Company Policy for Data Security

The COMPANY POLICY requires that, in line with the company mission, the management of all company processes is set up with the rules specific to the application of the Management System according to the ISO/IEC 27001:2017 standard.

Purpose and Objectives of the Company Policy

The management of Dilvio De Marco has defined, disclosed and is committed to keeping active at all levels of its organization this policy for the Management of Information Security.

The purpose of this policy is:

- to guarantee the protection and safeguarding from all threats, internal or external, intentional or accidental, of information within its activities in accordance with the indications provided by the ISO/IEC 27001 standard and the guidelines contained in the ISO/IEC 27002 standard in their latest versions.

Scope of Application

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

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

The company allows the communication and dissemination of information to the outside only for the correct performance of company activities that must take place in compliance with the rules and mandatory regulations.

Information Security Policy

The information assets to be protected are all the information managed through the services provided and located in all the company's offices, including those that may be established in the future.

It is necessary to ensure:

- The confidentiality of the information: that is, the information must be accessible only by those who are authorized.
- The integrity of the information: that is, protecting the accuracy and completeness of the information and the methods for its processing.
- The availability of the information: that is, that authorized users can actually access the information and related assets when they request it.

The lack of adequate levels of security can lead to damage to the company's image, lack of customer satisfaction, the risk of incurring sanctions related to the violation of current regulations as well as economic and financial damages.

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

The company identifies all security needs through risk analysis that allows it to acquire awareness of the level of exposure to threats of its information system. The risk assessment allows to evaluate the potential consequences and damages that may arise from the failure to apply security measures to the information system and what is the realistic probability of implementation of the identified threats.

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

The general principles of information security management cover various aspects:

□ There must be a constantly updated catalogue of company assets relevant for information management purposes and a person responsible for each must be identified. 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, each access to the systems must be subjected to an identification and authentication procedure. Access authorizations to information must be differentiated based on the role and duties of individuals, so that each user can access only the information they need, and must be periodically reviewed.

□ Procedures must be defined 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.

□ In order to manage incidents promptly, everyone must report any security problem. Each incident must be managed as indicated in the procedures.

□ Unauthorized access to the offices and individual company premises where information is managed must be prevented and the security of equipment must be guaranteed.

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

□ A continuity plan must be prepared that allows the company to effectively deal with an unforeseen event, ensuring the restoration of critical services in a time frame and in a manner that limits the negative consequences on the company mission.

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

□ Compliance with legal provisions, statutes, regulations or contractual obligations and any requirement relating to information security must be guaranteed, minimizing the risk of legal or administrative sanctions, significant losses or damage to reputation.

Responsibility for Compliance and Implementation

The 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 personnel are also responsible for reporting all anomalies and violations of which they may become aware.

2 All external parties who maintain relationships and collaborate with the company. They 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 with appropriate methodologies and adopt all measures for risk management

□ Establish all the rules necessary for the safe conduct of all business activities
□ Verify security violations and adopt the necessary countermeasures and control the company's exposure to the main threats and risks

□ Organize training and promote staff awareness for everything related to information security.

□ Periodically verify the effectiveness and efficiency of the Management System.

□ Anyone, employees, consultants and/or external collaborators of the Company, intentionally or attributable to negligence, disregards the established security rules and in this way causes damage to the company, may be prosecuted in the appropriate venues and in full compliance with legal and contractual constraints.

Review

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

The Head of the Management System 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 into account all changes that may influence 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 result of the review must include all decisions and actions relating to the improvement of the company's approach to information security management.

Management Commitment

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

Management commitment is implemented through a structure whose tasks are:

□ Ensure that all information security objectives are identified and that they meet business requirements;

□ Establish business 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;

□

□ Check that the SDG is integrated into all business processes and that procedures and controls are effectively developed;

□ Approve and support all initiatives aimed at improving information security;

□ Activate programs for the dissemination of awareness and culture of information security.

Airasca, 26/02/2024

DIREZIONE GENERALE