GCAA National Civil Aviation Cybersecurity Guidelines

Published by authority of the Director General,
General Civil Aviation Authority

Version 1 - September 2024

Table of Contents

FOREWORD 3
1. Introduction 4
2. Scope 4
3. Objectives 4
4. Governance and Organisation 4
8. Protection of Critical Information and Communication Technology Systems and Data 13
9. Requirements 14
10. Risk Response 16
11. Supply Chain Security 16
12. Physical Security 18
13. Information, Communication, Technology (ICT) Security 19
14. Incident Management and Continuity of Critical Functions 19
15. Cybersecurity Culture in Civil Aviation 21

GCAA NATIONAL CIVIL AVIATION CYBER SECURITY GUIDELINES

FOREWORD

In an era defined by rapid technological advancements, the aviation industry has embraced digital transformation, ushering in unprecedented levels of connectivity and efficiency. As aviation systems become increasingly reliant on digital infrastructure, the importance of robust civil aviation cybersecurity measures cannot be overstated. The General Civil Aviation Authority (GCAA) recognizes the critical role that civil aviation cybersecurity plays in safeguarding the integrity, confidentiality, and availability of information and systems within the aviation sector.

The GCAA National Civil Aviation Cybersecurity Guidelines represent a significant milestone in our commitment to ensuring the resilience and security of civil aviation operations. These guidelines provide a comprehensive framework that addresses the unique challenges and complexities of the civil aviation cybersecurity landscape.

Civil Aviation cybersecurity is a dynamic and evolving field, necessitating a proactive approach to identify, assess, and mitigate potential threats. The GCAA Guidelines serve as a foundational document, offering a structured set of principles, best practices, and recommendations that empower aviation stakeholders to enhance their civil aviation cybersecurity posture.

This document is designed to be a living document, capable of adapting to the ever-changing civil aviation cybersecurity landscape. Regular updates and revisions will be undertaken to ensure that the guidelines remain relevant and effective in addressing emerging threats. The GCAA acknowledges the collaborative efforts of industry experts, regulatory authorities, and cybersecurity professionals who have contributed to the development of these guidelines.

The successful implementation of the GCAA National Civil Aviation Cybersecurity Guidelines requires a collective commitment from all stakeholders, including government agencies, Airport and Aircraft Operators, maintenance organizations, and technology providers. By adhering to these guidelines, GCAA aims to establish a resilient and secure aviation ecosystem that instills confidence in passengers, fosters innovation, and ensures the sustained growth of the aviation industry.

GCAA expresses gratitude to all those who have contributed to the creation of these guidelines, and urge the aviation community to embrace and integrate these principles into their day-to-day operations. Together, we can build a cyber-secure aviation environment that not only meets the challenges of today but anticipates the complexities of tomorrow.

Director General
General Civil Aviation Authority

1. Introduction

1.1 The GCAA National Civil Aviation Cybersecurity Guidelines Version 1, September 2024 is in line with the GCAA National Civil Aviation Cybersecurity Strategy Version 1, June 2023 and the UAE Civil Aviation Cybersecurity Policy Issue 1, October 2023.

1.2 The term 'RESERVED' is used throughout this document to facilitate future inclusions, as applicable.

1.3 Comments on the content may be provided through Cyber@gcaa.gov.ae

2. Scope

2.1 This document addresses the protection and resilience of UAE's civil aviation's critical infrastructure against cyber threats, and the multilateral collaboration requirement within civil aviation as well as with external authorities such as military, cybersecurity entities, and other entities responsible for national security.

2.2 Primarily, the civil aviation ecosystem includes but not limited to:

a) Air Navigation Systems;

b) Aircraft Systems (such as communication systems, flight entertainment systems, and internal controls);

c) Airport Systems (such as passenger information systems, Departure Control Systems (DCS), airport information systems, and baggage screening and handling systems);

d) Emergency response systems (such as Firefighting systems, building management systems etc);

3. Objectives

3.1 The objective of these guidelines is to enhance the cyber security and resilience of civil aviation against cyber threats and risks. Enabling civil aviation cybersecurity stakeholders to develop, sustain, and implement a strong culture of cybersecurity within their organizations, by developing a systemic approach that not only enables civil aviation to be protected against cyber threats, but also to respond to and recover from cyber incidents in a timely fashion so as to withstand new threats without significant disruptions.

4. Governance and Organisation

4.1 In accordance with the United Arab Emirates (UAE) Ministerial Letter reference GCAA/C/54-23 to the International Civil Aviation Organization (ICAO) naming the General Civil Aviation Authority (GCAA) as the Appropriate Authority for Aviation Cybersecurity (AA/Cyber) with an overall mandate for civil aviation cybersecurity and cyber resilience.

4.2 Cybersecurity in civil aviation encompasses a broad range of areas within the civil aviation landscape, including safety, security, air navigation, and risk management. It also carefully considers the economic, operational, and additional impacts that may arise.

5. Cybersecurity Roles and Responsibilities in Civil Aviation

5.1 General Civil Aviation Authority

5.1.1 The roles and responsibilities of the GCAA in the realm of civil aviation cybersecurity are comprehensive and critical to ensuring the safety and integrity of the aviation sector. As the designated Appropriate Authority- Cyber (AA/Cyber), the key areas of focus for GCAA are:

a) Policy and Regulation Development

i) Formulate Policies: Develop national civil aviation cybersecurity policies and regulations specific to civil aviation, ensuring alignment with international standards and best practices.

ii) Establish Frameworks: Create frameworks that address the civil aviation cybersecurity needs of various aviation stakeholders, including airlines, airports, and air navigation service providers.

iii) Roles and Responsibilities: Coordinate the definition of roles and responsibilities for civil aviation entities under the GCAA through the State Safety Programme and National Civil Aviation Security Programs.

iv) Allocate Responsibilities: Allocate responsibilities to relevant entities to identify critical information and communication technology systems and data used for civil aviation, based on risk assessments, to mitigate vulnerabilities and implement protective measures against acts of unlawful interference and to respond appropriately to incidents, in accordance with national requirements.

