ANNEX 2 - COMPANY POLICY

The **Company Policy** requires that, in line with the company mission, the management of all company processes be set up with the rules specific to the application of the Management System according to the **ISO/IEC 27001:2022 standard** , integrated with the specific controls for the security of cloud services of the **ISO/IEC 27017** and **ISO/IEC 27018 standards** and the quality management principles of the **ISO 9001 standard** , from an integrated management system perspective.

PURPOSE AND OBJECTIVES

The management of **SINTE SRL** has defined, disclosed, and is committed to maintain this Information Security Management Policy at all levels of its organization.

The purpose of this policy is to ensure the protection and security of information from all threats, internal or external, intentional or accidental, within the scope of its activities, in accordance with the indications provided by the ISO/IEC 27001 standard and the guidelines contained in the ISO/IEC 27002 standard, as well as with the additional controls for the security of cloud services (ISO/IEC 27017) and for the protection of personal data (PII) processed in a cloud environment (ISO/IEC 27018), in their latest versions. Management is also integrated with the quality management principles of the ISO 9001 standard, to ensure customer focus, a process-based approach, and continuous improvement of the Management System.

SCOPE OF APPLICATION

This policy applies without distinction to all departments and levels of the Company.

The implementation of this policy is mandatory for all staff and must be included in the regulation of agreements with any external party who, in any capacity, may be involved with the processing of information that falls within the scope of the Management System (SGSD), including cloud service providers and their sub-suppliers.

The company permits the communication and dissemination of information externally only for the proper performance of company activities, which must be carried out 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 across all the company's offices and cloud services.

It is necessary to ensure:

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

Lack of adequate security can lead to damage to the company's image, lack of customer satisfaction, the risk of incurring penalties for violating current regulations, as well as economic and financial damage.

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

The company identifies all security needs through a risk analysis, which allows it to gain awareness of the level of threat exposure to its information system, including the specific risks arising from the use of cloud services. The risk assessment allows us to evaluate the potential consequences and damage that could result from not applying security measures to the information system and the realistic probability of the identified threats being implemented.

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 various aspects:

- A constantly updated catalog of company assets relevant to information management must exist, and a responsible person must be identified for each. Information must be classified according to its criticality level so that it can be managed with consistent and appropriate levels of confidentiality and integrity.
- To ensure information security, all system access must be subject to an identification and authentication procedure. Information access authorizations must be differentiated based on the role and responsibilities of each individual, so that each user can access only the information they need. These authorizations must be periodically reviewed.
- Procedures must be established for the safe use of company assets and information and their management systems.
- Full awareness of information security issues must be encouraged among all personnel (employees and collaborators) from the moment of selection and throughout the duration of the employment relationship.
- To ensure timely incident management, everyone must report any safety concerns. Each incident must be handled as outlined in the procedures.
- Unauthorized access to company offices and individual premises where information is managed must be prevented, and equipment security must be ensured.
- Compliance with legal requirements and information security principles must be ensured in contracts with third parties.
- A business continuity plan must be developed to enable the company to effectively address an unforeseen event, ensuring the restoration of critical services in a timely manner and in a manner that limits the negative impact on the company's mission.
- Security aspects must be included in all phases of design, development, operation, maintenance, support and decommissioning of IT systems and services.
- Compliance with legal provisions, statutes, regulations, or contractual obligations and any information security requirements must be ensured, minimizing the risk of legal or administrative sanctions, significant losses, or damage to reputation.

CLOUD SERVICES SECURITY (ISO/IEC 27017 AND ISO/IEC 27018)

In relation to the use and provision of cloud services, the company adopts specific controls, in accordance with the ISO/IEC 27017 and ISO/IEC 27018 standards:

- security responsibilities between the company (as a cloud customer) and the service provider (cloud service provider) must be clearly defined and formalized, according to the shared responsibility model;

- segregation and isolation of virtual environments and data of different customers in shared cloud infrastructures must be guaranteed;
- Administrative and privileged access to cloud services must be managed, monitored, and tracked, with particular attention to administrator operations;
- The correct removal or return of data at the end of the cloud service contract must be ensured, avoiding unauthorized recovery of information;
- the geographic location and jurisdiction in which the data, including personal data (PII), is processed and stored must be known and documented;
- The processing of personal data in the cloud must be limited to the purposes agreed with the customer, ensuring transparency, the management of data subject requests, and timely notification in the event of a data breach;
- Adequate monitoring, logging, and event management tools for cloud services must be activated.

QUALITY AND CONTINUOUS IMPROVEMENT (ISO 9001)

In accordance with the quality management principles of the ISO 9001 standard, the company adopts an integrated management system aimed at:

- customer orientation, ensuring that customer requirements and applicable statutory and regulatory requirements are understood and consistently met;
- a process approach, where activities are managed as interrelated processes that contribute to the achievement of business objectives;
- continuous performance improvement, through the Plan-Do-Check-Act (PDCA) cycle and the analysis of data and indicators;
- a decision-making process based on objective evidence and on the assessment of risks and opportunities;
- the involvement and empowerment of staff at all levels of the organization.

COMPLIANCE AND IMPLEMENTATION RESPONSIBILITIES

Compliance and implementation of the policies are the responsibility of:

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

All staff are also responsible for reporting any anomalies or violations they become aware of.

2- All external parties who maintain relationships and collaborate with the company 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:

- conduct risk analysis using appropriate methodologies and adopt all risk management measures;
- establish all necessary rules for the safe conduct of all company activities;
- verify security breaches and take necessary countermeasures and control 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 negligently disregards established safety regulations and thereby causes damage to the company, may be prosecuted in the appropriate courts and in full compliance with legal and contractual obligations.

REVIEW

Management will periodically and regularly review the effectiveness and efficiency of the Management System, or whenever significant changes occur, to ensure adequate support for the introduction of all necessary improvements and to facilitate the implementation of an ongoing process to maintain control and adapt the policy 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 adherence to the policy.

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

The outcome of the review should include all decisions and actions related to improving the company's approach to information security and quality management.

MANAGEMENT COMMITMENT

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

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

- ensure that all information security and quality objectives are identified and that they meet business and customer requirements;
- establish corporate roles and responsibilities for the development and maintenance of the SDG;
- provide sufficient resources for the planning, implementation, organization, control, review, management and continuous improvement of the SDG;
- ensure that the SDG is integrated into all company processes and that procedures and controls are developed effectively;
- approve and support all initiatives aimed at improving information security and the quality of services;
- activate programs to spread awareness and information security culture.

Milan, 16/07/2026

DGE