SECURITY POLICY

Information Security Management System

Kirey Group

Document History

Major Release	Action	Company Function	Date
1	Edited	CISO, PROCE	28/06/2022
	Checked	CISO, PROCE	28/06/2022
	Published	PROCE	28/06/2022

Change History

Major Release	Minor Release	Issue Date	Revision Reason
1	0	27/04/2021	First draft definition
1	1	29/04/2021	Document update and revision
1	2	08/06/2021	Review of the relevant legal entity
1	3	06/09/2021	Customization of the policy for Kirey S.r.l.
1	4	01/12/2021	Legal entity integration and update
1	5	28/06/2022	Update of the roles involved in drafting the document
1	6	09/05/2023	Update of the structure and change of document type in the Guidelines
1	7	07/01/2025	Addition of attachments PKG_CIS_AL15_External security measures and PKG_CIS_AL16_Internal security measures

SUMMARY

1. OBJECTIVE

The purpose of this document is to define the general information security principles to be followed for the implementation and maintenance of an efficient and secure Information Security Management System within the scope of Kirey Group's activities.
This document applies to Kirey Group's business lines, as specified in the *PKG_CIS_RE01_ISMS Perimeter* document.
The document is "public," intended for all stakeholders involved in Kirey Group's activities.

2. DEFINITIONS AND ACRONYMS

2.1. Definitions

The main reference terms and acronyms used in the document are indicated.

Term	Description
Confidentiality:	Ensures that information is accessible only by authorized personnel
Integrity:	Ensures that information is accurate and complete
Availability:	Ensures that information is accessible and usable, when needed, by authorized personnel

2.2. Acronyms

Acronym	Definition
ISMS	Information Security Management System
ISO	International Organization for Standardization
CISO	Chief Information Security Officer

3. SECURITY POLICY GUIDELINES

3.1. Security Policy

3.1.1. Introduction

The Information Security Management System is the tool with which Kirey Group intends to protect the confidentiality, integrity, and availability of its information assets. Achieving adequate levels of security allows us to mitigate and prevent losses and damage that could impact people, operations, the company's image and reputation, economic and financial aspects, and technologies, as well as ensuring compliance with applicable contractual and legislative frameworks regarding the protection of personal data and information.

To this end Kirey Group:

- adopts and implements recognized principles and best practices to ensure information security and promotes the acquisition of certifications of compliance with reference standards;
- identifies roles and responsibilities assigned to its staff, regardless of their hierarchical level, also involving third parties with key roles;

- Assigns the necessary resources to ensure the use of adequate information security measures, in the areas of organizational, physical, and information systems security, in the delivery of solution implementation processes, including application-based solutions, and in the management and maintenance of IT infrastructure;
- Continuously promotes the Management System, including through the ongoing commitment of senior management bodies and individuals;
- Identifies, documents, and enforces rules governing the use of information, assets, and tools, in order to meet current regulations and customer expectations, primarily from banking, financial, and public administration sectors, while taking into account the needs arising from relationships and dependencies with other Organizations' processes;
- Develops a security awareness program for staff, through periodic information and training sessions;
- Develops appropriate response and management measures in the event of incidents that may compromise information security and normal operations;
- is committed to carrying out a continuous process of improvement and evolution of the Management System, continuously planning, executing, verifying and implementing measures and precautions to counter events that could compromise the company's information assets.

3.1.2. Meaning and Objectives

Information security's primary objective is the protection of information, data, and the information system elements that manage them. Specifically, pursuing information security means defining, achieving, and maintaining at least the following properties:

- **Confidentiality.**
- **Integrity.**
- **Availability.**

The lack of commensurate levels of security, in terms of confidentiality, availability and integrity of information, may lead, in the context of any Kirey Group activity, to loss of reputation, customer disaffection, economic and financial damages, as well as criminal and administrative sanctions following violation of current legislation.

3.1.3. Security measures

To ensure information security and preserve the information of Kirey and its Customers, employees, suppliers, external parties and any person or entity that may impact such security must comply with the security requirements set out in the attachment PKG_CIS_AL15_External Security Measures and PKG_CIS_AL16_Internal Security Measures.

4. REFERENCES

The documents, regulations and standards used as a reference for the definition of this plan are indicated.

Reference documents
PKG_CIS_PR04_Business Continuity Management
PKG_CIS_PR02_Information Security Incident Management Procedure
PKG_HRE_AL07_Mansionary
PKG_CIS_RE01_ ISMS Perimeter
ISO/IEC 27001 - Information Security Management System – Requirements
ISO/IEC 27002 – Code of practice for Information Security Management
ISO/IEC 27005 – Information Security Risk Management
ISO 22301:2019 – Societal Security – Business Continuity Management System – Requirements
NIST – SP 800/53 - 2013 - Recommended security controls for federal information systems
ISO/IEC 20000:2018 – Information Technology Service Management
D.lgs. n. 196/2003 - Codice in materia di protezione dei dati personali e provvedimenti successivi
UE - Regolamento n. 679/2016 del Parlamento Europeo e del Consiglio
D.lgs. n. 231/2001 - Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica
D.lgs. n. 81/2008 - Tutela della salute e della sicurezza nei luoghi di lavoro
Legge n. 300/1970 – Statuto dei lavoratori

5. ATTACHMENTS

PKG_CIS_AL15_External Security Measures
PKG_CIS_AL16_Internal Security Measures