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: **Minimum Cybersecurity Baselines for Aviation Sector Entities**

Reference No: AVSEC/25/01/30 **S.N:** AVSEC. Dir. 009 **Date Issued:** 16/05/2025

This Directive provides practical guidance to holders of licenses, certificates, permits, authorizations, or approvals issued under the Civil Aviation Act No. 14 of 2010, to help them prepare for unforeseen cyber threats and implement best practices for mitigating and responding to such incidents.

With the ongoing transition from manual to digital systems, aviation operations are becoming increasingly vulnerable to cyber-enabled unlawful interference. The magnitude of this risk is closely tied to the degree of digitalization within the organization. Consequently, identifying system vulnerabilities and critical infrastructure is a fundamental step in enhancing cyber resilience.

Guidance

1. In accordance with the NCASP, all entities involved in civil aviation operations, shall identify their critical Information and Communications Technology (ICT) systems, as well as the data associated with these systems. Entities are also required to develop, implement, and maintain documented procedures specifying the measures in place to safeguard these systems.

2. Each organization should maintain a clear and well-defined exposition outlining its IT infrastructure and the associated human resources. In cases where administration is decentralized, each department must designate a responsible individual to act as the Chief Information Officer (CIO) or an equivalent point of contact.

3. All organizations should develop their own cybersecurity policy, incorporating the elements outlined in **Annex A**, which reflects the model cybersecurity policy proposed by ICAO.

4. It is recommended that all organizations identify and adhere to an established cybersecurity framework, such as NIST, ISO 20001, or the cybersecurity policies endorsed by Sri Lanka Computer Emergency Readiness Team(SLCERT).

5. Organizations shall implement measures to ensure the physical security of personnel, infrastructure, facilities, equipment, materials, and documents, safeguarding them against unauthorized access to protect critical information systems.

6. Staff members who have access to the core components of any digital system must undergo cybersecurity training. Staff who act as end users of such systems should receive awareness training on cyber threats and appropriate protective measures. Proof of such training should be documented and readily available.

7. All organizations or departments with Information Technology (IT) infrastructure, supporting civil aviation operations must be identified, including all associated assets—such as physical assets, personnel, critical information, and data.

8. All IT assets identified as per above point 7 must be recorded in the IT asset inventory.

9. It is recommended that a risk assessment be conducted at least annually to identify potential vulnerabilities. Entities may carry out the assessment internally or seek assistance from a government-recognized body, such as SLCERT.

10. Every entity must establish a written System Access Control Policy. This policy should define password requirements and specify access levels for each system.

11. Airport operators and airline operators are required to provide the following information upon request by CAASL inspectors or auditors.

    a) What systems are managed by the company, department, or section?
    b) Is the data being used encrypted?
    c) Is multifactor authentication implemented to protect systems from unauthorized access?
    d) Are all systems running licensed versions, and are they up to date? If not, what are the reasons for using outdated versions?
    e) Are all machines and servers used for civil aviation purposes equipped with antimalware software?
    f) Does the company use firewalls to safeguard its servers and other digital systems?
    g) Have you communicated guidelines to users regarding the safe and secure use of IT devices as part of your protection measures?

12. The company or department should establish a mechanism for reporting suspicious activities, vulnerabilities, thefts, or tampering with hardware and software files within the organization.

13. Any incident must be reported to CAASL immediately via the following online link: https://portal.caa.lk/avsec-reporting/index.php.

14. In the event of such an incident, comprehensive investigation reports shall be submitted to CAASL without delay by the entity relevant. Such documents will be classified as "**Top Secret**".

15. Every entity should develop and maintain a contingency plan to address various cyber threats, or incorporate security measures for emergencies into their existing contingency or emergency plan. Additionally, a disaster recovery plan should be developed for each potential situation.

All addressee please acknowledge receipt of this directive and its compliance status.

