Civil Aviation Authority of Sri Lanka

Civil Aviation Authority of Sri Lanka, No 152/1, Minuwangoda Road, Katunayaka
Tele: +94-11-2358800, Fax: +94-11-2253038, e-mail: info@caa.lk, web: www.caa.lk

Aviation Security Directive

Document Classification: *Please mark (√)*	Top Secret		Secret		Confidential		Unclassified	√

Title: **Confidential Reporting System - Aviation Security Incidents**

Reference No: AVSEC/25/01/30 **S.N:** AVSEC. Dir. 008 **Date:** 20/04/2023

This Confidential Reporting System on Aviation Security Incidents is established for reporting of information concerning incidents related to Aviation Security to the Director General of Civil Aviation (DGCA), by following parties:

1) any holder of licence, certificate, permit, authorization or approval, issued or granted under reference to the Civil Aviation Act No. 14 of 2010; and
2) sources such as passengers, persons other than passengers, entities & organizations in the aviation system and general public

This system allows any person to submit Mandatory, Voluntary and Confidential incident reports and the system also provides for the gathering of information on aviation security from sources outside the quality control system, such as reports on a voluntary basis from passengers, persons other than passengers, entities & organizations in the aviation system and general public.

Any holder of licence, certificate, permit, authorization or approval, issued or granted under reference to the Civil Aviation Act No. 14 of 2010 and passengers, persons other than passengers, entities & organizations in the aviation system and general public, are to be followed by the content of the Annex A (6 pages) to this Aviation Security Directive.

Civil Aviation Authority of Sri Lanka
No.152/1, Minuwangoda Road,
Katunayake,
Sri Lanka.

P A Jayakantha
Director General of Civil Aviation and
Chief Executive Officer
Date: 20.04.2023

1. Introduction

1.1. Reportable aviation security incidents shall be identified as any security-related events that may detrimental to the interest of aviation security outcome that may increase the operational risk or endanger the safety of passengers, crew, ground personnel and the general public, or is a potential compliance breach of established security measures of the respective security programme. This includes the identification or observation of a vulnerability in the protection of civil aviation against acts of unlawful interference as well.

1.2. The aim of this reporting system is to contribute towards the enhancement of aviation security oversight system in Sri Lanka by providing a centralized system to capture outcome of security incidents in an effective and efficient manner, to protect and manage information, and to maintain the confidentiality of the information of the person submitting the anonymous or voluntary reports.

1.3. Hence, this Aviation Security Directive set out the required information that must be included in an incident report with the purpose of effective data collection and information contained in such reports allows the DGCA to capture and monitor aviation security incidents efficiently. The report also gather information that enables the DGCA to comply with its international obligations to report aviation security incidents to the ICAO - International Civil Aviation Organization as well.

2. Aviation Security Mandatory Incident Reporting Process

2.1. Every holder of licence, certificate, permit, authorization or approval, issued or granted under reference to the Civil Aviation Act No. 14 of 2010, shall report any Aviation Security Incidents, defined as follows to DGCA as early as possible;

a) a threat of unlawful interference with aviation
b) an unlawful interference with aviation
c) any event that may detrimental to the interest of security outcome of security measures
d) any event that a compliance breach of a security measure
e) any event that may increase the operational risk or endanger the safety of passengers, crew, ground personnel and the general public

2.2. Such incidents shall be reported by the respective entity as soon as possible, within 24 hours from the time of incident occur via telephone: + 94 112 358 832, mobile: + 94 773 115 977, email: davsec@caa.lk or Civil Aviation Authority (CAA) web portal - https://portal.caa.lk/caa-reporting/. Then an official report shall be submitted by the respective entity within 03 days of incident occurred to DGCA. This report shall contain as much of the following information with evidence.

a) description of the incident as originally reported
b) additional description information

c) class and category of the incident as per the aviation security incident categorization
d) immediate actions taken following the report of the incident
e) estimated consequences and perceived severity of the incident
f) plan of remedial or additional actions required
g) details of the entity providing the incident report

2.3. In parallel to this process, in-house Aviation Security Mandatory Incident Reporting Process shall be established for the staff by every holder of licence, certificate, permit, authorization or approval, issued or granted under reference to the Civil Aviation Act No. 14 of 2010. Outcomes of this process also shall be reported to DGCA.