v) ICAO SARPs: Implement and enforce compliance requirements for civil aviation cybersecurity standards and regulations in line with ICAO SARPs and other international guidelines.

b) Oversight and Coordination

i) Supervise Implementation: Oversee the implementation of civil aviation cybersecurity measures and protocols across civil aviation entities to ensure consistency and effectiveness.

ii) Coordinate with Stakeholders: Collaborate with domestic and international stakeholders, including other government agencies, industry groups, and international organizations, to enhance civil aviation cybersecurity efforts.

iii) Monitor and Evaluate: Continuously monitor the civil aviation cybersecurity posture of aviation entities and evaluate their adherence to established standards and practices.

c) Risk Management

i) Risk Assessments: Perform regular risk assessments to identify vulnerabilities and potential threats within the civil aviation sector's cybersecurity landscape.

ii) Risk Mitigation Strategies: Create and promote strategies to address identified risks and minimize their impact on aviation operations and safety.

iii) Reports and Recommendations: Submit reports and recommendations to the Board of Directors and the Audit and Risk Committee on the civil aviation sector's cybersecurity risks and business continuity plans related to civil aviation cybersecurity threats.

d) Incident Response and Management

i) Establish Incident Response Plans: Develop and maintain comprehensive incident response plans to address civil aviation cybersecurity breaches or threats effectively.

ii) Coordinate Response Efforts: Lead and coordinate the response to civil aviation cybersecurity incidents, including communication with affected parties and public disclosure when appropriate.

iii) Post-Incident Review: Conduct post-incident analyses to assess the impact, identify lessons learned, and improve future response and prevention measures.

iv) Reporting: Ensure that entities with aviation safety and security responsibilities report all actual or suspected security occurrences, including security incidents, breaches, cyber incidents, or acts of unlawful interference, to the GCAA for follow-up and corrective action as follows:

(aa) Immediately via the AVSEC Hotline at +971 50 6424 911 and email: avsec-di@gcaa.gov.ae;

(bb) Within 48 hours via the Reporting of Security Breaches (ROSB) system; and

(cc) Through the Aviation Security – Voluntary Reporting System.

e) Training and Awareness

i) Provide Training Programs: Develop and deliver civil aviation cybersecurity training programs for aviation personnel, including air traffic controllers, airport staff, and aircraft operator employees.

ii) Promote Awareness: Raise awareness about civil aviation cybersecurity issues and best practices among civil aviation stakeholders to foster a culture of security.

f) Infrastructure and Technology

i) Oversee Security Infrastructure: Ensure that the civil aviation cybersecurity

architecture, infrastructure, including surveillance and communication systems, is robust and up-to-date.

ii) Implement Technological Solutions: Promote the adoption of advanced cybersecurity technologies and solutions to protect critical civil aviation systems and data. Ensure the protection of all safety and security data capture and processing systems from cyber-attacks and other vulnerabilities.

g) Compliance and Audits

i) Ensure Compliance: Ensure that entities with aviation safety and security responsibilities comply with civil aviation cybersecurity policies and procedures to protect information technology and air navigation systems, thereby safeguarding their integrity, availability, and confidentiality, and ensuring the safety and efficiency of air traffic management.

ii) Conduct Audits and Inspections: Perform regular audits and inspections of aviation entities to ensure compliance with civil aviation cybersecurity regulations and standards.

iii) Enforce Penalties and Corrective Actions: Apply penalties or corrective actions as necessary for non-compliance or failure to adhere to civil aviation cybersecurity requirements.

iv) Security Assessments: Conduct periodic security assessments and vulnerability scans to evaluate the security controls of IT systems, networks, and applications, and implement appropriate controls to protect against civil aviation cybersecurity threats

h) Research and Development

i) Stay Informed on Trends: Keep abreast of emerging civil aviation cybersecurity threats, technologies, and trends to inform and update civil aviation cybersecurity strategies and policies.

ii) Promote Innovation: Encourage research and development in civil aviation cybersecurity to enhance protective measures and adapt to evolving threats.

j) Collaboration and Information Sharing

i) Coordination with the UAE Cybersecurity Council: Determine, in coordination with the UAE Cybersecurity Council, the roles and responsibilities of each authority and entity within the UAE regarding civil aviation cybersecurity and cyber resilience.

ii) Facilitate Information Sharing: Encourage and facilitate the sharing of civil aviation cybersecurity information and threat intelligence among aviation stakeholders and with other relevant sectors.

iii) Coordinate with non-aviation stakeholders: Coordinate cross-cutting civil aviation cybersecurity issues with relevant non-aviation stakeholders,

including information sharing and incident investigation.

iv) Participate in International Forums: Engage in international forums and working groups to contribute to and benefit from global civil aviation cybersecurity initiatives and standards.

k) Regulatory and Legal Framework

i) Assist to Develop Legal Frameworks: Recommend and update legal frameworks that address cybersecurity issues within the civil aviation sector, including, but not limited to, data protection and privacy laws.

ii) Ensure Enforcement: Ensure that legal and regulatory frameworks are effectively enforced to protect aviation systems and data from cyber threats.

5.1.2 By fulfilling these roles and responsibilities, the GCAA helps ensure the cybersecurity of civil aviation operations, safeguarding the sector against evolving cyber threats and maintaining public confidence in air travel.

5.2 Civil Aviation Cybersecurity Stakeholders

5.2.1 Civil aviation cybersecurity stakeholders encompass a wide range of entities both within and outside the country. These stakeholders are involved in various aspects of securing aviation systems and data from cyber threats. By engaging with these stakeholders, aviation organizations can enhance their cybersecurity posture and contribute to a more secure global civil aviation system.

