REPUBLIC OF ALBANIA

AUTORITETI I AVIACIONIT CIVIL

ALBANIAN CIVIL AVIATION AUTHORITY

GUIDANCE MATERIAL FOR CYBER THREATS TO CIVIL AVIATION AND INFORMATION SECURITY

ACAA-DAS-GM4-CTCA

Issue: 01, Revision 00

Date: 21.03.2024

Approved by:

Maksim Et'hemaj

Executive Director of the Civil Aviation Authority

REPUBLIKA E SHQIPERISE - MINISTRIA E INFRASTRUKTURËS DHE ENERGJISË - AUTORITETI I AVIACIONIT CIVIL - TIRANË

Intentionally left blank

0 ADMINISTRATION

Table of Contents

0.3 Revision Table

Page #	Issue No.	Revision No.	Date	Edited by:

0.4 Distribution List

Control #	Responsible Person	Type of Document
Original	SCOS/SSS	Hard Copy
Electronic	DAS staff	Electronic copy

0. 5 Definitions

For the purpose of this manual, the following terms mean:

Availability: the property of being accessible and usable upon demand by an authorized entity.

Confidentiality: that data or information is not made available to unauthorized individuals, entities or processes.

Cyber security: is the application of technologies, processes, and controls to protect systems, networks, programs, devices and data from cyber-attacks.

Denial of Service: An attempt to make a machine or network resource unavailable to its intended users, such as to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet. Denial of service is typically accomplished by flooding the targeted machine or resource with superfluous requests to overload systems and prevent some or all legitimate requests from being fulfilled.

Integrity: the accuracy and completeness of data and information assets.

Malware: A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or of otherwise annoying or disrupting the victim, e. g.: Virus, Trojan Horse, Worm, Spyware, Ransomware.

Mitigations: measures in place to reduce the likelihood of attack (i.e. to deter, detect and disrupt it) and to reduce its consequences.

Risk: the potential for an adverse outcome, assessed as a function of the threat, consequences and vulnerabilities associated with a specific attack.

Risk assessment: the process, which collects relevant information and assigns values to identified risks for the purpose of informing priorities, developing or comparing courses of action and informing decision-making. It provides the basis for the rank ordering of risks and for establishing priorities for countermeasures.

Threat: the assessed likelihood or probability of an act of deliberate interference be, it a terrorist attack or other crime being attempted (target, type of attack, perpetrator) within certain time frame; A result of motivation, intent and means/capabilities.

Vulnerability: the features of something potentially under threat which can be exploited by an attacker e.g. at an airport or on an aircraft, or which mean the asset may be inadvertently effected by a deliberate act of interference against a non-aviation target, combined with any weakness in current security measures.

0.6 Abbreviations

In this guidance material, the following abbreviations will be used, which will mean:

ACAA	Albania Civil Aviation Authority
DAS	Directorate of Aviation Security
NCASP	National Civil Aviation Security Program
NCASTP	National Civil Aviation Security Training Program
ICAO	International Civil Aviation Organization
BYOD	Bring your own device
InfoSec	Information Security

1. OBJECTIVES AND APPLICABILITY

1.1 Purpose

Cyber security in civil aviation has become an important topic where states and operators are focusing, besides the classical security measures applied. This manual aims to provide a guidance for operators in the field of civil aviation, in order to assist them in establishing effective security measures for the implementation of National Civil Aviation Security Program, and also to address their needs and improve overall cybersecurity framework.

The objectives of security measures applied for cyber security at minimum should be to prevent unauthorized access and use of the system and to preserve the availability, integrity and confidentiality of the data.

The measures should also ensure that the systems are not used to facilitate unauthorized access by persons or the introduction of prohibited articles into security restricted areas or on to aircraft. Additionally, measures that will detect attacks on the system should also be deployed.
The most important thing is to identify and ensure that the protection of the relevant, especially critical, aviation information systems (including their hardware, software, and data) are included in the normal risk assessment processes established by appropriate authorities.

1.2 Legal basis

This guidance material has been drafted with the following legal references:

- Decision of the Council of Ministers No. 1115, dated 24.12.2021 for "Approval of the National
- Civil Aviation Security Program".
- Law No. 10/2023 for Classified Information
- Law No. 2/2017 for Cyber Security
- Decision of the Council of Ministers No. 553, dated 15.7.2020 for “Approval of the list of critical information infrastructures and the list of important information infrastructures”.

