Implementation of PART-IS Requirements by Aerodrome Operators

(In accordance with Commission Implementing Regulation (EU) 2022/1645)

Civil Aviation Directorate (CAD)

Air Navigation Services & Aerodromes Unit (ANS&AU)

Malta Transport Centre, Pantar Road, Lija LJA 2021, Malta.

Tel: +356 2555 5608, Fax: +356 2123 9278

info.tm@transport.gov.mt, http://www.transport.gov.mt

Document Approval

Prepared by:	Stephen J Muscat	Senior Inspector	
Approved by:	Capt. Charles Pace	Director General for Civil Aviation	

Contents

1. Revision History....4
2. Introduction....5
3. Applicability 5
4. Definitions and Abbreviations 5
5. Governance and Accountability……...6
6. Information Security Management System (ISMS)....6
7. Information Security Risk Management....7
8. Information Security Controls 7
9. Human Factors, Training, and Awareness 7
10. Information Security Incident Management……8
11. Business Continuity and Resilence……8
12. Interfaces and Third Party Management..……8
13. Compliance Monitoring and Management Review...……8
14. Documentation and Records…..……...8
15. Relationship with the CA……..…… 9
16. Entry into Application…...……..……..……..……..…..9
17. Appendix A - PART-IS Compliance Mapping Table (Aerodromes)… ……..10

1. REVISION HISTORY

Version	Date	Change
1	18 February 2026	Initial Issue.

2. Introduction

The objective of this Aerodrome Standards Advisory Document (ASAD) is to provide structured guidance to aerodrome operators for the implementation of PART-IS (Information Security) requirements introduced by Commission Implementing Regulation (EU) 2022/1645. This Document supports harmonized, risk-based, and proportionate implementation on aerodromes under the EASA scope.

This ASAD supports compliance with: (EU)2022/1645; (EU)139/2014 as amended featuring PART IS requirements applicable to aerodrome operators. Additionally, this document should be read in conjunction with applicable EASA AMC and GM, any applicable national implementation measures, and other relevant EU legislation.

3. Applicability

This ASAD applies to the following:

- Certified Aerodrome Operators under (EU)139/2014;
- Applicants for aerodrome certification under EASA Rules;
- Organisations managing aerodrome-related information and communication technology (ICT) systems supporting operations;

PART-IS applies to information, data, and systems that support:

- Aerodrome operational functions;
- Safety critical and safety supporting services;
- Security, maintenance, and emergency response functions;
- Interfaces with external aviation stakeholders (ANSPs, GHSPs, etc);

Implementation shall be proportionate to the aerodrome size and complexity and operational environment and traffic volume. It shall also take into consideration the degree of digitalization and system interconnectivity.

4. Definitions and Abbreviations

For the purpose of this ASAD, the following definitions apply:

- PART-IS: The set of information security requirements established under (EU) 2022/1645.
- INFORMATION SECURITY: Preservation of confidentiality, integrity, authenticity, and availability of network and information systems.
- ISMS: Information Security Management System.
- ICT SYSTEM: Any system, network, or application used to process, store, or transmit information.

- INFORMATION SECURITY INCIDENT: An event that compromises, or has the potential to compromise, information security.
- ACCOUNTABLE MANAGER (AM): The person with overall authority and responsibility for the organisation.

Terms not defined herein shall have the meaning assigned in applicable EU aviation regulations.

5. Governance and Accountability

Accountable Manager Responsibilities:

The Accountable Manager shall be responsible for compliance with PART-IS requirements and ensure allocation of adequate human, technical, and financial resources. S/he shall approve the information security policy and promote an organizational culture supporting information security.

Information Security Management Function:

Aerodrome operators must designate an Information Security Manager or equivalent function responsible for coordinating PART-IS implementation and maintenance. This person shall manage information security risks and advise management on information security matters. S/he shall act as focal point with competent authorities and external stakeholders. All roles, responsibilities and authorities shall be documented.

6. Information Security Management System (ISMS)

Aerodrome operators shall establish and maintain an ISMS as part of the overall management system required by (EU) 139/2014. It is thus expected that the associated document will form part of the Aerodrome Manual as a sub-part. This shall be approved by TM-CAD, and the manual shall be introduced and processed through the established change management process.