5.2.2 Civil Aviation Cybersecurity Stakeholders includes but not limited to the following:

a) Airport Operators;

b) Aircraft Operators;

c) Airport and Airline IT Departments;

d) Regulated Agents;

e) Air Traffic Service Providers (ATSPs);

f) Air Navigation Service Providers (ANSPs);

g) IT and Communications service providers;

h) Cybersecurity Consultants and Contractors;

i) Ground handling agents and service providers at UAE airports;

j) Maintenance, repair and overhaul service providers;

k) Command and control service providers for Remotely-Piloted Aircraft

Systems (RPAS), electric Vertical Take-off and Landing aircrafts (eVTOLs), Drones (manned & unmanned) etc.;

l) Advance Passenger Information (API);

m) Training and Certification Bodies;

n) Multilateral and Bilateral Partnerships;

o) Collaborative and Information Sharing Platforms like Cybersecurity Information Sharing and Analysis Centers (ISACs), Aviation Security and Cybersecurity Conferences, Industry Working Groups etc.; and

p) Other relevant national and international entities.

5.2.3 Civil aviation cybersecurity stakeholders in the UAE ***shall***:

a) Identify critical information and communication technology systems and data used for civil aviation purposes;

b) Establish, implement, operate, monitor, review, and improve cyber security activities, policies, standards, and procedures;

c) Conduct continuous cyber risk assessments to mitigate new vulnerabilities and implement appropriate measures;

d) Protect critical information and technology systems from acts of unlawful interference;

e) Conduct periodic security assessments and implement adequate security controls to ensure protection against cyber security threats;

f) Respond appropriately to an incident, in accordance with national requirements;

g) Support & ensure alignment to national studies and research related to cyber security advancements; and

h) Ensure compliance with government initiatives and relevant national and international standards and regulations concerning information security.

6. Identification of Critical Information and Communication Technology Systems and Data

6.1 Civil Aviation Cybersecurity Stakeholders should identify critical data and information systems software and hardware used in their operations, which may include, but are not limited to:

a) Systems and data identified as critical from an aviation safety perspective, such as:

i) air navigation services systems;

ii) departure control systems;

iii) communication, navigation and other safety-critical systems of an aircraft; and

iv) aircraft command, control and dispatch systems;

b) Systems and data identified as critical from an aviation security perspective, such as:

i) regulated agent and/or known consignor databases;

ii) access control and alarm monitoring systems;

iii) closed-circuit television surveillance systems;

iv) passenger and baggage reconciliation systems; and

v) screening systems and/or explosive detection systems, whether networked or operating in a stand-alone configuration;

c) Systems and data identified as critical from an aviation facilitation perspective, such as:

i) aircraft operator reservation and passenger check-in systems;

ii) flight information display systems;

iii) baggage handling and monitoring systems; and

iv) border crossing and customs systems.

7. Threats and Risk Management

7.1 Threats

7.1.1 Cyberattacks on Civil Aviation Systems:

7.1.1.1 Air Navigation Services Systems Attacks: Targeting air navigation infrastructure to disrupt communications between controllers and aircraft or manipulate ATC systems data, causing potential flight delays, route deviations, or air traffic management confusion.

7.1.1.2 Aircraft Systems Hacking: Unauthorized access attempts on aircraft systems like the Flight Management System (FMS) or avionics, potentially interfering with flight controls and onboard systems.

7.1.1.3 Airport Systems Compromise: Cyberattacks on various airport systems including the AODB, baggage handling, security, and passenger information systems, leading to operational disruptions and security breaches.

7.1.1.4 Aviation Communication Network Attacks: Interception or manipulation of critical aviation communications, affecting safety-critical instructions and causing miscommunication.

7.1.1.5 Cyber-Physical Attacks: Targeting the intersection of cyber and physical systems within aviation, like surveillance cameras and access control, to gain unauthorized access or disrupt security measures.

7.1.1.6 Malware and Ransomware: Infecting aviation systems with malicious software to disrupt operations, compromise data, or demand ransom.

7.1.1.7 Social Engineering and Phishing: Trickery to deceive aviation personnel into divulging sensitive information or granting unauthorized access.

7.1.1.8 Insider Threats: Authorized individuals misusing their access for malicious purposes, such as data theft or system tampering.

7.1.1.9 Advanced Persistent Threats (APTs): Well-resourced, targeted cyberattacks aiming for persistent access to systems for espionage or disruption.

7.1.1.10 Distributed Denial of Service (DDoS) Attacks: Overwhelming systems or networks with traffic to cause service disruptions.

7.1.1.11 Zero-Day Exploits: Exploitation of unknown vulnerabilities in software or systems, leaving them open to attacks until patched.

7.1.1.12 Supply Chain Attacks: Targeting vulnerabilities in the supply chain to introduce compromised components into aviation infrastructure.

7.1.1.13 Data Manipulation: Unauthorized alteration of aviation data, such as flight plans or maintenance records, compromising safety and decision-making.

7.1.1.14 Cyber Espionage: State-sponsored or corporate espionage targeting sensitive aviation information or technology.

7.1.1.15 Nation-State Attacks: Sophisticated attacks by nation-states on critical aviation infrastructure for geopolitical objectives.

7.2 Risks

7.2.1 Operational and Security Risks:

7.2.1.1 Unauthorized Access and Data Breaches: Risk of unauthorized access leading to system disruptions, data breaches, or compromised flight operations.

7.2.1.2 Insider Threats and Sabotage: Risk from internal personnel misusing privileges, causing harm, or introducing vulnerabilities.

7.2.1.3 System Disruptions: Cyber-attacks or technical failures disrupting critical aviation systems, affecting operations and safety.

7.2.1.4 Identity Theft: Stealing personal information of aviation personnel to gain unauthorized system access.

7.2.1.5 IoT and Cloud Vulnerabilities: Exploitation of vulnerabilities in IoT devices and cloud environments, risking critical system access or data breaches.

7.2.1.6 Advanced Malware and Infrastructure Attacks: Sophisticated malware evading detection and targeting critical infrastructure, posing significant operational and safety threats.

7.2.1.7 Lack of Security Awareness and Regulatory Compliance: Risks from insufficient civil aviation cybersecurity awareness among personnel and non-compliance with industry regulations, potentially leading to security breaches and legal consequences.

7.2.1.8 Geopolitical Threats: State-sponsored cyber-attacks for political or strategic disruption, compromising national security.

7.3 Management

7.3.1 Civil Aviation cybersecurity risk management is a critical undertaking that requires a comprehensive and proactive approach to protect aviation systems, data, and operations from cyber threats. It involves identifying potential risks, assessing their likelihood and impact, and implementing strategies to mitigate or minimize those risks.