2. RISK MANAGEMENT

To enable the management of cyber risks, Civil Aviation Authority ensures together with operators, including air navigation systems providers, airports, air carriers and regulated agents, implementation of measures to identify, assess the risks to and, as appropriate, protect relevant, especially critical, aviation information systems and data.

Based on National Civil Aviation Security Program, Civil Aviation Authority requires operators to implement adequate measures for the protection of their relevant, especially critical, aviation information system. This protection can be achieved using, at a minimum, one or a combination of measures including:

- Limiting the number of persons with authorised access to the system.
- Requiring two persons for approvals within systems
- Implementing authentication systems verifying that only those authorised to access are accessing the system e.g. biometric log on to critical aviation information systems.
- Ensuring systems hardware, particularly servers, is in access-controlled areas.
- Installing software to protect the systems from unauthorised access e.g. firewalls; and
- Ensuring virus protection systems are implemented and maintained.

Civil Aviation Authority will verify that appropriate measures have been implemented by including cyber security as part of their regular compliance monitoring activities (e.g. inspections, audits).

Civil Aviation Authority will consider the type of quality control activities appropriate to relevant, especially critical, aviation information systems and for example, may choose simply to verify that security measures exist for these systems. Also, will choose to implement quality control activities that verify the robustness of the security measures in place, for example, by conducting penetration tests on these systems. Irrespective of the method adopted, all quality control activities should be undertaken in accordance with an agreed methodology that does not compromise the safety and security of the civil aviation operation being subject to the test.

For those entities responsible for aviation information systems who come under the remit of an authority other than that of the Civil Aviation Authority and for whom may not have direct responsibility, the Authority should use its offices to promote a coordinated approach to the implementation of cyber security measures for relevant especially critical aviation information systems.

3. RISK ASSESSMENT PROCESS

The same approach should be taken to cyber threats as to other threat types considering:

• Plausible scenarios: targets, relevant systems and data (especially critical ones), types of attack (e.g. denial of service, importation of false data), perpetrators e.g. insiders.
• Reasonable worst-case consequences (human, economic etc).
• Current mitigating measures (physical, procedural, personnel, IT etc).
• Remaining vulnerabilities; and
• The residual risk of such an attack happening.

This analysis should also identify and assess where such scenarios may occur as ways to facilitate other forms of attack e.g. by interfering with or disabling relevant IT-based security systems e.g. access control.

The protection of critical, aviation information systems (including their hardware, software, and data) should be included in the normal risk assessment processes established by appropriate authorities.
Authority should encourage operators to conduct a vulnerability assessment of relevant, especially critical, aviation information systems and ensure that mitigation measures are established. For example,

individual login usernames and passwords or biometric logins are preferable to access critical aviation information systems to mitigate unlawful attempts to access directly or undermine the integrity of these systems.

Similarly, activity logs can be useful in auditing and evaluating that systems are performing within normal parameters and in some cases, these logs have automatic alerting systems (e.g. by email or SMS) when there is activity outside of normal operating parameters.

4. SECURITY MEASURES

4.1 Network separation

The Civil Aviation Authority will ensure that networks used for critical aviation information systems are separated from networks to which the public have access. Where these critical aviation information systems require connectivity to other operational systems, these connections should be minimized to the extent practicable. If separation is not possible, connection and access should be monitored and always controlled. Critical aviation information systems on board an airplane should be always separated from networks to which the public have access.

The software and hardware of today's relevant, especially critical, aviation information systems cannot operate without the necessary cables and connectivity that ensure that data can be transmitted and exchanged. In that regard the network should be examined to ensure that the security objectives are not compromised by exposing such aviation information systems to uncontrolled or open access communications networks.

Networks used by such aviation information systems should be separated from networks to which the public have access. This can be achieved through physical or virtual separation. The more critical the system is though, the more desirable a physically separated network becomes.
Critical aviation information systems are virtually separated within a wider, common airport or air carrier network, thus providing security by way of being difficult for an attacker to identify the critical aviation information system information.

Operators should conduct a risk assessment which is based on their local knowledge and will assist in determining the best solution.
It is unlikely that a critical aviation information system can exist effectively without any means of communication with a network. To that end, where connectivity is required, appropriate policies and practices should be in place that firstly reduce the number of connections to the minimum required.

When the number of connections has been reduced, the next step is to ensure that the connection takes place under controlled conditions i.e. that the nature (type of information, frequency, method of data exchange etc.) of the interface between the system and the network is known. An effective management system for these network interfaces will ensure that all connections to the system are documented,

reviewed, upgraded as necessary and that adequate virus and malware protection is in place, where applicable.