3. Aviation Security Voluntary Incident Reporting Process

3.1. Events and activities that appear to be abnormal, unusual, strange, etc. in respect of Aviation Security could be notified to DGCA by passengers, persons other than passengers, entities & organizations in the aviation system and general public via telephone: + 94 112 358 832, mobile: + 94 773 115 977, email: davsec@caa.lk or CAA web portal - https://portal.caa.lk/caa-reporting/. This notification might contain as much of the following information.

a) description of the incident - precise as possible
b) location of the incident, date and time of the incident
c) name of the person reporting (Not mandatory); and
d) immediate action(s) taken (if any) upon the identification of the security incident, such as notifying local law enforcement and/or airport authorities of the situation.

3.2. In parallel to this process, in-house Aviation Security Voluntary Incident Reporting Process shall be established for passengers, persons other than passengers, entities & organizations in the aviation system and general public by any holder of licence, certificate, permit, authorization or approval, issued or granted under reference to the Civil Aviation Act No. 14 of 2010. Outcomes of this process also shall be reported to DGCA.

4. “Just Culture” Reporting System

4.1. This Reporting System promotes the ICAO’s “Just Culture” concept which refer to reporting systems through which aviation security incidents can be reported anonymously or confidentially to the DGCA, thereby allowing reporting individuals to be exempted from any kind of retaliation under specific circumstances. This system aim to encourage individuals to report incidents that would otherwise remain unnoticed and would therefore not been corrected.

4.2. Exemptions from punishment may be granted only in cases where the legal basis allows for such exemptions and where reporting individuals have not acted wrongfully on purpose or in culpable negligence. In case of serious security incidents which include incidents, deficiencies and breaches shall not be exempted from punishment will not normally be granted to perpetrators, even if they willingly reported the incidence.

4.3. Further the CAA hereby promotes the implementation of this “Just Culture” reporting system and recommends to encourage the implement a “Just Culture” reporting system in parallel to “Security Culture” principles within entities who are holders of licence, certificate, permit, authorization or approval, issued or granted under reference to the Civil Aviation Act No. 14 of 2010, by:

a) establishing a system that guarantees confidentiality of reporting individuals whereby personal data is not collected and/or stored. Where personal data is collected it should be used only to either gain clarification and further information about the reported incidents, or to offer feedback to the reporter;
b) identifying an independent body or person tasked with managing, maintaining and guaranteeing the confidentiality of data collections, as well as analyzing and following up on reports;
c) providing appropriate training on the functioning of the “Just Culture” reporting system, its benefits, and individuals’ rights, responsibilities and duties in relation to incidence; and
d) Implementing an incentive programme aimed at encouraging personnel to report aviation security incidence, while preventing malicious and defamatory reporting. Such a programme should also encourage personnel to provide constructive feedback on security measures with a view to improving the system as a whole and achieving greater security performance.

5. Aviation Security Incident Categorization – Taxonomy

5.1. Establishment of a clear categorization and taxonomy with harmonized procedure for reporting of aviation security occurrences and incidents, would encourage the aviation security incident reporting process and increase the probability of reporting of security incidents affecting civil aviation, which will result in the development of a strong security culture, since security data should ideally be categorized using taxonomies and supporting definitions so that the data can be captured and stored using meaningful terms.

5.2. Hence any holder of licence, certificate, permit, authorization or approval, issued or granted under reference to the Civil Aviation Act No. 14 of 2010 and passengers, persons other than passengers, entities & organizations in the aviation system and general public, are to be guided by following Aviation Security Incident Categorization – Taxonomy, while reporting aviation security incidents, in order to have a harmonized system with the quality of information and communication.

Incident Class: describes the topic the security incident would refer to.

Incident Category: indicates a more specific description of the security incident involved. The categories differ per class as the possible security incidents vary depending on which aviation security process they relate to.

Note: The Incident Class “Other” shall only be used when none of the other incident class or incident categories that seems to be suitable.

