subjects to be taught. Security awareness training should focus on developing and running training that fits the context of the overall security requirements of the aerodrome.

The aerodrome operator needs to decide appropriate initial and recurrent training needs for the different categories of personnel involved in security. Some parts of the training may be the same through all levels of the organisation, but others will need to be tailored to the needs of personnel in different roles.

A recommended method of matching the training needs of different personnel with the courses or modules available is a training matrix/register in which:

- each category of personnel whose activities involve security is listed on the vertical axis, and
- the various training modules available, and the areas for which training needs to be developed are listed on the horizontal axis.

This makes it easier for training planners to work out:

- what training modules or courses are available
- what else needs to be developed to ensure personnel are properly trained
- the areas each category of personnel need to be trained in, and
- the picture of security training needs across the organisation, by course, and also by who needs to do which course.

Operators need accurate records for every person who is trained. These should be more than a record of attendance and include information on:

- when a person was trained in each segment of training that is undertaken
- the method of assessment
- results of test or examinations or comprehension exercise
- a complete picture of that person's instruction, and

[3] Section 13(4) of the CA Act 2023 is also relevant.

- a full assessment of that person’s competence to understand and perform the security measures in which they have been trained.

As well as ensuring continued knowledge and competence, recurrent training, at no more than three-yearly intervals, should cover changes to:

- regulatory requirements and standards
- the organisation's procedures and programme, and
- threats affecting the organisation's operations.

The aerodrome operator must have procedures:

- that define the minimum required levels of competence for each topic
- to assess the results of training, such as presentations or examinations
- that show how trainers assess learners to ensure a person has been trained successfully.

Appendix B – Security Signage

Note 1: *These signs should be displayed prominently in operational areas that are not airside security areas or security-enhanced but are adjacent to them.*

Note 2: *The signs are subject to changes in legislation and the NCASP. Operators should keep up to date with changes to the NCASP to ensure they have the correct signage.*

Security designated aerodromes

Approved security signs must be displayed at security designated aerodromes and security designated navigation installations.

The Director of Civil Aviation may declare, by a sign or signs affixed at the perimeter thereof, that an area within any security designated aerodrome or security designated navigation installation is an airside security area, under the Civil Aviation Act 2023, section 121. The specifications for each sign shall be as follows:

Airside Security Area signs

<table>
<tr><td rowspan="5"><u>Class 1 Gate Signs</u>
 
</td><td>Size</td><td colspan="2">750 mm x 600 mm</td></tr>
<tr><td>Backing</td><td colspan="2">Of not less strength than 18-gauge aluminium</td></tr>
<tr><td>Fixing</td><td colspan="2">Securely fixed next to or on each perimeter fence gate, clearly visible at all times to pedestrians and persons in vehicles, whether the gate is open or closed</td></tr>
<tr><td rowspan="2">Text</td><td>AIRSIDE SECURITY AREA</td><td>60mm high letters in red printing on white background</td></tr>
<tr><td>ACCESS PROHIBITED - AUTHORISED PERSONS ONLY
AIRPORT IDENTITY CARDS MUST BE DISPLAYED
UNAUTHORISED PERSONS ARE LIABLE TO BE REMOVED OR ARRESTED</td><td>30mm high letters in black printing on a white background</td></tr>
<tr><td>DIRECTOR OF CIVIL AVIATION</td><td>10mm high letters in black printing on a white background</td></tr>
<tr><td rowspan="4"><u>Class 2 Fence Signs</u>
 
</td><td>Size</td><td colspan="2">750 mm x 200 mm</td></tr>
<tr><td>Backing</td><td colspan="2">Of not less strength than 18-gauge aluminium</td></tr>
<tr><td>Fixing</td><td colspan="2">Securely fixed to fences or barriers as follows:
(a) Adjacent to terminal buildings at not more than 30 m between signs.
(b) Along fence lines with direct access to public roads or other public areas at not more than 70m between signs.
(c) In more remote areas to which the public do not have access, not more than 200 m between signs.
(d) Where practicable they should be fixed approximately 1.5 m from ground level.
(e) On automatic or controlled access points to be so located that they are clearly visible to approaching persons/vehicles whether the gate is opened or closed.</td></tr>
<tr><td colspan="3"></td></tr>
</table>