A layered approach to software management should also be considered. A limited number of individuals should have administration rights on any critical aviation information system. Access to systems should be based on the principle of legitimate need. For example, some individuals may only be granted read-only rights, others with access only to parts of the system relevant to their specific tasks.

4.2 Responsibility

The Civil Aviation Authority will ensure that responsibility for securing relevant, especially critical, aviation information systems and data is allocated by operators to a properly selected, recruited and trained and resourced individual. This individual should ensure that these security measures are coordinated and consistent with existing aviation and IT security measures.

Throughout the aviation security system there is a reliance upon properly selected, recruited and trained individuals who have responsibilities for aviation security within operator organizations and the necessary resources to execute that role. In that regard, this Recommendation is an extension of that process to include cyber risks.

4.2.1 List of Skills/Competencies Related to Cyber Security Personnel

List of relevant competencies required by aviation security experts (with responsibility for cyber security at organisational/national level), national auditors with cyber security responsibility and general aviation personnel to perform their duties.

1. AVIATION SECURITY EXPERTS

List of skills and competencies on cyber security for aviation security experts (with cyber security responsibility at organisational and/or national level):

- Knowledge of previous acts of unlawful interference against civil aviation and other industry sectors, including but not limited to current and evolving cyber security threats.
- Knowledge of the national and specific local cyber security policy/regulations including up-to-date privacy and security regulation and reporting procedures for incidents.
- Knowledge of international and national aviation security legislative framework and how it relates to aviation security programmes.
- Knowledge of information security management framework and processes.
- Understanding of risk management principles applicable to the protection of critical information and communications technology systems and data from cyber threats.

- Ability to organise and conduct technical vulnerability assessments.
- Knowledge of the prevention, impact and management of cyber security incident.
- Knowledge of security and protection measures applied to critical information and communications technology systems and data.
- Knowledge of overlap and hand-over points between aviation security and aviation safety as it pertains to information security.
- Knowledge of applicable contemporary IT/IoT standards, best practices, procedures, protocols, and methods (where relevant to cyber security matters).
- Knowledge of physical access points to IT infrastructure resources.
- Knowledge of the systems and networks used for critical information systems.
- Knowledge of potential threats to and risks imposed by cloud computation/data storage and relevant security measures.
- Knowledge of the procedure for modification and upgrade of critical aviation information systems, procurement and maintenance of hardware and software components (where relevant to cyber security matters).
- Ability to manage and interpret journaling events.
- Knowledge of different cyber security solutions.
- Knowledge of the BYOD (Bring your own device) policy to understand the risks and be able to protect sensitive information on employee-owned devices used for work matters.

2. NATIONAL AUDITORS

List of skills and competencies on cyber security for national auditors (with cyber security responsibility):

- Knowledge of the scenario of previous acts of unlawful interference against civil aviation, including but not limited to current and evolving cyber threats which could affect the security of civil aviation.
- Ability to identify possible cyber security vulnerabilities, most common attack types and threat vectors.
- Knowledge of international and national aviation security legislative framework and relate to aviation security programmes and cyber security procedures.
- Understanding of risk management principles applicable to the protection of critical information and communications technology systems and data from cyber threats.
- Ability to perform quality control activities, inspections and audits to address cyber security compliance matters.
- Knowledge of the cooperation/coordination process for cyber security with aviation safety experts.
- Analytical and diagnostic skills (for the purpose of investigating cyber security issues);

- Ability to identify critical information and communications technology systems and data used within the aviation system.
- Knowledge of the cyber security policies and regulations of the entities being audited.
- knowledge of the different groups of malwares and their impact to information security.
- Ability to understand penetration test reports and coordinate their implementation in a safe and secure manner.
- Knowledge of security and protection measures applied to critical information and communications technology systems, networks/data and ability to identify and evaluate their effectiveness.
- Ability to deal with cyber security incidents.
- Knowledge of the BYOD policy to understand the risks and be able to protect sensitive information on employee-owned devices used for work matters.
- Knowledge of different authentication methods and protocols.
- Knowledge of cloud security services.

