General Information Security Policy

Version 3rd: 30-03-2025

1. Purpose

The company aims to provide its services in accordance with the applicable legal and regulatory framework and its other contractual obligations, in a way that protects information from intentional or unintentional theft, destruction, or use in violation of laws and regulatory provisions.

The purpose of information security is to ensure the business continuity of the company and to minimize the risks threatening information, by avoiding security incidents and reducing their potential impact.

2. Scope of Application

The General Information Security Policy applies to all company personnel involved in the delivery of services, as well as to the equipment used and the facilities employed by the company in the execution of services, including any additional terms set forth in the relevant contracts.

3. Responsibilities

Management Responsibilities

The core responsibilities of Management in relation to Information Security Management within the company are:

- Formulation of the company's information security policy.
- Approval and review of Information Security Policies, as well as related Procedures and Work Instructions.
- Approval of Risk Management Plans and Business Continuity Plans (Emergency Management).
- Ensuring the necessary resources for the effective implementation of the Information Security Management System (ISMS) within the broader Management System.
- Establishing appropriate conditions within the company to promote understanding and awareness among personnel regarding their roles and responsibilities related to information security.
- Ensuring continuous improvement within the scope of the Management System.
- Making decisions to impose sanctions in cases of disciplinary violations related to information security.

Responsibilities of the ISMS Manager

The representative of Management on Information Security matters is the ISMS Manager, who is appointed by Management and, in addition to other duties, has the following responsibilities:

- Collaborating with Management on the development of Security Policies, procedures, and standardized methods, in accordance with the company's General Information Security Policy.
- Ensuring the implementation, maintenance, and monitoring of the Security Policies to ensure compliance with legal and regulatory requirements, current legislation, and relevant standards.
- Informing Management about the performance and improvement of Security Policies.
- Updating the company's information asset inventory and classifying the importance of these assets, in collaboration with relevant business stakeholders.
- Coordinating the Information Security Management Team to identify and assess risks to the company's information assets, in cooperation with relevant business stakeholders.
- Working with Management and the Information Security Management Team to determine the necessary controls to address risks.

- Monitoring and reporting to Management any security incidents and activating the corresponding plans and strategies to address and prevent recurrence.
- Monitoring the effectiveness of the controls implemented to mitigate risks and reporting findings to Management.
- Organizing and conducting Internal Audits to assess the effectiveness of the System.
- Communicating with external bodies regarding Information Security Management.
- Ensuring staff training on Information Security Management and the importance of their participation in the implementation of the System.
- Preparing and coordinating the Management Review of the Management System.

The ISMS Manager reports directly to Management on all Information Security matters and is authorized to act on its behalf regarding such matters.

Responsibilities of the Information Security Management Team

Members of the Information Security Management Team are:

- The ISMS Manager
- The Security Technician

The main responsibilities of the Information Security Management Team are:

- Reviewing the company's activities within the scope of the ISMS and identifying related information assets and associated risks.
- Assessing and evaluating the severity of identified risks.
- Proposing and documenting control measures to address the risks.
- Periodically reviewing the effectiveness of risk management plans.
- Identifying emergency situations and coordinating the development and approval of emergency response plans.
- Reviewing the effectiveness of emergency plans.

Responsibilities of Department Heads

The main responsibilities of Department Heads regarding Information Security Management are:

- Participating in the identification, assessment, and design of risk management plans related to the information assets managed by their department.
- Overseeing compliance with Security Policies by their department's staff.
- Actively participating in the review of security incidents to investigate causes and plan corrective actions.
- Identifying significant changes and trends that may affect information security practices within their area of responsibility, and cooperating with the ISMS Manager and Management to adapt to new conditions.

Responsibilities of Staff

The primary responsibilities of staff involved in the Management System, and specifically in Information Security Management, include:

- Implementing Security Policies, relevant procedures, and work instructions as applicable to their duties.
- Immediately reporting to the ISMS Manager any security incident they become aware of.

Description

The objective of this policy is to protect the company's and its clients' information assets from all internal, external, intentional, or unintentional threats. The specific objectives of the company concerning Information Security are:

- Ensuring information is protected from any unauthorized access.
- Ensuring information confidentiality.
- Maintaining the integrity of information.
- Maintaining the availability of information.
- Ensuring compliance with legal and regulatory requirements.
- Developing, maintaining, and testing Business Continuity Plans.
- Providing Information Security training for all personnel.

All actual or suspected security incidents must be reported to the ISMS Manager and be fully investigated.

To achieve the above objectives, individual Security Policies and Procedures have been developed and implemented. These define management's direction, the implementation method, and all related responsibilities of staff. All personnel and external partners (when required) are obliged to adhere to the Security Policies relevant to their activities.

Management is committed to providing all necessary resources and means for the implementation of this and all other Security Policies.

To document the implementation of the Information Security Management System under the company's Management System, the ISMS Manager is responsible for completing the "Statement of Applicability."

CEO / Managing Director