	Text	AIRSIDE SECURITY AREA	60mm high letters in red printing on white background
		UNAUTHORISED ACCESS PROHIBITED	40mm high letters in black printing on a white background
		DIRECTOR OF CIVIL AVIATION	10mm high letters in black printing on a white background
Class 3 Door Signs 	**Size**	500 mm x 350 mm	
	Backing	Backing – Adhesive backing, to be firmly fixed on walls, doors or glass	
	Fixing	These signs shall be fixed at all access-ways leading to airside security areas so that the signs are clearly visible to all persons whether doors are open or closed.	
	Text	AIRSIDE SECURITY AREA	40mm high letters in red print on white or clear background
		ACCESS PROHIBITED – AUTHORISED PERSONS ONLY AIRPORT IDENTITY CARDS MUST BE DISPLAYED UNAUTHORISED PERSONS ARE LIABLE TO BE REMOVED OR ARRESTED	15mm high letters in black print on white or clear background
		Director of Civil Aviation	10 mm high letters in black print on white or clear background
Class 4 Door Signs 	**Size**	500 mm x 350 mm	
	Backing	Backing – Adhesive backing, to be firmly fixed on walls, doors or glass	
	Fixing	These signs shall be fixed at all access-ways leading to airside security areas so that the signs are clearly visible to all persons whether doors are open or closed.	
	Text	AIRSIDE SECURITY AREA	40mm high letters in red print on white or clear background
		PASSENGERS AND AUTHORISED PERSONS ONLY AIRPORT IDENTITY CARDS MUST BE DISPLAYED UNAUTHORISED PERSONS ARE LIABLE TO BE REMOVED OR ARRESTED	15mm high letters in black print on white or clear background

	DIRECTOR OF CIVIL AVIATION	10 mm high letters in black print on white or clear background

Security Enhanced Area signs

Class 1 Gate Signs 	**Size**	750 mm x 600 mm
	Backing	Backing – Of not less strength than 18-gauge aluminium
	Fixing	These signs shall be securely fixed adjacent to or on each perimeter fence gate, so as to be clearly visible at all times to pedestrians and persons in vehicles whether the gate is open or closed.
	Text	SECURITY ENHANCED AREA — 60 mm high letters in red printing on a white background
		ACCESS PROHIBITED - AUTHORISED PERSONS ONLY AIRPORT IDENTITY CARDS MUST BE DISPLAYED UNAUTHORISED PERSONS ARE LIABLE TO BE REMOVED OR ARRESTED — 30 mm high letters in black printing on a white background
		DIRECTOR OF CIVIL AVIATION — 10 mm high letters in black printing on a white background
Class 2 Fence Signs 	**Size**	750 mm x 200 mm
	Backing	Backing – Of not less strength than 18-gauge aluminium
	Fixing	To be securely fixed to fences or barriers as follows: (a) Adjacent to terminal buildings at not more than 30 m between signs. (b) Along fence lines with direct access to public roads or other public areas at not more than 70 m between signs. (c) In more remote areas to which the public do not have access, not more than 200 m between signs. (d) Where practicable they should be fixed approximately 1.5 m from ground level. (e) On automatic or controlled access points to be so located that they are clearly visible to approaching persons/vehicles whether the gate is opened or closed.

	Text	SECURITY ENHANCED AREA	60 mm high letters in red printing on a white background
		UNAUTHORISED ACCESS PROHIBITED	40 mm high letters in black printing on a white background
		DIRECTOR OF CIVIL AVIATION	10 mm high letters in black printing on a white background
Class 3 Open Boundary Signs Between security and SEAs within aerodrome operational areas  	**Size**	750 mm x 200 mm	
	Backing	Backing – Of not less strength than 18-gauge aluminium	
	Fixing	These signs are to be securely fixed as follows: (a) Adjacent to vehicle roadways within security areas where such roadways enter into the SEA. (b) At such a height and manner to be so located that they are clearly visible to persons driving approaching vehicles. (c) Adjacent to other points to which access can be formally gained to an SEA from the wider security areas with cognisance to the particular circumstances in question.	
	Text	SECURITY ENHANCED AREA	60 mm high letters in red printing on a white background
		SEARCHING MAY BE REQUIRED	40 mm high letters in black printing on a white background
		DIRECTOR OF CIVIL AVIATION	10 mm high letters in black printing on a white background
Class 4 Door Signs	**Size**	500 mm x 350 mm	
	Backing	Backing – Adhesive backing, to be firmly fixed on walls, doors or glass	
	Fixing	These signs shall be fixed at all access-ways leading to security enhanced areas so that the signs are clearly visible to all persons whether doors are open or closed.	
	Text	SECURITY ENHANCED AREA	40 mm high letters in red printing on a white or clear background