7.3.2 Effective risk management in civil aviation cybersecurity includes conducting regular risk assessments, staying informed about emerging threats and vulnerabilities, implementing robust security controls, and establishing incident response plans. It also involves promoting a strong security culture, providing continuous employee training and awareness programs, and collaborating with industry stakeholders to share information and best practices.

7.3.3 By prioritizing risk management in civil aviation cybersecurity, organizations can enhance their resilience, safeguard critical assets, and ensure the safe and secure functioning of aviation systems in an increasingly interconnected and digital environment.

7.3.4 Organizations can establish a robust civil aviation cybersecurity risk management framework that enhances their resilience and safeguards critical aviation assets, systems, and operations from cyber threats by following these steps:

a) Identify and Assess Risks: Conduct a comprehensive assessment of potential civil aviation cybersecurity risks specific to the aviation industry. This includes considering threats such as unauthorized access, data breaches, malware attacks, insider threats, and supply chain vulnerabilities. Evaluate the likelihood and potential impact of each risk.

b) Prioritize Risks: Prioritize identified risks based on their potential impact on aviation systems, data, and operations. Focus on risks with high likelihood or severe consequences and allocate resources accordingly.

c) Implement Security Controls: Develop and implement robust security controls and measures to mitigate identified risks. This includes implementing access controls, encryption, intrusion detection systems, firewalls, and regularly updating and patching software and systems.

d) Incident Response Planning: Develop a comprehensive incident response plan that outlines the procedures to be followed in the event of a civil aviation cybersecurity incident. This includes roles and responsibilities, communication protocols, containment measures, evidence collection, and recovery processes.

e) Training and Awareness: Provide regular training and awareness programs to employees, contractors, and stakeholders to enhance their understanding of civil aviation cybersecurity risks and best practices. Emphasize the importance of strong

passwords, recognizing and reporting suspicious activities, and adhering to security policies and procedures.

f) Continuous Monitoring: Implement a robust monitoring system to detect and respond to civil aviation cybersecurity incidents in real-time. This includes monitoring network traffic, system logs, and user activities to identify any unusual or suspicious behaviour.

g) Regular Testing and Auditing: Conduct regular penetration testing, vulnerability assessments, and security audits to identify weaknesses in systems and processes. Address identified vulnerabilities promptly to minimize the risk of exploitation.

h) Collaboration and Information Sharing: Engage in industry collaboration and information sharing initiatives to stay updated on emerging threats, vulnerabilities, and best practices. Participate in civil aviation cybersecurity forums, conferences, and organizations to exchange knowledge and experiences with peers.

i) Regulatory Compliance: Stay informed about relevant civil aviation cybersecurity regulations, standards, and Policy. Ensure compliance with applicable requirements and maintain documentation to demonstrate adherence to cybersecurity best practices.

j) Continual Improvement: Regularly review and evaluate the effectiveness of the civil aviation cybersecurity risk management framework. Identify areas for improvement, incorporate lessons learned from civil aviation cybersecurity incidents, and adapt security measures to evolving threats and technologies.

8. Protection of Critical Information and Communication Technology Systems and Data

8.1 The protection of civil aviation against cyber-attacks is addressed through the implementation of ICAO cybersecurity Standards and Recommended Practices (SARPs), procedures, and guidance material. It includes the implementation of robust risk management practices, the identification of critical infrastructure, and the implementation of a holistic multilayered approach to civil aviation cybersecurity. This approach should ensure that a successful attack on one layer does not compromise other layers of the system and/or lead to loss of safety, security or continuity of critical functions. The system should also adopt a continuous improvement approach to ensure that necessary enhancements to planned technical or procedural evolutions are coordinated, implemented, and kept up to date.

8.2 Civil Aviation cybersecurity stakeholders should include appropriate provisions for the protection of critical information and communication technology systems (including their hardware and software) and data, against cyber-attacks and interference, in their respective cybersecurity programmes/manuals.

8.3 Cybersecurity programs in civil aviation should be designed to safeguard the critical systems and data that are essential to the safety and security of aviation operations. To achieve comprehensive protection and resilience against cyber threats, these programs should, at a minimum, include the following objectives:

a) Protect Systems and Data: Implement robust security measures to guard against

unauthorized access, modification, and use of aviation systems and data.

b) Detect and Respond to Security Incidents: Develop capabilities for the timely detection of civil aviation cybersecurity incidents and formulate a robust response plan to mitigate their impact.

c) Continuous Risk Assessment and Management: Conduct regular assessments and management of civil aviation cybersecurity risks to adapt to evolving threats and vulnerabilities.

8.4 The following objectives should also be added to the program:

a) Enhance Physical Security: Strengthening physical security to protect critical infrastructure against unauthorized access and tampering complements civil aviation cybersecurity efforts, addressing physical avenues for cyber threats.

b) Enhance Resilience: Build redundancy and failover capabilities into systems and processes to maintain operations in the face of cyber attacks.

c) Foster Civil Aviation Cybersecurity Awareness: Cultivate a culture of civil aviation cybersecurity awareness and training among all personnel to minimize risks of breaches caused by human error.

d) Compliance with Standards and Regulations: Align with national and international civil aviation cybersecurity standards, guidelines, and regulations to ensure effective and consistent security practices.

e) Collaborative Information Sharing: Facilitate the sharing of threat and incident information within the aviation ecosystem and with relevant authorities to improve collective defense efforts.

f) Ensure Data Privacy: Adopt measures to protect the privacy and security of individuals' data in compliance with applicable laws and regulations.

g) Regular Updates and Patching: Maintain systems and software with regular updates and patches to protect against known vulnerabilities.

h) Incident Recovery Planning: Develop and regularly test incident recovery plans to ensure the organization's preparedness to restore normal operations swiftly after a civil aviation cybersecurity incident.

8.5 By integrating these objectives, civil aviation cybersecurity programs can provide a robust framework for protecting civil aviation operations from cyber threats, ensuring the safety, security, and resilience of the aviation infrastructure.