The ISMS shall be appropriately documented, implemented, and follow a continuous improvement cycle and integrated with the Aerodrome's Safety Management System (SMS).

The Aerodrome Operator should define an information security policy aligned with organisational objectives and measurable information security objectives.

7. Information Security Risk Management

Aerodrome Operators shall maintain an inventory of information assets, ICT systems and networks, and interfaces and data exchanges.

They shall identify potential threats which may include: *cyber-attacks and malware*; *insider threats (intentional or unintentional*); *system failures*, *loss of availability, and physical (analogue)*. Additionally, vulnerabilities related to people, processes, and technology should be identified.

Furthermore, they must ensure that information security risks are assessed using defined criteria, evaluated against risk acceptance thresholds and treated using appropriate controls. Risk assessments and treatment decisions should be documented and reviewed periodically.

8. Information Security Controls

The Aerodrome Operator shall ensure that controls are selected based on risk assessment outcomes and may include the following:

- Access control and authentication;
- Network security and segmentation;
- Data protection and backups;
- Change and configuration management;
- Physical protection of ICT assets.

It shall be ensured that controls address confidentiality, integrity, authenticity, and availability.

9. Human Factors, Training, and Awareness

Aerodrome operators shall ensure that personnel understand their information security responsibilities by receiving initial and recurrent training appropriate to their role. It must also be ensured that they are aware of reporting mechanisms for information security events.

10. Information Security Incident Management

Aerodrome operators must develop and implement procedures for identifying and reporting information security incidents. These procedures should ensure prompt detection, response, and recovery, reduce impacts on operational safety and security, and enable effective investigation and the documentation of lessons learned. They should also include processes for identifying vulnerabilities.

Incident management activities should be aligned and coordinated with existing emergency and crisis management arrangements.

11. Business Continuity and Resilience

The ISMS should support organisational resilience by identifying critical information and systems, defining recovery objectives, implementing backup and recovery solutions, and periodically testing continuity arrangements.

12. Interfaces and Third-Party Management

The Aerodrome Operator shall manage information security risks associated with external parties by conducting risk assessments of third-party services. In addition, safety related information security requirements shall be defined within contracts, and appropriate oversight and monitoring of service providers shall be maintained.

13. Compliance Monitoring and Management Review

It is expected that the Aerodrome Operator ensures compliance with PART-IS through the conduct of internal audits and inspections. It shall also monitor information security performance indicators and facilitate reviews by management.

14. Documentation and Record keeping

Aerodrome Operators should maintain controlled documentation demonstrating ISMS implementation. Furthermore, records of risk assessments, controls, training, incidents, audits, and reviews shall be maintained.

15. Relationship with the Competent Authority

Aerodrome Operators are expected to cooperate with TM-CAD by providing information related PART-IS compliance. They shall notify significant information security events in accordance with established procedures and applicable requirements.

16. Applicability

This ASAD supports readiness for the applicability dates set out in Regulation (EU) 2022/1645 for both currently certified aerodromes and future applications for certification under EU regulatory requirements.

APPENDIX A – PART-IS Compliance Mapping Table for Aerodromes

PART-IS Requirement Area	Aerodrome Implementation Element	Typical Evidence	Management System Interface
Governance & Accountability	Accountable Manager responsibility for IS	Accountable Manager statement	Management System Manual
IS Policy & Objectives	Information Security Policy	Approved policy document	Management System/SMS
Risk Management	IS risk assessment process	Risk register, assessments	SMS risk management
Asset Management	ICT and information inventory	Asset register	Configuration management
Security Controls	Technical and organisational controls	Procedures, system configs	Engineering/IT
Training & Awareness	IS Training programme	Training records	Human factors
Incident Management	IS incident procedures	Incident reports	Emergency response
Business Continuity	ICT continuity arrangements	BCP, test results	Aerodrome emergency planning
Third-Party Management	Supplier IS oversight	Contracts, audits	Procurement
Compliance Monitoring	Internal audits & reviews	Audit reports	Compliance monitoring