INFORMATION SECURITY POLICY

AIR NOSTRUM LÍNEAS AÉREAS DEL MEDITERRÁNEO, S.A.U. and AIR NOSTRUM ENGINEERING AND MAINTENANCE OPERATIONS, S.L.U. (hereinafter collectively referred to as "the organisation") are committed to developing, implementing, maintaining, and improving the strategies and processes that ensure all activities are carried out with appropriate organisational resources, in order to achieve the highest levels of safety and comply with all regulatory requirements.

The organisation's Information Security Policy promotes a culture that prioritises the protection of its passengers, employees, aircraft, and information systems against information security risks.

All personnel and contracted service providers across all departments share responsibility for information security in their daily activities and are expected to actively contribute to safeguarding the organisation's information.

The Accountable Manager will hold overall responsibility for the Information Security Management System (ISMS).

The above objective will be achieved by undertaking the following measures:

- Compliance with all applicable legislation, regulatory requirements, and consideration of relevant standards and best practices in information security detailed in the organisation's ISMS.
- The establishment of information security objectives and performance indicators and targets.
- Defining and implementing appropriate and acceptable levels of security for information assets, communication systems, technology infrastructure, supporting systems that may have an impact on aviation safety.
- Applying ISMS requirements within operational and support processes of the organisation.
- Maintaining, monitoring, and improving its ISMS to adapt to evolving threats, technologies, and business requirements, thereby protecting aviation safety, operational resilience, and stakeholder trust.
- Satisfying all applicable requirements regarding information security through proactive and systematic management, supported by adequate resources for implementation and operation.
- Assigning information security as one of the essential responsibilities of all managers, ensuring leadership accountability.
- Promoting awareness and understanding of this policy through regular training and awareness sessions for all personnel and subcontractors, as well as following updates or modifications.
- Encouraging the implementation of a 'just culture' and fostering the reporting of vulnerabilities, suspicious/anomalous events, and information security incidents without fear of reprisal.
- Communicating this policy to all relevant stakeholders, both internal and external, as appropriate.

This policy shall be reviewed annually or when significant changes occur, to ensure continuous relevance, adequacy, and effectiveness within the organisation.

Revision date:
16/10/2026