9. Requirements

9.1 Civil Aviation cybersecurity stakeholders should apply security considerations throughout the life cycle of aviation information and communication technology systems, from design and development through operation and maintenance, continuing through the safe and

secure disposal of hardware and software. Modifications, revisions, updates and upgrades to existing systems should also take into account security. Data contained within these systems should similarly follow data governance policies which prescribe the level of necessary security based on data classification, as well as the appropriate retention periods and disposal methods.

9.2 The physical and logical protection of such systems and data should begin at the design stage to ensure that they continually meet the goals of confidentiality, integrity and availability, and are as robust as possible against cyber-attacks. This may be achieved using a multi-layered approach, which includes, but is not limited to:

a) Administrative controls, such as:

   i) security standards, policy and procedures;

   ii) access management;

   iii) background investigations, selection criteria, and training of staff, particularly persons with
   administrator rights or those with the ability to access or modify sensitive and/or critical data;

   iv) continuous threat and risk assessment to determine the vulnerability of a system and likelihood of attack;

   v) the development and enforcement of acceptable use policies governing utilization of hardware, software, applications, and data by organizational and contractor personnel; and

   vi) segregation of duties, job rotation, separation of duties;

b) Quality control, including audits, inspections and tests:

   i) hardware and software supply chain security;

   ii) disaster, emergency and contingency plans;

   iii) security reviews and audits;

   iv) interdependencies with critical services supply chain; and

   v) systems configuration control and management;

c) Logical or technical controls, such as:

   i) access control policies based on least privilege;

   ii) firewalls and other security-related network components;

   iii) data protection and encryption;

iv) data destruction according to policy;

v) malware and intrusion detection systems;

vi) anomaly detection systems;

vii) system end-point protection;

viii) network integrity;

ix) strong password policies;

x) log management policies and programmes;

xi) continuous patch management; and

xii) mobile device management; and

d) physical controls, such as:

i) ensuring data centers, communication facilities, and other spaces where hardware may be
located, are appropriately secured with limited access;

ii) physical access control systems using multi-factor authentication, biometric log-on methods;

iii) limiting the number of persons with authorized access and administrative privileges; and

iv) contingency measures including the use of remote backup systems, in the event of loss of the primary system.

10. Risk Response

10.1 Risk response includes the development of a comprehensive approach to reducing or eliminating the vulnerabilities identified, as well as the techniques of risk avoidance, mitigation, transfer and acceptance.

10.2 A management-approved risk response must be developed for each identified vulnerability in accordance with national requirements.

10.3 Continual review of risk mitigation efforts is an essential element in a civil aviation cybersecurity risk management programme.

11. Supply Chain Security

11.1 Civil Aviation cybersecurity stakeholders should:

a) Conduct a thorough risk assessment of suppliers and vendors involved in the aviation supply chain. Evaluate their civil aviation cybersecurity practices, policies, and

controls to ensure they align with industry standards and best practices. Consider factors such as their access to critical systems, data handling processes, and incident response capabilities.

b) Implement a robust supplier selection process that includes civil aviation cybersecurity considerations. Prioritize suppliers who demonstrate a strong commitment to civil aviation cybersecurity and have appropriate security certifications or accreditations. Include specific contractual obligations related to civil aviation cybersecurity, data protection, incident reporting, and compliance with relevant regulations.

c) Clearly define the civil aviation cybersecurity requirements and standards that suppliers must adhere to. This can include compliance with industry frameworks such as ISO 27001, National Institute of Standards and Technology (NIST) Cybersecurity Framework, or specific civil aviation cybersecurity Policy. Specify the security controls and practices expected from suppliers, including data encryption, access controls, and vulnerability management.

d) Implement mechanisms for ongoing monitoring and auditing of suppliers' civil aviation cybersecurity practices. Regularly assess their compliance with contractual obligations and industry standards. Conduct periodic civil aviation cybersecurity assessments, vulnerability assessments, and penetration testing to identify and mitigate potential risks in the supply chain.

e) Define the procedures and expectations for suppliers to report civil aviation cybersecurity incidents promptly. Establish a clear incident response plan and coordinate with suppliers to ensure effective incident management.

f) Encourage suppliers to have their incident response capabilities and plans in place to mitigate the impact of potential cyber incidents.

g) Foster a culture of information sharing and collaboration with suppliers to address emerging threats and vulnerabilities. Encourage the exchange of civil aviation cybersecurity best practices, threat intelligence, and lessons learned. Participate in industry forums, working groups, and initiatives to enhance supply chain security in the aviation sector.

h) Regularly assess supplier performance in terms of civil aviation cybersecurity. Monitor their adherence to contractual obligations, track incident response and resolution, and evaluate their compliance with security standards.

i) Consider performance indicators and metrics to objectively measure supplier performance and address any identified shortcomings.

j) Provide civil aviation cybersecurity education and awareness programs to suppliers. Promote the importance of civil aviation cybersecurity best practices, secure coding standards, and data protection measures. Encourage suppliers to prioritize cybersecurity in their internal processes and train their employees on civil aviation cybersecurity awareness and incident response.

k) Require suppliers to have robust business continuity and contingency plans to address

potential disruptions in the supply chain. Ensure they have adequate backup systems, redundancy measures, and recovery procedures in place to minimize the impact of cyber incidents.

l) Stay updated on relevant regulations and legal requirements related to supply chain security in civil aviation cybersecurity. Ensure suppliers are aware of their obligations and are compliant with applicable laws and regulations, including data protection and privacy regulations.

