


INFORMATION SECURITY POLICY

INFORMATION FOR INTERNAL USE

	Policy	PO
	INFORMATION SECURITY POLICY	
	Page 2 of 3	

INFORMATION SECURITY POLICY

GESTAIR's senior management establishes, approves, disseminates, monitors and reviews the Information Security Policy, considering it to be the most appropriate tool for the organisation to achieve its objectives in this area.

The company's management is committed to leading and promoting a security culture aligned with the requirements of the ISO 27001 standard and to ensuring full compliance with all applicable legislation and regulations regarding civil aviation security and cybersecurity, including the provisions of Part-IS. This commitment expressly covers:


- Compliance with the standards, recommended practices and guidelines issued by the International Civil Aviation Organisation (ICAO).
- The application of the regulations, decisions and guidance material published by the European Union Aviation Safety Agency (EASA).
- Strict compliance with the requirements, provisions and circulars issued by the competent national civil aviation authority.

To achieve these objectives, senior management ensures that the policy:

- Is fit for purpose in meeting the organisation's objectives and serves as a framework for establishing and reviewing Information Security objectives.
- Includes an explicit commitment to protect the confidentiality, availability and integrity of information within the scope of the ISMS and to continuously improve its effectiveness.
- Once approved, it is published through the various available channels for the information of all staff and communicated throughout the organisation, ensuring that it is correctly understood and applied.
- It is reviewed annually, ensuring its continued suitability for the organisation's activities, its integration into business processes, alignment with corporate strategy and the allocation of necessary resources.

GESTAIR's ISMS applies to all information and systems that support the provision of business aviation services, including:

- Operational flight information (planning, coordination, permits, handling and associated documentation).
- Customers' personal and contractual data.
- Crew and employee information.
- Financial, administrative and strategic information.
- Technical and aeronautical documentation.

 GESTAIR <small>BY BOOST AIR GROUP</small>	Policy	PO
	INFORMATION SECURITY POLICY	
	Page 3 of 3	

- Technological infrastructure, networks, information systems, communications and corporate devices.

GESTAIR protects information by ensuring its confidentiality, integrity and availability. Access is restricted to authorised personnel, and a systematic risk management approach is applied to identify, analyse and address threats, maintaining risks at acceptable levels defined by management.

The organisation keeps its security and cybersecurity procedures, systems and controls up to date, ensuring they are aligned with current regulations and best practices in the civil aviation sector.

Management sets information security objectives consistent with this policy and regularly monitors compliance through assessments, internal audits and management reviews to ensure its effectiveness and continuous improvement.

All staff and third parties with access to GESTAIR information are responsible for its proper protection and for compliance with this policy. Non-compliance may result in disciplinary or contractual measures.

To achieve these objectives, GESTAIR maintains an Information Security Management System based on the requirements of the ISO 27001 standard, contributing to excellence in the provision of business aviation services.

27 May 2026

Signed by management