3. GENERAL AVIATION PERSONNEL

List of skills and competencies on cyber security for general aviation personnel:

- Knowledge of previous acts of unlawful interference against civil aviation, including but not limited to current and evolving cyber security threats.
- Awareness of social engineering tactics, countermeasures and the possible signs of cyber-attack and methods of reacting in a timely manner.
- Awareness of the possible risks involved by using external storage media.
- Knowledge of timing and procedures to report suspicious behaviour from either humans or computers.
- Knowledge of procedures that explain how to change and protect access control credentials.
- Knowledge of the BYOD (Bring your own device) policy to understand relevant risks and the importance of protecting sensitive information on employee-owned devices used for work matters.
- Awareness of the possible risks involved by public Wi-Fi access points (airport, hotels, restaurants, etc.).
- Knowledge of the policy and procedures for departing employees with access to remote applications and credentials that provide access to data and systems.

It is advised that this knowledge be transmitted through Cyber Awareness Training for this category of staff, in accordance with the requirements of NCASP.

For those operators who already employ persons with information security expertise, they could opt to include critical aviation information systems within the remit of their existing regime. If this is the case, training in aviation security for the individual should be done. Furthermore, this individual should be

considered for the purposes of the National Civil Aviation Security Training programme and National Civil Aviation Security Quality Control Programme as someone who has a security role and should be included accordingly. Finally, persons with administrator rights on critical aviation information systems should undergo regular background checks, as appropriate.

4.3 Security by design

Operators should ensure that appropriate security measures are considered in the design, implementation, operation, and disposal of new, especially critical aviation information systems. Modifications to existing aviation information systems should take security considerations into account to the extent practicable.

Like the design and construction of airports, air carrier facilities, cargo and logistics centers for airport supplies and aircraft themselves is best served when security is taken into consideration at the earliest stage of the process. This offsets the costs and negative operational impact of having to retrofit these facilities or equipment.
The same applies to the specification, procurement and or modification of new critical aviation information systems. Suppliers should be asked to provide details as to how the information and operation of the system is secured. The arrangements for ongoing support and maintenance should be considered. Decisions regarding remote access to systems are also needed.

Furthermore, it is important to locate the hardware for critical aviation information systems in access-controlled rooms. Such a measure will help prevent unauthorized access to the equipment and minimize the opportunity for individuals to interfere with the integrity of the system. Similarly, it is also important to plan routes for cables to ensure that critical aviation information systems cannot be easily infiltrated is also important.

4.4 Supply chain security

Operators should ensure that reasonable and appropriate supply chain security measures for data, hardware and software are applied to relevant, especially critical, aviation information systems. The Civil Aviation Authority should be informed of details of security measures from potential suppliers when procuring such systems.

Relevant, especially critical, aviation information systems need to be introduced or upgraded from time to time either due to changes in operating requirements (modifications) or due to changes in versions (software upgrades). Additionally, hardware will need to be added or replaced. In each of these circumstances there is a possibility to introduce software or hardware that can attack, infiltrate, or compromise the integrity of the critical aviation information system and the data it carries.

Measures should be in place to ensure firstly, that reputable and legitimate suppliers are used to procure

hardware and software for critical aviation information systems. Secondly, suppliers should be asked to provide details of the security measures they have in place not only at the installation stage but over the lifetime of the system.

4.5 Remote access control

Operators should ensure that remote access to relevant, especially critical aviation information systems is only permitted under pre-arranged and secure conditions. Civil Aviation Authority and operators should ensure that suppliers do not have unauthorized access to these systems after they have been procured.

Operators are also obliged to have support and maintenance arrangements for their relevant especially critical aviation information systems.
However, remote access requires that the supplier has a means of accessing a critical aviation information system. Operators should ensure that this access route is known to them, that the means and conditions of entry are agreed. The supplier may be required to call a designated official from the operator to inform them that they are accessing the critical aviation information system. Alternatively, an automatic email can be generated to notify someone from the operator each time access is sought. Remote access, for planned maintenance, may be at pre-arranged times.

These types of measures should be complemented with an appropriate audit and exception reporting system. Audit logs on the critical aviation information system itself should be reviewed regularly to identify and follow-up on exceptional access.

Another important and helpful tool is to request the supplier to limit the number of persons authorized to provide support and maintenance to a critical aviation information system. Suppliers will want to maintain flexibility in allocating their staff to support and maintenance activities and may resist any attempts to identify individuals. Nevertheless, from a security perspective, having a limited number of identified persons accessing the critical aviation information system is desirable. Background checks also be conducted on these individuals.

An additional consideration when purchasing relevant, especially critical, aviation information systems is that suppliers frequently use “back doors”; these are unofficial pieces of code within the software that can be used by those who know about them to enter and use a system undetected. This vulnerability is almost impossible to mitigate but certain measures will at least aid detection. Regular system audits should identify any unusual activity on the system. Having the software behind a firewall not provided by the same supplier would also assist in this regard. When procuring the system, operators can request a certificate from the supplier stating that no such access exists, effectively guaranteeing the integrity of the system.