		ACCESS PROHIBITED – AUTHORISED PERSONS ONLY AIRPORT IDENTITY CARDS MUST BE DISPLAYED UNAUTHORISED PERSONS ARE LIABLE TO BE REMOVED OR ARRESTED	15 mm high letters in black printing on a white or clear background
		DIRECTOR OF CIVIL AVIATION	10 mm high letters in black printing on a white or clear background
Class 5 – Door Signs	**Size**	500 mm x 350 mm	
	Backing	Backing – Adhesive backing, to be firmly fixed on walls, doors or glass	
	Fixing	These signs shall be fixed at all access-ways leading to security enhanced areas so that the signs are clearly visible to all persons whether doors are open or closed.	
	Text	SECURITY ENHANCED AREA	40 mm high letters in red printing on a white or clear background
		ACCESS PROHIBITED – AUTHORISED PERSONS ONLY AIRPORT IDENTITY CARDS MUST BE DISPLAYED UNAUTHORISED PERSONS ARE LIABLE TO BE REMOVED OR ARRESTED	15 mm high letters in black printing on a white or clear background
		DIRECTOR OF CIVIL AVIATION	10 mm high letters in black printing on a white or clear background

Non-security designated aerodromes

Approved operational area signs should be displayed at non-security designated aerodromes. The specifications for each sign shall be as follows:

<table>
<tr><td rowspan="5"><u>Class 1 Operational Area</u>
 
</td><td>Size</td><td>390 mm x 490 mm</td><td>350 mm x 450 mm</td></tr>
<tr><td>Backing</td><td>Of not less strength than 18-gauge aluminium.</td><td>Adhesive backing, to be firmly fixed on walls, doors or glass</td></tr>
<tr><td>Fixing</td><td colspan="2">These signs shall be fixed at all access-ways leading to operational areas so that the signs are clearly visible to all persons whether doors are open or closed.</td></tr>
<tr><td rowspan="3">Text</td><td>OPERATIONAL AREA</td><td>40 mm high letters in red printing on a white background (aluminium) or white or clear background (adhesive)</td></tr>
<tr><td>UNAUTHORISED ACCESS PROHIBITED
PASSENGERS ONLY BEYOND THIS POINT
TRESPASSERS ARE LIABLE TO REMOVAL AND PROSECUTION</td><td>15 mm high letters in black printing on a white background (aluminium) or white or clear background (adhesive)</td></tr>
<tr><td>DIRECTOR OF CIVIL AVIATION</td><td>10 mm high letters in black printing on a white background (aluminium) or white or clear background (adhesive)</td></tr>
<tr><td rowspan="5"><u>Class 2 Operational Area</u>
 
</td><td>Size</td><td>390 mm x 490 mm</td><td>350 mm x 450 mm</td></tr>
<tr><td>Backing</td><td>Of not less strength than 18-gauge aluminium</td><td>Adhesive backing, to be firmly fixed on walls, doors or glass</td></tr>
<tr><td>Fixing</td><td colspan="2">These signs shall be fixed at all access-ways leading to operational areas so that the signs are clearly visible to all persons whether doors are open or closed.</td></tr>
<tr><td rowspan="3">Text</td><td>Operational Area</td><td>40 mm high letters in red printing on a white background (aluminium) or white or clear background (adhesive)</td></tr>
<tr><td>UNAUTHORISED ACCESS PROHIBITED
TRESPASSERS ARE LIABLE TO REMOVAL AND PROSECUTION</td><td>15 mm high letters in black printing on a white background (aluminium) or white or clear background (adhesive)</td></tr>
<tr><td>DIRECTOR OF CIVIL AVIATION</td><td>10 mm high letters in black printing on a white background (aluminium) or white or clear background (adhesive)</td></tr>
</table>

<table>
<tr><td rowspan="6"><u>Class 3 Operational Area</u>
 
</td><td>Size</td><td>240 mm x 790 mm</td><td>200 mm x 750 mm</td></tr>
<tr><td>Backing</td><td>Of not less strength than 18-gauge aluminium</td><td>Adhesive backing, to be firmly fixed on walls, doors or glass</td></tr>
<tr><td>Fixing</td><td colspan="2">These signs are to be securely fixed to fences or barriers as follows:
(a) Adjacent to terminal buildings at not more than 30 m between signs
(b) Along fence lines with direct access to public roads or other public areas at not more than 70 m between signs
(c) In more remote areas to which the public do not have access, not more than 200 m between signs
(d) Where practicable they should be fixed approximately 1.5 m from ground level
(e) On automatic or controlled access points to be so located that they are clearly visible to approaching persons/vehicles whether the gate is open or closed</td></tr>
<tr><td rowspan="3">Text</td><td>OPERATIONAL AREA</td><td>60 mm high letters in red printing on a white background</td></tr>
<tr><td>UNAUTHORISED ACCESS PROHIBITED</td><td>40 mm high letters in black printing on a white background</td></tr>
<tr><td>DIRECTOR OF CIVIL AVIATION</td><td>10 mm high letters in black printing on a white background</td></tr>
</table>