Attachment

Kirey Advisory Service Management Policy

Document History

Major Release	Action	Company Function	Date
1	Edited	COMP, PROCE	23/01/2025
	Checked	COMP	24/01/2025
	Published	PROCE	28/01/2025

Change History

Major Release	Minor Release	Issue Date	Revision Reason
1	0	28/01/2025	First Revision

1. Service Management Policy

As the management of Kirey Advisory S.r.l., we intend to protect information from a broad spectrum of threats to ensure the continuity of our operations, minimize risks, guarantee return on investments, business opportunities, legal compliance, and profitability. All data and related processing used to manage our operations must be protected to ensure they reach their intended users intact, that they are not lost, or, worse still, that they do not fall into the hands of competitors or profiteers.

Information is an asset, and like other tangible or intangible assets, it is essential to the Kirey Advisory organization; as such, it also needs to be protected. Protection is all the more necessary as the interconnectedness becomes greater, which exposes information to a wider variety of risks and vulnerabilities: fraud, espionage, vandalism, accidents.

We must all be aware of the problem and are committed to sharing the objectives and principles of information security. Kirey Advisory's organizational structure and existing processes have integrated an information security management system (ISMS), a system of operations and controls to manage information risk.

Specifically, with the implementation of this system:

- Risks are analyzed;
- Risks are managed based on risk acceptance criteria, without compromising compliance with state laws and contractual requirements.
- Therefore:
    - We knowingly accept risks if they meet those criteria;
    - We avoid risks by not permitting actions/activities that could cause them;
    - Or we transfer risks to third parties.
- We raise awareness of the need to operate responsibly through training at all levels;
- We introduce specific control activities and have taken precautions against disasters;
- We will take appropriate action whenever violations occur;
- This system includes:
    - Monitoring all events, verifying the effectiveness of the required controls and subsequent review;
    - Implementing improvement actions;
    - Managing system documentation and records;
    - Training all personnel to achieve competence and awareness of information security issues;
    - Internal audits to verify that controls are effective, control objectives are achieved, and procedures are being implemented: in short, that the SMS complies with the reference standard ISO/IEC 27001 and ISO/IEC 20000-1:2018;
    - Management Review;
    - Improvement through Corrective Actions and Improvement Plans.

Within this system, the following responsibilities are assigned:

- Management, to define the domain of assets to be protected;
- The SMS Manager, to assess the risks to which the various assets may be exposed;

- The SMS Manager, to establish, implement, and monitor controls;

- The ISMS Manager, to record all verified threats and plan and implement new controls;
- Each employee, to comply with the required authorizations and report any threats encountered to the ISMS Manager;
  Management, to periodically review the information security status and the effectiveness of this policy;
- The ISMS Manager, to undertake improvement actions.