4.6 Cyber-attack incident records

Civil Aviation Authority and operators should record and evaluate incidents of cyber-attacks and ensure their risk assessments and responses are adjusted as appropriate in the light of such incidents.

To ensure that civil aviation can be appropriately protected against cyber risks, understanding the threat and the likely method of attack is important. One source of information that is helpful in this process is the review of incident reports. There are several steps for this to be effective:

- The reporting of incidents to the appropriate authority will improve its understanding the risks of cyber-attack.
- Civil Aviation Authority should encourage operators to implement a reporting regime in their organizations.
- The nature of each incident should be analysed, and existing risk assessments and response measures adjusted accordingly. Industry specific trends identified should be communicated to other entities within that sector. Some, incidents may have implications for other operators and/or for entities in, other aviation sectors and an alerting system should be established to facilitate communication. In Albania we have National Authority on Electronic Certification and Cyber Security (AKCESK) for incident reporting or information sharing about incidents.

The National Civil Aviation Security Committee and AKCESK should receive collated and anonymised reports of cyber-attacks to enable them take appropriate action or develop policy to address cyber threat trends.

5 INFORMATION SECURITY

5.1 Introduction

Aviation security relies on two key principles about information i.e. “need to know” and the security clearance of individuals. In other words, only people that need to have information to be able to perform a function or task shall have access to it and if access is granted that it is at the level for which the person has been given clearance.

Information security, sometimes referred to as InfoSec, is defined as processes methodologies standards mechanisms and tools which are designed and implemented for the purposes of protecting information from unauthorized access use modification or destruction in order to ensure confidentiality integrity and availability of information.

Information security is a general term that can apply to any format of information whether it is electronic or physical, whether information in transit, in rest, or in motion, whether information is created, stored, destroyed, processed, or transmitted.
The aviation security regulatory environment at Standards level comprises information described as

RESTRICTED, CONFIDENTIAL, SECRET and TOP SECRET, as provided in LAW No. 10/2023 FOR CLASSIFIED INFORMATION. These levels are collectively termed EU classified information. These are consistent with the national security classification system. Hence the Authority requires certain staff to be cleared to ensure that necessary information is available to them for the conduct of their duties.

5.2 Organization

To facilitate the implementation of this procedure, it is necessary for operators to have an organizational chart showing the categories of persons who need to know about aviation security matters. Only those persons with access rights at the specified levels are allowed to access the documentation/information.

5.3 Classified Information Storage

Once data is created, it need to be stored to make accessible to other applications and processes. Information is stored onsite using storage devices such as hard drive, flash drives, or network storage or offsite such as another physical location or using the cloud. Once information is created and stored, it must be protected from unauthorized access, whether such information is located onsite or offsite, using different security measures such as encryption, and passwords. Other kinds of information in physical formats must be protected using physical security measures such as magnetic stripe ID cards and locks.

Classified information will be stored in accordance with Law No. 10/2023 for Classified Information.

5.4 Dissemination of Classified Information

In line with the principles set out in the Albanian Law related to classification of information, it is a matter for the originator of the information to decide if it needs to be classified and if so, to determine the appropriate level.

The following table sets out the procedures for the further dissemination of security classified information. If there is a doubt over the status of a document the matter should be referred to an Aviation Security Inspector, who will determine the classification level as appropriate. It is important that the security status of all documents is determined by the Authority prior to dissemination.

Information Security Level	Means of Dissemination by Authority	Examples of security information
Top Secret	None	State secrets e.g. military
Secret	Hard copy available to read, isolated room, no electronic	

	recording devices, computers, or phones	
Confidential	Hard copy disseminated by courier with recorded delivery to the individual recipient or handed directly to the intended recipient with signed receipt. OR Secure electronic portal that is password protected.	Law No. 10/2023 NCASP
Restricted	Password protected, sent by email with a separate email containing the password	AvSec reports
Public	Sent by email without a password or made available on the Authority's website	Application forms

5.5 Breach of Procedure

A breach of procedure will result in an immediate investigation, initially with the intention of limiting the further spread of information to unauthorised persons. The investigation will then establish how the breach occurred. If necessary remedial action will be taken to prevent future similar events from occurring.

5.6 Retention of Records

All security clearance records will be held indefinitely. Documentation classified as confidential or higher will be destroyed by personnel authorised to access such material and in a manner that prevents it being retrieved.