12. Physical Security

12.1 Civil Aviation cybersecurity stakeholders should:

a) Implement strict access controls, video surveillance, and environmental controls (such as fire
suppression systems and temperature regulation) in data centers and server rooms where critical aviation systems and data are stored.

b) Implement robust access control measures, including the use of access cards, biometric systems, and security personnel, to restrict physical access to critical areas where aviation systems and network infrastructure are located.

c) Physically secure network equipment, such as routers, switches, and firewalls, in locked cabinets or secure rooms to prevent unauthorized access or tampering.

d) Ensure proper cable management to prevent unauthorized access or damage to network cables, which can compromise the integrity and availability of aviation systems.

e) Establish procedures for the secure disposal of IT equipment, such as computers, servers, and storage devices, to prevent unauthorized access to sensitive data. This may involve securely wiping data or physically destroying storage media.

f) Deploy closed-circuit television (CCTV) cameras and monitoring systems to monitor and record activities in critical areas, including server rooms, control centers, and other sensitive locations.

g) Provide civil aviation cybersecurity awareness training to employees and contractors to educate them about physical security best practices and the importance of safeguarding physical assets and infrastructure.

h) Develop incident response plans that address both cyber incidents and physical security incidents. Establish clear procedures for reporting and responding to physical security breaches or suspicious activities.

i) Foster collaboration and coordination between civil aviation cybersecurity teams and physical security teams to ensure a holistic and integrated approach to protecting aviation systems and infrastructure.

j) Conduct regular physical security assessments to identify vulnerabilities and gaps in security measures. These assessments should be performed by qualified personnel

and follow established methodologies.

k) Install intrusion detection and alarm systems in critical areas to detect and alert security personnel of unauthorized access attempts or breaches. Regularly test and maintain these systems to ensure their effectiveness.

l) Employ trained security personnel to patrol critical areas, conduct security checks, and respond to incidents. Provide them with appropriate training, equipment, and procedures to carry out their duties effectively.

13. Information, Communication, Technology (ICT) Security

13.1 Civil aviation is highly reliant on the availability of information and communication technology (ICT) systems and data, as well as on the accuracy and confidentiality of data, in order to operate efficiently, safely and securely. The protection and resilience of aviation systems against cyber threats and vulnerabilities can only be progressed through a collaborative approach involving the collective expertise of aviation security, air navigation, ICT security and other civil aviation cybersecurity stakeholders.

13.2 Civil Aviation cybersecurity stakeholders should:

a) Ensure the confidentiality, integrity, and availability of information and communication systems to safeguard aviation operations from cyber threats.

b) Perform comprehensive risk assessments to identify and evaluate potential civil aviation cybersecurity risks associated with ICT systems.

c) Develop threat models specific to aviation operations to understand potential attack vectors and vulnerabilities.

d) Formulate a robust ICT security policy that outlines organizational commitments, roles, responsibilities, and compliance requirements.

e) Implement ongoing user awareness programs to educate personnel about ICT security policies and practices.

f) Implement role-based access controls to ensure that personnel have the minimum necessary access required for their responsibilities.

g) Utilize multi-factor authentication to enhance the security of access to critical systems.

13.3 Examples of ICT security controls of relevance to civil aviation cybersecurity include, inter alia, access control policies and application of least privilege principles, software/hardware firewalls and network security, cryptography, organizational password policies, end-point protection, network monitoring and detection of anomalies, network separation, device management, etc.

14. Incident Management and Continuity of Critical Functions

14.1 Safety of operations and continuity of critical functions shall be the main drivers in incident management processes. Testing crisis management and recovery plans shall be an integral part of incident management to maintain continuity of critical functions.

14.2 Civil Aviation cybersecurity stakeholders should:

a) Create a comprehensive incident response plan that outlines the steps to be taken in the event of a civil aviation cybersecurity incident. This plan should include roles and responsibilities, communication protocols, escalation procedures, and clear Policy on incident detection, containment, eradication, and recovery.

b) Form a dedicated incident response team comprising individuals with the necessary technical expertise and knowledge of aviation systems. Ensure that team members have defined roles and responsibilities and are trained in incident response procedures.

c) Regularly conduct tabletop exercises and simulations to test the effectiveness of the incident response plan. These exercises can help identify any gaps or weaknesses in the response process and allow the team to practice their roles and responsibilities in a controlled environment.

d) Deploy robust civil aviation cybersecurity tools and systems for proactive incident detection and monitoring. This can include intrusion detection systems (IDS), security information and event management (SIEM) solutions, and network traffic analysis tools. Continuous monitoring allows for early detection of cyber threats and prompt response.

e) Set up clear communication and reporting channels for incident reporting and escalation. Ensure that all employees are aware of how and where to report civil aviation cybersecurity incidents promptly. Implement a process for regular communication updates to stakeholders, including management, IT teams, and regulatory authorities.

f) Establish relationships and lines of communication with external partners, such as cybersecurity incident response firms, aviation regulatory bodies, and law enforcement agencies. Collaborating with these entities can provide additional resources, expertise, and support during incident response and investigation.

g) In the event of a civil aviation cybersecurity incident, preserve all relevant evidence and conduct forensic analysis to determine the root cause, extent of the breach, and any potential impact. Document and maintain a chain of custody for the evidence to support any legal or regulatory requirements.

h) Establish procedures for notifying and engaging relevant stakeholders, including customers, partners, regulatory agencies, and affected individuals, in the event of a significant civil aviation cybersecurity incident. Comply with legal and regulatory requirements for timely and accurate disclosure of incidents.

i) Develop robust recovery and business continuity plans to minimize the impact of a civil aviation cybersecurity incident on operations. These plans should outline

procedures for restoring affected systems, validating data integrity, and resuming normal business activities in a secure and controlled manner.

14.3 After the incident is resolved, civil aviation cybersecurity stakeholders should conduct a thorough analysis of the incident response process and identify areas for improvement, and document lessons learned and update the incident response plan and other relevant policies and procedures accordingly.

15. Cybersecurity Culture in Civil Aviation

15.1 Cybersecurity culture is commonly understood to be a set of assumptions, attitudes, beliefs, behaviours, norms, perceptions, and values that are inherent in the daily operation of an organization and are reflected by the actions and behaviours of all entities and personnel in their interaction with digital assets.

15.2 A positive cybersecurity culture aims to make civil aviation cybersecurity considerations part of the organization's habits, conducts, and processes, by embedding them in daily operations as reflected by the actions and behaviours of all personnel.

15.3 The establishment of a strong and effective civil aviation cybersecurity culture, as an integral part of an organizational culture, assists organizations in improving their overall performance through the early identification of potential cyber risks.

