ANNEX 2 - CORPORATE POLICY

The **CORPORATE POLICY** requires that, in line with the corporate mission, all business processes be managed in accordance with the rules governing the application of the Management System under **ISO/IEC 27001:2022**.

PURPOSE AND OBJECTIVES

The management of **TECNOSYS ITALIA S.R.L.** has defined and communicated this Information Security Management Policy and is committed to keeping it in effect at all levels of the organisation.

The purpose of this policy is:

to safeguard and protect information within the scope of the company's activities against all threats, whether internal or external, intentional or accidental, in accordance with the provisions of ISO/IEC 27001 and the guidelines contained in ISO/IEC 27002, in their latest versions.

SCOPE

This policy applies equally to all bodies and levels of the Company.

Implementation of this policy is mandatory for all personnel and must be included in the terms governing agreements with any external party that may, in any capacity, be involved in processing information within the scope of the Management System (SGSD).

The company permits the communication and disclosure of information outside the organisation solely for the proper conduct of business activities, which must comply with applicable rules and mandatory requirements.

INFORMATION SECURITY POLICY

The information assets to be protected comprise all information managed through the services provided and held at all company premises.

The following must be ensured:

- **Confidentiality of information:** information must be accessible only to authorised persons.
- **Integrity of information:** the accuracy and completeness of information and the methods used to process it must be protected.
- **Availability of information:** authorised users must be able to access information and related assets when required.

Inadequate security levels may damage the company's image, lead to customer dissatisfaction, expose it to penalties for breaches of applicable regulations, and cause economic and financial losses.

An adequate level of security is also essential for sharing information.

The company identifies all security requirements through risk analysis, which provides an understanding of its information system's exposure to threats. Risk assessment enables the company to evaluate the potential consequences and damage arising from a failure to implement security measures for the information system, as well as the realistic likelihood of the identified threats materialising.

The results of this assessment determine the actions needed to manage the identified risks and the most appropriate security measures.

The general principles of information security management cover several aspects:

- An inventory of company assets relevant to information management must be kept up to date, and an owner must be assigned to each asset. Information must be classified according to its criticality so that it is managed with consistent and appropriate levels of confidentiality and integrity.
- To ensure information security, all access to systems must be subject to an identification and authentication procedure. Information access rights must be differentiated according to each individual's role and duties, so that users can access only the information they need. These rights must be reviewed periodically.
- Procedures must be defined for the secure use of company assets, information and the systems used to manage them.
- Full awareness of information security issues must be encouraged among all personnel (employees and other staff), from recruitment and throughout the working relationship.
- To enable incidents to be handled promptly, everyone must report any security-related issue. Every incident must be managed in accordance with the procedures.
- Unauthorised access to company premises and individual rooms where information is managed must be prevented, and equipment security must be ensured.
- Contracts with third parties must ensure compliance with legal requirements and information security principles.
- A continuity plan must be prepared to enable the company to respond effectively to an unforeseen event, ensuring that critical services are restored within timeframes and in a manner that limit adverse effects on the corporate mission.
- Security aspects must be included in every stage of the design, development, operation, maintenance, support and decommissioning of IT systems and services.
- Compliance with laws, statutes, regulations, contractual obligations and all information security requirements must be ensured, minimising the risk of legal or administrative penalties, significant losses or reputational damage.

RESPONSIBILITY FOR COMPLIANCE AND IMPLEMENTATION

Responsibility for complying with and implementing the policies lies with:

1. All personnel who work with the company in any capacity and are in any way involved in processing data and information within the scope of the Management System.

All personnel are also responsible for reporting any irregularities and breaches of which they become aware.

2. All external parties that have dealings with and work with the company. They must ensure compliance with the requirements of this policy.

The Management System Manager must, within the framework of the Management System and through appropriate rules and procedures:

- conduct risk analysis using appropriate methodologies and adopt all measures needed to manage risk;
- establish all rules necessary for the secure conduct of all company activities;
- investigate security breaches, take the necessary countermeasures, and monitor the company's exposure to major threats and risks;
- organise training and promote personnel awareness of all matters relating to information security;
- periodically verify the effectiveness and efficiency of the Management System.

Anyone, including employees, consultants and/or external contractors of the Company, who intentionally or negligently fails to comply with the established security rules and thereby causes damage to the company may be subject to legal action through the appropriate channels, in full compliance with legal and contractual constraints.

REVIEW

Management will verify the effectiveness and efficiency of the Management System periodically and regularly, or whenever significant changes occur, to ensure adequate support for the introduction of all necessary improvements and to promote a continuous process that maintains oversight of the policy and adapts it to changes in the company environment, business and legal conditions.

The Management System Manager is responsible for reviewing the policy.

The review must verify the status of preventive and corrective actions and compliance with the policy.

It must take account of all changes that may affect the company's approach to information security management, including organisational changes, the technical environment, resource availability, legal, regulatory or contractual conditions, and the results of previous reviews.

The outcome of the review must include all decisions and actions relating to improvements in the company's approach to information security management.

MANAGEMENT COMMITMENT

Management actively supports information security within the company through clear direction, demonstrable commitment, explicit assignments and recognition of information security responsibilities.

Management's commitment is implemented through an organisational structure whose duties are to:

- ensure that all information security objectives are identified and meet business requirements;
- establish company roles and responsibilities for developing and maintaining the SGSD;
- provide sufficient resources for planning, implementing, organising, monitoring, reviewing, managing and continually improving the SGSD;
- ensure that the SGSD is integrated into all business processes and that procedures and controls are developed effectively;
- approve and support all initiatives aimed at improving information security;
- implement programmes to promote information security awareness and culture.

Place, 13 January 2024

DGE _____