INFORMATION SECURITY POLICY – Finsuge S.p.A.

BONDIOLI & PAVESI

The Finsuge S.p.A. Information Security Policy reflects the commitment of the Management and the entire organisation to guaranteeing the protection of information from any threat, internal or external, deliberate or accidental.
The Board of Directors defines and implements this Policy and entrusts its implementation to the Group Information System Management, ensuring its dissemination, understanding and application at every level of the company.
Information security management is based on the protection of three fundamental principles:

- Confidentiality: ensuring that information is accessible only to duly authorised persons.

- Integrity: preserving the accuracy and completeness of information and processing methods.

- Availability: ensuring that information and the systems that process it are accessible and usable in a timely manner upon request by authorised users.

In order to safeguard these principles, Finsuge S.p.A. has implemented an Information Security Management System compliant with the international standard ISO/IEC 27001, based on the following strategic commitments:

- Information protection: adopting suitable organisational and technical measures to protect company data and the data of customers, suppliers and data subjects, throughout the entire life cycle thereof.

- Training, awareness and empowerment: promoting a culture of security through structured training and awareness programs for all staff.

- Incident management and business continuity: adopting structured procedures for recognising, reporting and managing security incidents, preparing business continuity and disaster recovery plans to limit impacts, ensure service resilience and promote continuous improvement.

- Supplier selection and control: qualifying suppliers based on stringent information security criteria, drawing up specific contractual agreements and carrying out periodic monitoring and checks.

- Access control: enforcing strict policies to manage physical and logical access to information, ensuring that permissions are assigned, revoked or modified in a timely manner based on business roles.

- Continuous improvement and organisational ethics: ensuring the constant improvement of the Information Security Management System through audits, analyses and reviews, operating in compliance with the principles of correctness, transparency and responsibility towards all stakeholders.

The Policy is reviewed in the event of significant changes to the regulatory, organisational or technological context, to ensure its continued adequacy, consistency with the company strategy and alignment with international best practices.

Chairman of Finsuge S.p.A. Board of Directors