Fandis
colors of engineering

INFORMATION SECURITY POLICY

The security and protection of information assets are an essential condition for business success, operational continuity, and the trust of Fandis' stakeholders. Information security requirements are aligned with business objectives, and the Information Security Management System (ISMS) represents the tool that enables information sharing, the execution of correct operations, and the reduction of information-related risks to acceptable levels.

In view of this, the performance of corporate activities must always ensure an adequate degree of:

- **Confidentiality:** the property that information is not made available or disclosed to unauthorized individuals, entities, or processes;
- **Integrity:** the property of safeguarding the accuracy and completeness of information and associated assets;
- **Availability:** the property of being accessible and usable upon request by an authorized entity;

of information, through the adoption of a formal "Information Security Management System" (ISMS) in line with the expectations of Fandis' stakeholders and in compliance with current regulations.

Specifically, the organization's Information Security Management System (ISMS) covers the activities of *"Design, manufacture and trade of components and devices for temperature control of electromechanical and electronic equipments and of insect screen systems and solar screens."*

The general objectives of the ISMS, pursued through management's commitment, are:

- To minimize the risk of loss and/or unavailability of managed data, by planning and managing activities to guarantee service continuity;
- To conduct continuous and appropriate risk assessment to periodically identify, evaluate, and treat cyber and information security risk, constantly examining the vulnerabilities and threats associated with system activities in order to reduce exposure to both internal and external factors;
- To promote training and sensitization programs (Cyber Security Awareness) for all personnel, increasing their awareness and reducing the risk associated with the human factor (e.g., Phishing);
- To promote collaboration, understanding, and awareness of the ISMS by strategic suppliers;
- To comply with current laws and regulations, contractual requirements, and the established procedures;
- To comply with the principles and controls established by ISO/IEC 27001:2022 or other standards/regulations governing the company's activities, including, in particular, regulations regarding personal data processing and its security (GDPR and national legislation);
- To guarantee a timely response to security incidents through the application of proven operational procedures for their detection, reporting, and management, in order to minimize business impact and quickly restore normal operations.

All personnel, within the scope of their respective responsibilities, are involved in reporting any security events or incidents encountered, as well as any identified weaknesses in the ISMS.

The entire organization, starting from top management, is committed to supporting the implementation, operation, and periodic review for the continuous improvement of the ISMS.

Top management commits to pursuing the objectives of this policy with adequate means and resources.

Borgo Ticino,

19 May 2026

CEO

Silvano Zilioli