Information Security Policy (ISO27001)

May 2026

Summary version website

Isati Srl, with registered office in Via Broggi 9, 21049 Tradate (VA), operates in the design, technical assistance, maintenance services in the aerospace sector and in the assembly, installation, maintenance and repair of aircraft.

The Company recognizes that information (in electronic and non-electronic format), IT systems and network infrastructures are fundamental strategic assets and is committed to protecting them adequately, in line with best practices and the requirements of ISO 27001.

In this context, Isati Srl undertakes to:

1. Information protection

   Guarantee the confidentiality of information, allowing access only to authorized persons, according to the principle of least privilege. Ensure the integrity of the information, preserving it from unauthorized modification, loss or deletion. Maintain the availability of information and services, including through adequate backup systems and business continuity and disaster recovery procedures. Protect the reliability and quality of data to support business decisions and services rendered to customers.

2. Regulatory and contractual compliance

   Operate in full compliance with the applicable legislation on information security and personal data protection, with reference to Regulation (EU) 679/2016 (GDPR) and the national implementing legislation. Ensure compliance with security commitments made to customers, suppliers and contractual partners.

3. Risk management and continuous improvement

   Periodically carry out the analysis and assessment of risks related to information security and information systems. Adopt technical and organizational measures for the prevention, mitigation and treatment of cyber risks, consistent with the risk appetite defined by the company. Monitor the effectiveness of security measures and regularly update the Information Security Management System (ISMS) with a view to continuous improvement.

4. Business continuity, backup and disaster recovery

   Define and update the Business Continuity Plan and the Disaster Recovery Plan, with periodic tests and audits. Ensure that data is backed up regularly and protected by appropriate tools (including encryption) so that it can be restored in the event of adverse events.

5. Management of security incidents and data breaches

   Prepare procedures for the detection, management and recording of anomalous events and IT security incidents. In the event of a personal data breach (data breach), notify the competent authorities and data subjects within the time and in the manner provided for by current legislation.

6. Empowerment and training of staff

   Make all employees and collaborators aware of their roles and responsibilities in the field of information security. Promote training and awareness-raising activities aimed at the correct management of information, information systems and company tools.

7. Management of suppliers and third parties:

Select and manage suppliers and partners based on criteria of competence, reliability and compliance with information security requirements. Ensure, through specific contractual agreements, that third parties who process information or data on behalf of Isati Srl comply with the same security standards adopted by the Company.

8. Physical and logical asset protection:

   Protect business premises and critical infrastructure with physical access controls and monitoring systems. Adopt logical security measures (e.g., strong credentials, multi-factor authentication where applicable, access profiling) to protect access to systems and applications. Safeguard systems from malware and other cyber threats, through up-to-date technical solutions and control procedures.

9. Processing of personal data:

   To process personal data in compliance with the principles of lawfulness, fairness, transparency, minimisation, storage limitation, integrity and confidentiality. To keep the data for the time strictly necessary for the purposes for which they were collected and in accordance with the provisions of laws, regulations and contracts.

This Information Security Policy is reviewed at least annually, as well as whenever there are significant changes of a regulatory, organizational, technological or contextual nature that may affect the level of risk or the commitments made to stakeholders.

The Policy is made available to all personnel, suppliers and partners, and is published on the company website as an expression of Isati Srl's commitment to the protection of information, data and its interlocutors.