15.4 Cybersecurity culture in civil aviation builds upon the sector's experience, efforts, and success in implementing robust aviation safety and security cultures, and shares with them many core elements. This cross-domain nature of cybersecurity culture not only leads to enhancing civil aviation cybersecurity posture, but also results in positive spill-overs across the three domains in supporting the promotion and reinforcement of positive safety, security, and civil aviation cybersecurity cultures.

15.5 In summary, civil aviation cybersecurity culture allows every person in the organization, regardless of their role, to better perform in the digital environment. Examples of benefits of designing and implementing an effective and robust cybersecurity culture include:

a) Enhanced civil aviation cybersecurity maturity of the organization;

b) Appropriate handling of information by all personnel;

c) Improved civil aviation cybersecurity posture that supports the effectiveness and efficiency of the organization in mitigating cyber risks;

d) Enhanced awareness of all personnel to cyber risks and the role that they individually play identifying and mitigating those risks; and

e) Willingness to report personal oversight in applying organizational civil aviation cybersecurity processes and procedures as well as reporting of suspicious cyber activities, leading to proactiveness and better detection of cyber risks.

15.6 The core elements of an effective organizational civil aviation cybersecurity culture are illustrated in the following sections of this guidance. However, although these core elements are

well defined, cybersecurity culture should be uniquely designed within each organization. It should take into account different aspects, including the organizational civil aviation cybersecurity maturity level, existing cultures and values, and the overall civil aviation cybersecurity threat landscape.

15.7 The core elements of a robust and effective civil aviation cybersecurity culture in civil aviation are:

a) Leadership;

b) Cross-domain links;

c) Communication;

d) Awareness, training and education;

e) Reporting systems;

f) Continuous review and improvement; and

g) Positive work environment.

15.7.1 Leadership

15.7.1.1 An effective civil aviation cybersecurity culture depends on the commitment of every person in the organization, starting with senior management. Senior management should provide their full commitment to civil aviation cybersecurity culture, always and across all activities, strategies, policies and organizational objectives.

15.7.1.2. Senior management should comply with civil aviation cybersecurity policies, lead by example, and become role models for the organization's managers and personnel. They should also advocate for civil aviation cybersecurity as an organizational and personal value while similarly working towards aligning their behaviours with such value.

15.7.1.3. In that regard, senior management should:

a) Endeavour to enhance their knowledge of cybersecurity in civil aviation.

b) Abide by civil aviation cybersecurity rules, processes, and procedures always and lead by example.

c) Clearly include civil aviation cybersecurity as an organizational priority.

d) Enshrine civil aviation cybersecurity in the written policies of the organization to become an integral part of the company's management plan;

e) Provide visible support to the implementation of civil aviation

cybersecurity culture;

f) Ensure and support civil aviation cybersecurity training and capacity building for all personnel;

g) Ensure the processing of civil aviation cybersecurity reports in a timely fashion and ensure the prompt implementation of any required corrective and preventive actions;

h) Intervene appropriately whenever civil aviation cybersecurity is compromised; and

i) Monitor the development of the civil aviation cybersecurity posture of the organization, civil aviation cybersecurity culture, and the measures and resources assigned to support the continuous improvement of civil aviation cybersecurity culture's adoption across the organization.

15.7.1.4. Following the lead of senior management, the organization's management layers should also strive to adopt the actions included in paragraph 4.3, in line with their responsibilities and span of management, in order to propagate the commitment to civil aviation cybersecurity culture across the organization.

15.7.2 Cross-Domain Links

15.7.2.1 Taking into account the multitude of cyber risks and vulnerabilities in every organization, cross domain links should be formally established.

15.7.2.2 A multidisciplinary Task Force reporting to senior management might be established as a means to support coordination of civil aviation cybersecurity culture across the organization.

15.7.2.3 The Task Force's objectives would include the following:

a) Periodically assess the maturity of civil aviation cybersecurity culture within the organization;

b) Identify risks and opportunities with regards to civil aviation cybersecurity culture implementation;

c) Bridge the perspectives of different internal stakeholders with regards to civil aviation cybersecurity culture; and

d) Support the development and implementation of cross-domain activities related to fostering civil aviation cybersecurity culture in the organization.

15.7.3 Communication

15.7.3.1 Communication plays an essential role, both internally and externally, in ensuring the
implementation of successful civil aviation cybersecurity culture. It is the main means through which the expected level of awareness can be reached.

15.7.3.3 Senior management should ensure that internal policies and Policy regarding civil aviation cybersecurity, as well as the reason for their introduction, are duly communicated to all personnel. A robust internal communication programme contributes to the acceptance and understanding of civil aviation cybersecurity measures by all personnel, and helps promote civil aviation cybersecurity culture in the organization.

15.7.3.4 In addition, internal communication programmes would greatly assist in:

a) Ensuring that all personnel are fully aware of their duties, rights, and the reporting mechanisms in place in the organization; and

b) Promoting the organizational digital code of conduct, that includes the processes, measures
and controls those personnel should comply with at all times.

15.7.4 Awareness, Training & Education

15.7.4.1 Awareness, training and education are key areas of the learning process that should be leveraged for a robust civil aviation cybersecurity culture. Awareness provides people with knowledge, training teaches skills, and education provides knowledge and skills within a theoretical framework, hence integrating awareness and training.

15.7.4.2. All civil aviation personnel who interact with the organization's digital assets, regardless of their roles or functions, should undertake a civil aviation cybersecurity awareness, training, and education programme in order to ensure that they are equipped with required knowledge and skills on civil aviation cybersecurity risks, measures and objectives. These programmes should be adapted to the audience, as necessary and possible.

15.7.4.3 Civil aviation cybersecurity awareness programmes should be delivered to all personnel upon their hiring, as well as a recurrent training. The time intervals for the recurrence of the awareness programme should be identified based on the level of maturity of civil aviation cybersecurity culture in the organization, and can be revisited in line with the development of this maturity level.

15.7.4.4 It is recommended that civil aviation cybersecurity awareness programmes be delivered at least once in person (in a physical or virtual classroom setting). Civil aviation cybersecurity is not a familiar topic to all personnel and is sometimes hard to be digested without guidance from a professional. As such, interaction with a professional in a classroom setting

facilitates the understanding of civil aviation cybersecurity topics. It allows the trainer to explain concepts, processes, procedures, and controls in a simplified manner to be understood by the non-technically savvy personnel, as well as explain the benefits in enhancing the civil aviation cybersecurity posture of the organization and its positive impact on the overall productivity of personnel.

