In accordance with Italian Legislative Decree no. 138 of 04/09/2025 and subsequent amendments implementing Directive (EU) 2022/2555 (NIS2)

The Company recognises that information security and the operational continuity of its digital services play an essential role in protecting data, information and the interests of its stakeholders. To this end, Management establishes this Cybersecurity Risk Management Policy, which sets out the general principles for adopting organisational and technical measures in line with Directive (EU) 2022/2555 (*NIS2*) and the national implementing legislation.

The Company undertakes to:

- Define and formalise cybersecurity roles, responsibilities and powers, promoting accountability and effective decision-making processes.
- Establish and maintain an information security organisation approved by the governing bodies, ensuring its dissemination and understanding within the relevant functions.
- Maintain an up-to-date list of personnel holding specific cybersecurity roles and responsibilities, making it available to relevant internal stakeholders.
- Establish a Cybersecurity Risk Management Policy based on the operational context, company priorities and the digital protection strategy.
- Adopt documented policies for the following security domains:
  a) Risk management
  b) Roles and responsibilities
  c) Reliability of human resources
  d) Security compliance and audit
  e) Supply chain risk management
  f) Asset management
  g) Vulnerability management
  h) Business continuity and disaster recovery
  i) Digital identity management, authentication and access control
  j) Physical security
  k) Staff training and awareness
  l) Data security
  m) Information and network systems life cycle
  n) Protection of networks and communications
  o) Monitoring of security events
  p) Incident response and recovery

This Policy is communicated to personnel and stakeholders and is subject to review at least once a year and whenever significant incidents, organisational changes or shifts in threat exposure and associated risks occur. Management commits to provide the resources necessary to ensure the effective implementation of the principles set out herein and to promote a process of continuous improvement of the Company's security posture.

Chairman of the Board of Directors

INFORMATION SECURITY POLICY – FINSUGE S.P.A.

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's IT 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 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.

In accordance with Italian Legislative Decree no. 138/2024 implementing Directive (EU) 2022/2555 (NIS2), the Company incorporates the core principles of the European legislation into this Policy and undertakes to:

- Ensure a clear definition of cybersecurity roles and responsibilities.
- Maintain an information security organisation approved by Management.
- Adopt technical and organisational measures appropriate for cyber risk management, asset security, vulnerability management, business continuity and incident response.
- Ensure the dissemination, awareness and compliance with NIS2 requirements across the organisation.

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 the Board of Directors