Incident Class	Incident Category
1. Access control	A. Breach or attempted breach of perimeter
	B. Unauthorized access to security restricted area (SRA) or other controlled area (non-staff)
	C. Unauthorized/unescorted access within SRA (staff)
	D. Suspicious behaviour of staff
	E. Deficiency in the access control system
	F. Deficiency in the ID pass issuing system
	G. Deficiency in the vehicle access control system including application of security controls and/or screening of occupants and vehicles
2. Hold Baggage	A. Discovery or use of prohibited item/IED
	B. Deficiency in protecting screened hold baggage
	C. Evidence of tampering of screened hold baggage
	D. Deficiency in the hold baggage screening (HBS) system or process (including passenger baggage reconciliation)
	E. Deficiency in the process of transportation of dispatched weapons
3. Passengers and cabin baggage	A. Discovery or use of prohibited item/IED
	B. Deficiency in the security checkpoint screening process
	C. Mixing of screened and unscreened passengers
	D. Suspicious behaviour
4. Aircraft protection on the ground	A. Unauthorized passenger on the aircraft
	B. Unauthorized staff on the aircraft
	C. Deficiency in the aircraft security search/check
	D. Deficiency in aircraft protection measures, including where aircraft are parked overnight
	E. Discovery or use of prohibited item/IED in the aircraft cabin or hold
5. Aircraft in-flight security measures	A. Unruly passenger (to be considered for level 3 and 4 (see ICAO Aviation Security Manual) only to be reported)
	B. Deficiency in the cockpit door process/protection
	C. Discovery or use of prohibited item/IED
	D. CBR attack
	E. Hijacking in flight
	F. Bomb threat in flight
6. Staff and crew	A. Deficiency in the security checkpoint screening process
	B. Discovery or use of prohibited item/IED
	C. Sabotage
	D. Insider bypassing security controls
	E. Deliberate attempt to circumvent vetting/background check regime

7. Cargo and Mail	A. Unauthorized access to cargo screening facility
	B. Deficiency in the screening process
	C. Discovery or use of prohibited item/IED
	D. Deficiency in protecting secured cargo
	E. Evidence of tampering of secured cargo
	F. Deficiency in the acceptance process
	G. Suspicious activity
8. In-flight supplies	A. Unauthorized access to in-flight supply facility
	B. Deficiency in protecting secure supplies
	C. Evidence of tampering of secured in flight supplies
	D. Deficiency in applying security controls
	E. Discovery or use of prohibited item/IED
9. Airport Supplies	A. Unauthorized access to facility
	B. Deficiency in protecting secure supplies
	C. Evidence of tampering of secured airport supplies
	D. Deficiency in applying security controls
	E. Discovery or use of prohibited item/IED
10. Landside Security	A. Discovery or use of vehicle-borne improvised explosive device (IED)
	B. Discovery or use of person-delivered IED
	C. Armed attack
	D. Unattended/suspicious items (also applicable airside)
	E. Chemical, biological and radiological (CBR) attack
	F. Damage to critical infrastructure/vulnerable points
	G. Suspicious behaviour
	H. Unplanned disruptions, including bomb threat or hoax
11. Air Traffic Control	A. Armed attack against air traffic control (ATC) facility
	B. Destruction or damage of air navigation aids
	C. Unauthorized access
12. Cyber Security	A. Attack against aircraft system(s)
	B. Attack against air traffic management (ATM) system(s)
	C. Attack against airport system(s)
	D. Attack against other critical systems and data
13. Unmanned aircraft systems (UAS) / Unmanned aerial vehicle (UAV) / Remotely-piloted aircraft system (RPAS)	A. Unauthorized incursion into controlled airspace
	B. Near miss/Encounter with aircraft in flight
	C. Strike/Collision with aircraft in flight
	D. Sighting from aircraft/airport
	E. Unmanned aerial vehicle (UAV) caused threat against aircraft
	F. UAV caused threat against airport infrastructure
	G. UAV caused threat against passengers
14. Stand-off weapon (MANPADs, etc.)	A. Attack on aircraft or airport facility
	B. Reported sighting

15. Lasers	A. Attack on aircraft or airport facility
	B. Reported sighting
	C. Suspicious activity
16. Aviation security information	A. Deficiency in protecting sensitive aviation security information
	B. Loss of integrity and availability of information systems
17. General Aviation/ Flying Schools/ Aero clubs	A. Unauthorized access
	B. Discovery of prohibited item/IED
18. Other	A. Other

****

Intentionally left blank