15.7.4.5 Following an initial in-person awareness/training session, organizations may consider using e-learning methods (computer managed learning) for recurrent training. Such decision should take into account the development of civil aviation cybersecurity culture in the organization, as well as changes in civil aviation cybersecurity processes, controls, and procedures introduced in the organization in response to the evolving civil aviation cybersecurity risk landscape.

15.7.4.6 Civil aviation cybersecurity awareness programmes should be delivered by professionals that possess the required technical knowledge. However, one of the challenges faced with technical awareness programmes is the lack of soft skills by the presenters, whereby adequate communication and “sales” skills go a long way in engaging personnel and ensuring their buy-in and support to civil aviation cybersecurity culture. Accordingly, organizations should ensure that awareness programme leaders are equally equipped with the technical knowledge and soft skills necessary to instill in personnel behavioural changes to support the adoption of civil aviation cybersecurity culture.

15.7.4.7 A typical civil aviation cybersecurity awareness programme should include the following subjects:

a) The purpose of the awareness programme;

b) Existing communication mechanisms in the organization;

c) A general overview of cyber risks to civil aviation and potential consequences (including examples);

d) Civil aviation cybersecurity controls, processes, and procedures of the organization;

e) The role of the human element in safeguarding the organization against cyber risks; f) the importance of personnel reminding each other of organizational civil aviation cybersecurity principles when observing non-compliant actions by their colleagues;

f) Overview of the different exploit methods that may target people and their consequences (including examples);

g) How to identify suspicious cyber activities;

h) The impact of complacency on the organization (including examples);

i) Principles of cyber hygiene;

j) Proper handling of sensitive data and information; and l) reporting mechanisms, how to use them, and follow-up mechanisms

15.7.4.8 Civil aviation cybersecurity awareness campaigns should also be used periodically, as a reminder, in order to reinforce the knowledge and skills of personnel. Various tools are available for that purpose including:

a) Paper-based tools – such as posters, brochures, booklets, etc. This type of media can be easily distributed and digested. However, they are passive tools and require frequent update (and a new print with each update); and

b) Online tools – such as e-mails, newsletters, messages on screen savers, intranet, short videos, faq pages, e-learning (computer managed learning), etc. The main advantage of these tools compared to paper-based tools is their ability to reach the whole organization. They are relatively easy to update in terms of resources, and have a low production cost.

15.7.5 Reporting Systems

15.7.5.1 A cornerstone of civil aviation cybersecurity culture is the development and implementation of an internal civil aviation cybersecurity reporting system. Such system allows the organization to proactively manage its cyber risks, measure the development of the organization's civil aviation cybersecurity posture, identify and plan awareness and training needs of staff, and adapt its internal processes, controls, and measures in line with the development of civil aviation cybersecurity trends and with the maturity of civil aviation cybersecurity culture.

15.7.5.2 Civil aviation cybersecurity reporting systems gather elements from both aviation safety and aviation security reporting systems. As such, they address two areas: the first area is reporting of self-actions/errors that are not in line with the organizational information security policies and processes, and the second area is reporting of suspicious/erroneous behaviour of other employees.

15.7.5.3 When developing their civil aviation cybersecurity reporting mechanism, organizations are encouraged to benefit from the experience gained in developing and implementing aviation safety and aviation security reporting systems.

15.7.5.4 The following elements should be considered when implementing a civil aviation cybersecurity reporting system:

a) Confidentiality of personal information, whereby personal data is not collected and/or stored. When personal data is collected it should only

be used to either gain clarification, further information about the reported occurrence or offer feedback to the reporter;

b) In order to ensure the confidentiality of personal information, a policy should be developed that clearly identifies, and holds accountable, the person(s) tasked with managing, maintaining, guaranteeing the confidentiality, analyzing, and following up on collected information;

c) Providing adequate training to all personnel on how to use the reporting system;

d) Implementing a just culture in civil aviation cybersecurity reporting, and providing adequate awareness to all personnel on how a just culture works so that they are more comfortable providing information; and

e) Implementing, as applicable, an incentive programme aimed at encouraging personnel to report their own errors as well as any suspicious cyber behaviours they observe.

15.7.6 Continuous review and improvement

15.7.6.1 Organizations should develop a performance indicator framework designed to assess the impact of measures in place on civil aviation cybersecurity culture as well as to determine the gap existing between desired and actual culture outcomes.

15.7.6.2 As some elements of civil aviation cybersecurity culture may not be directly observed, a range of possible indicators can be used to measure the effectiveness of cybersecurity culture. Such measures may include:

a) Statistics on reported incidents (considered comparatively with data mined from the organization's logs) to measure civil aviation cybersecurity performance of personnel, their level of awareness, and the progress achieved in promoting civil aviation cybersecurity reporting;

b) Results of recurrent training sessions;

c) Results from simulations of malicious attacks to test response of personnel; and

d) Questionnaires and interviews.

15.7.7 Positive work environment

15.7.7.1 A general positive work environment may also greatly influence commitment of personnel to civil aviation cybersecurity culture and enhance cybersecurity performance.

15.7.7.2 A positive work environment should include, at a minimum:

a) The involvement of personnel in decision-making processes (e.g. Suggestions for improvement to civil aviation cybersecurity awareness training programmes);

b) The allocation of sufficient time for personnel to complete training on proper cyber hygiene;

c) A mechanism for recognizing good performance (i.e. Incentives and/or reward programmes);

d) The provision of feedback to personnel on suggestions and on civil aviation cybersecurity reports;

e) Setting clear, achievable and measurable goals with regards to civil aviation cybersecurity incidents, and periodic feedback to personnel on how the organization is advancing in that regard;

f) The provision of the necessary procedures, awareness, training, and tools to enable personnel to perform their duties; and

g) Providing personnel with the appropriate levels of autonomy and responsibility.

— **END** —