# INFORMATION SECURITY POLICY

The Organization is committed to ensuring the achievement of its business objectives through the fu ll adherence, by all employees and collaborators, to the principles identified in the Information Sec urity Management System, to the requirements of ISO/IEC 27001:2022, and to all applicable legislati ve, statutory, and regulatory requirements.

This Information Security Policy is based on the following fundamental principles:

- Ensuring the protection of information through the constant application of the principles of Confidentiality, Integrity, and Availability (CIA), applied to all business activities, internal pro cesses, IT systems, services provided, and customer data;
- Meeting the requirements of interested parties, in particular customers, by offering products and services that effectively meet their needs in terms of reliability, operational continuity, a nd information security;
- Promoting the continuous improvement of the Information Security Management System thr ough systematic performance monitoring, risk analysis, internal audits, Management Review , and the adoption of effective corrective and preventive actions;
- Assessing and mitigating information security risks through a structured process of risk identifi cation, analysis, and treatment, ensuring the adoption of appropriate and proportionate te chnical and organizational measures;
- Ensuring compliance with applicable standards, contractual obligations, legal and regulato ry requirements, including those related to data protection and cybersecurity;
  Making available adequate resources and competencies to ensure the effective implemen tation of security measures, promoting awareness, training, and accountability of all person nel;
- Ensuring the operational continuity of critical services by planning, testing, and updating bus iness continuity and incident management plans in order to minimize the impact of any disr uptions or threats;
- Monitoring and managing security incidents by adopting structured procedures for the iden tification, reporting, analysis, and resolution of events, with the aim of reducing residual risks and preventing recurrence;
- Promoting innovation and technological updating, keeping infrastructures and IT solutions al igned with industry standards and best practices in information security.

The Management of **Softech**, with the full involvement of all collaborators, is committed to **communicating, disseminating, and implementing** the principles of this Policy, making it **available to all interested parties** and ensuring its periodic review to verify its continued suitability and effectiveness.

Gallarate, 24 November 2025

The Management of Softech S.r.l.

*Mauro Roncari*