AVM Sagara Kotakadeniya (Retd)
Director General of Civil Aviation & Chief Executive Officer
Civil Aviation Authority of Sri Lanka

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

Enclosure Attachment : Annex A

Attachment : Annex A - Extract from ICAO - Cybersecurity Policy Guidance
Model Cybersecurity Policy

1. Introduction

1.1 This cybersecurity policy shall be the framework for further development and implementation of aviation cybersecurity. It shall be published, disseminated to relevant stakeholders, and periodically reviewed.

1.2 Further guidance material shall be developed to support the implementation of this cybersecurity policy.

2. Scope

2.1 Aviation cybersecurity shall address the security and resilience of the civil aviation system, as well as support the collaboration with concerned non-aviation entities and authorities, including national cybersecurity authority, national security, law enforcement and military, as appropriate.

2.2 Aviation cybersecurity shall be coordinated at the national level with aviation safety, aviation security, critical infrastructure protection, cyber defense and military.

2.3 Aviation cybersecurity shall be coordinated at the international level with equivalent Foreign Appropriate Authorities designated for Aviation cybersecurity.

3. Objectives

3.1 The overall objectives of this aviation cybersecurity policy are to ensure the security, resilience, and self-strengthening of the civil aviation system against cyber threats and risks, and to ensure the coordination of aviation cybersecurity with concerned national authorities and entities.

4. Governance and Organization

(Amended ICAO document para according to the organizational requirements)

4.1 In this chapter, the entity shall ensure the following requirements are implemented in accordance with the instructions outlined in this Directive.

a) define, support, and monitor the implementation of the cybersecurity culture programme within the organization;
b) define regulations, processes, requirements, and roles for cybersecurity crisis management according to the organization infrastructure.

5. Risk Management

5.1 Cybersecurity shall be intelligence driven, threat based and risk managed.

5.2 Risk management shall be an integral part of overall systems' life cycle.

5.3 All data and systems shall have identified ownership at all times.

6. Critical Systems Security

6.1 Critical functions, systems, and infrastructure shall be identified through risk management processes.

6.2 Security by design approach, coupled with Defense in depth principles, shall be applied to protect critical systems.

6.3 Redundancy of critical systems shall be considered as an enabler for system security.

7. Data Security

7.1 Data and information shall be protected during storage and transmission, in line with its sensitivity profile.

8. Supply Chain Security

8.1 End-to-end management of software/hardware supply chain shall be part of aviation cybersecurity management.

8.2 Software and hardware used in critical aviation functions shall comply with cybersecurity requirements throughout the life cycle of aviation systems.

9. Physical Security

9.1 Physical security (including personnel security) shall be part of aviation cybersecurity management.

9.2 Physical security shall safeguard people, infrastructure, facilities, equipment, material, and documents from unlawful interference and protect critical aviation systems from unauthorized physical access.

9.3 Physical security shall contribute to risk management through supporting the identification of threat actors and/or the likelihood of attacks on civil aviation critical infrastructure.

10. Information, Communication, Technology (ICT) Security

10.1 ICT security shall be part of aviation cybersecurity management.

10.2 ICT security shall define and implement logical security measures as well as contribute to cyber incident management, recovery, and operation continuity processes.

10.3 ICT security shall contribute to risk management through the identification of vulnerabilities, attack vectors, and monitoring the evolution of the aviation cybersecurity threat landscape.

11. Incident Management and Continuity of Critical Functions

11.1 Safety of operations and continuity of critical functions shall be the main drivers in incident management processes.

11.2 Testing crisis management and recovery plans shall be an integral part of incident management.

12. Cybersecurity Culture

12.1 An education, awareness, training, and exercise plan shall be an integral part of aviation cybersecurity management.

12.2 Cybersecurity culture shall be fully coordinated with existing safety and security cultures.

12.3 Cybersecurity culture shall be supported by robust internal and, to the extent possible, external information sharing practices.

— END —