THE UAE CIVIL AVIATION CYBERSECURITY POLICY

1. INTRODUCTION

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

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

2. SCOPE

2.1 Civil Aviation cybersecurity shall address the security and resilience of the civil aviation system, as well as support the collaboration with concerned non-aviation entities and authorities, including the UAE National Cybersecurity Council, State Security Department, Ministry of Interior and Ministry of Defence, as appropriate.

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

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

3. OBJECTIVES

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

4. GOVERNANCE AND ORGANIZATION

4.1 In accordance with the United Arab Emirates (UAE) Ministerial Letter reference GCAA/C/54-23 Date: 31 Oct. 2023 from the Minister of Economy and the Chairman of GCAA Board to the International Civil Aviation Organization (ICAO) nominating 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 The GCAA shall:

(i) determine, in coordination with the National Competent Authority for Cybersecurity, which is the UAE National Cybersecurity Council, the roles and responsibilities to be undertaken by each authority and entity in the UAE related to civil aviation cybersecurity and cyber resilience;

(ii) lead the development of civil aviation cybersecurity regulations (CARs);

(iii) define roles and responsibilities for the sectors within the General Civil Aviation Authority related to cybersecurity;

(iv) coordinate the definition of roles and responsibilities of civil aviation entities overseen by the General Civil Aviation Authority through the National State Safety Programme and National Civil Aviation Security Programme;

(v) define the elements of civil aviation cybersecurity culture and monitor its implementation;

(vi) define regulations, processes, requirements, and roles for civil aviation cybersecurity crisis management, including testing requirements and frequencies;

(vii) coordinate cross-cutting civil aviation cybersecurity issues with relevant nonaviation stakeholders involved in civil aviation cybersecurity such as information sharing and incident investigation;

(viii) represent the UAE at civil aviation related Cybersecurity forums at the international, regional, multilateral and bilateral forums, including but not limited to the International Civil Aviation Organisation (ICAO) Cybersecurity Panel, its working groups, task forces etc. as appropriate;

(ix) undertake other roles and responsibilities in accordance with the ICAO Standards and Recommended Practices, as well as other concerned international civil aviation safety and aviation security entities, as appropriate.

5. RISK MANAGEMENT

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

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

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

6. CRITICAL SYSTEMS SECURITY

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

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

6.3 Redundancy of critical systems shall be considered as an enabler for system security and continuous availability and operational resilience against failures from cyber threats.

6.4 To achieve and maintain appropriate protection of organizational assets.All assets should be accounted for and have a nominated owner.

7. DATA SECURITY

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

7.2 Access to information, information processing facilities, and business processes should be controlled on the basis of business and security requirements.

8. SUPPLY CHAIN SECURITY

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

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

9. PHYSICAL SECURITY

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

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

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

10. INFORMATION, COMMUNICATION, TECHNOLOGY (ICT) SECURITY

10.1 ICT security shall be part of Civil aviation cybersecurity management.

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

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

11. INCIDENT MANAGEMENT AND CONTINUITY OF CRITICAL FUNCTIONS

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

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

12. CYBERSECURITY CULTURE

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

12.2 Cybersecurity culture shall be fully coordinated/integrated within existing safety and security cultures.

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

-END-