CYBERSECURITY POLICY

CERTIFICATE OF TRANSPOSITION OF DIRECTIVE (EU) 2022/2555 “NIS2”

[INTRODUCTION AND REFERENCE REGULATIONS]

Cybersecurity is a top priority for STEP SPA. This policy outlines the Management's commitment to implementing a “Cybersecurity Model” designed to safeguard the company's IT systems and the information contained therein against both internal and external threats. To develop this Model, STEP collaborates with a consultancy firm specialized in “Data Governance & Protection,” which supports the certification of the measures outlined in this document. The Model is aligned with the EU Directive 2022/2555 “NIS2”, which serves as the regulatory framework, ensuring its full implementation.

[OBJECTIVES]

The adoption of an effective “Cybersecurity Model” pursues the following objectives:

- protect corporate information from unauthorized access, modification, disclosure or destruction;
- ensure business continuity, minimizing cybersecurity risks;
- comply with applicable IT security regulations and standards;
- contribute to increasing the national and community level of cybersecurity, to protect society and markets.

[SCOPE OF APPLICATION]

This policy applies to all employees, collaborators, suppliers and third parties who access the computer systems and company information of STEP.

[CYBERSECURITY PRINCIPLES]

STEP undertakes to adopt adequate and proportionate technical, operational and organizational measures to manage the risks posed to the security of IT and network systems, used in its business or in the provision of its services, as well as to prevent or minimize the impact of incidents for the recipients of its services. The measures adopted are based on a multi-risk approach, aimed at protecting IT systems and include:

- risk analysis and IT system security policies;
- incident management plans and sharing of information on threats;
- business continuity plans.

[RESPONSIBILITY, TRAINING, AWARENESS]

- **Company Management**: exercises decision-making power in the field of Cybersecurity; assigns roles and responsibilities; approves security measures; supervises their implementation.
- **IT Staff**: is responsible for implementing, monitoring and updating IT security measures.
- **Employees**: follow security policies, procedures and rules; participate in security training; promptly report any incidents.
- **Suppliers and third parties**: must comply with the same security standards applicable to internal employees and ensure adequate protection measures.

STEP will provide regular training and updates on cybersecurity to all employees, to ensure awareness and understanding of Cybersecurity best practices. STEP will select suppliers who guarantee adequate security standards, periodically monitoring their level of reliability.

[POLICY REVIEW]

The application of this policy will be regularly monitored and, if necessary, integrated in the event of significant changes in cyber threats or regulatory requirements. The Management is therefore committed to continuously improving its Cybersecurity posture, to protect its resources, consolidate the trust of stakeholders and contribute to the development, security and progress of the company.