Data Security Management System (DSMS)

ANNEX 2 – COMPANY POLICY

The **Company policy** requires that, in line with the company mission, the management of all company processes be set up in accordance with the rules governing the application of the management system in accordance with **ISO/IEC 27001:2022.**

PURPOSE

The management of SINTE SRL has defined, disclosed, and undertakes to maintain this Information Security Management policy at all levels of its organization.

The purpose of this policy is to ensure the protection and safeguarding of information from all threats, whether internal or external, intentional or accidental, within the scope of its activities, in accordance with the guidelines provided by the ISO/IEC 27001 standard and the guidelines contained in the ISO/IEC 27002 standard in their latest versions.

APPLICABILITY

This policy applies to all departments and levels of the Company.

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

The company allows the communication and dissemination of information to external parties only for the proper conduct of business activities, which must take place in compliance with applicable rules and regulations.

INFORMATION SECURITY POLICY

The information assets to be protected consist of all the information managed through the services provided and located in all company offices.

It is necessary to ensure:

- the confidentiality of information: i.e., information must only be accessible to authorized persons;
- the integrity of information: i.e., protecting the accuracy and completeness of information and the methods used to process it;
- the availability of information: i.e., that authorized users can actually access the information and related assets when they request it.

The lack of adequate security levels can damage the company's image, lead to customer dissatisfaction, and result in penalties for violating current regulations, as well as economic and financial damage.

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

The company identifies all security needs through risk analysis, which allows it to gain awareness of the level of exposure to threats to its information system. Risk assessment allows the company to evaluate the potential consequences and damage that may result from the failure to apply security measures to the information system and the realistic probability of the identified threats being carried out.

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

The general principles of information security management cover various aspects:

▪ There must be a constantly updated list of company assets relevant to information management, and a person responsible must be identified for each asset. Information must be classified according to its level of criticality so that it can be 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. Authorizations to access information must be differentiated according to the role and duties of each individual, so that each user can access only the information they need, and must be reviewed periodically.

▪ Procedures must be defined for the secure use of company assets and information and their management systems.

▪ Full awareness of information security issues must be encouraged among all staff (employees and collaborators) from the moment of selection and throughout the duration of the employment relationship.

▪ In order to manage incidents in a timely manner, everyone must report any security-related issues. All incidents must be handled as outlined in the procedures.

▪ Unauthorized access to company premises and individual rooms where information is handled must be prevented, and the security of equipment must be ensured.

▪ Compliance with legal requirements and principles related to information security in contracts with third parties must be ensured.

▪ A continuity plan must be in place to enable the company to deal effectively with an unforeseen event, ensuring that critical services are restored in a timely manner and in a way that limits the negative impact on the company's mission.

▪ Security aspects must be included in all phases of the design, development, operation, maintenance, support, and decommissioning of IT systems and services.

- Compliance with legal provisions, statutes, regulations, contractual obligations, and all requirements relating to information security must be guaranteed, minimizing the risk of legal or administrative penalties, significant losses, or damage to reputation.

RESPONSIBILITY FOR COMPLIANCE AND IMPLEMENTATION

Compliance with and implementation of the policies are responsibility of:

1- All personnel who, in any capacity, collaborate with the company and are in any way involved in the processing of data and information that fall within the scope of the Management System.

All personnel are also responsible for reporting any anomalies and violations of which they become aware.

2- All external parties who have relations and collaborate with the company, who must ensure compliance with the requirements contained in this policy.

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

- Perform risk analysis using appropriate methodologies and adopt all measures necessary for risk management
- Establish all rules necessary for the safe conduct of all company activities
- Verify security breaches and adopt the necessary countermeasures, and monitor the company's exposure to major threats and risks
- Organize training and promote staff 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 collaborators of the Company, who intentionally or as a result of negligence fails to comply with the established safety rules and thereby causes damage to the company, may be prosecuted in the appropriate forums and in full compliance with legal and contractual obligations.

REVIEW

Management will periodically and regularly, or in conjunction with significant changes, verify the effectiveness and efficiency of the Management System in order to ensure adequate support for the introduction of all necessary improvements and to promote the activation of a continuous process whereby the policy is monitored and adapted in response to changes in the corporate environment, business, and legal conditions.

The Management System Manager is responsible for reviewing the policy.

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

It shall take into account any changes that may affect the company's approach to information security management, including organizational changes, the technical environment, the availability of resources, legal, regulatory, or contractual conditions, and the results of previous reviews.

The outcome of the review shall include all decisions and actions to improve the company's approach to information security management.

MANAGEMENT COMMITMENT

Management actively supports information security within the company through clear guidance, visible commitment, clear assignments, and recognition of responsibilities related to information security.

Management's commitment is implemented through a structure whose tasks are:

- to ensure that all information security objectives are identified and that they meet company requirements;
- to establish company roles and responsibilities for the development and maintenance of the DSMS;
- providing sufficient resources for the planning, implementation, organization, control, review, management, and continuous improvement of the DSMS;
- ensuring that the DSMS is integrated into all company processes and that procedures and controls are developed effectively;
- approving and supporting all initiatives aimed at improving information security;
- implementing programs to spread awareness and a culture of information security.

Milan, li 07/08/2025

DGE