Aerosystems Information Security Policy

Scope

This Information Security Policy applies to all employees, contracted organisations, and third parties who access, process or manage information and systems owned or operated by Aerosystems, including physical and digital assets, within the scope of aviation safety related operations.

Policy Statement

Aerosystems is committed to protecting the confidentiality, integrity, and availability of its information systems and aviation data. This policy applies to all information systems, networks, applications and data used within the scope of design, modification and certification activities under UNI EN ISO 9100:2028 / ISO 9001:2015 and UNI EN ISO 14001:2015+A1:2024, Part-21, Part-145 and SMS Safety Management System; sensitive technical, operational and administrative data relevant to aviation safety.
This policy ensures appropriate safeguards are in place to prevent unauthorized access, disclosure, alteration, or destruction of information, in compliance with applicable laws, industrial standards, regulations and associated Acceptable Means of Compliance (AMC); all activities shall comply with Regulation (EU) 2022/1645 and Regulation (EU) 2023/203, Regulation (EU) 2018/1139 and Directive (EU) 2016/1148 (NIS Directive).

In accordance with the Regulation, Aerosystems has implemented an ISMS that includes:

- Risk assessment and treatment processes;
- Defined roles and responsibilities for managing information security risk;
- Monitoring, measurement, analysis and evaluation of the ISMS effectiveness;
- Continuous improvement through regular audits and management reviews.

Objectives

- **Ensure Data Protection:** Protect sensitive operational, customer, and personnel data from unauthorized access, use, disclosure, disruption, modification or destruction;
- **Mitigate Risks**: Identify, assess, and mitigate risks to the company's information systems through regular reviews and controls.
- **Support Business Continuity:** Maintain reliable and secure Information Security Management System (ISMS) aligned with Regulatory Requirements to ensure uninterrupted operations and timely recovery in case of incidents.
- **Promote Awareness and Responsibility:** Promote the policy through training or awareness sessions within the organisation to all personnel on a regular basis or upon modifications, encouraging the implementation of a "just-culture" and the reporting of vulnerabilities, suspicious/anomalous events and/or information security incidents;

Regulatory Compliance

Aerosystems ensures its information security practices align with Regulation (EU) 2022/1645 and Regulation (EU) 2023/203, addressing aviation cybersecurity risk management and incident notification, including:

- **Implementing cybersecurity risk assessment** and mitigation strategies for critical systems.
- **Ensuring timely notification reporting** of security incidents to the competent authorities as mandated.
- **Maintaining up-to-date** technical and organizational measures to manage cyber threats effectively.
- **Communicating** the information security policy to all relevant parties, as appropriate.

Responsibility and Review

The Accountable Manager is responsible for enforcing this policy.
The policy will be reviewed annually or following significant changes in the regulatory environment or operational structure.

Approved by Accountable Manager: Stefano Zambra
Effective Date: June 20, 2025

Signature: