elepro projects

Information Security Policy

Information Security Policy

Version	Date	Update description	Author
1.0	24.07.2025	First version	Andrea Tarlarini

1 Information Security Policy

Elepro Projects S.r.l. (hereinafter referred to as "the Company") considers the protection of the Confidentiality, Integrity, and Availability of its corporate information assets and the data managed through its infrastructure to be an essential prerequisite for the Company's competitiveness and reputation.

To implement its information security policy, Elepro Projects S.r.l. has developed and is committed to maintaining an information security management system compliant with the requirements of UNI CEI EN ISO/IEC 27001:2022 and applicable mandatory regulations, as a means of managing information security within its operations — including Regulation (EU) 2016/679 (GDPR) and IEC 62443, which governs the protection of automation and control systems.

In this context, Elepro Projects S.r.l. adopts a strategic approach to information security as a structured and integrated system of technical, organizational, procedural, and behavioral measures, in which all responsibilities related to information security are clearly defined and assigned. This is aimed at preventing, addressing, and overcoming any action or event that could cause actual or potential harm to the Availability, Integrity, or Confidentiality of information.

This strategy is based on a holistic approach to security, taking into account:

● the polymorphic nature of threats, which often combine physical, logical, and behavioral tools and techniques in an interconnected and concurrent manner;

● the various states of information that must be protected, as it may simultaneously exist as a paper document, a digital file, a telephone conversation, or a meeting discussion.

The Company is committed to ensuring information security for its clients, stakeholders, and shareholders by implementing processes that guarantee full protection of:

- **Confidentiality**: ensuring that access to and handling of information is restricted to authorized individuals, entities, or processes, based on their authorization level;
- **Integrity**: protecting information from unauthorized, accidental, or intentional changes, alterations, or destruction;
- **Availability**: ensuring that information is accessible to authorized users whenever it is needed;
- **Control**: ensuring that data is always managed through secure and tested processes and tools;
- **Privacy**: ensuring the protection and control of personal data.

The Information Security Policy is based on the following principles:

- ensuring maximum protection against risks, aimed at enhancing the Company's assets, operations, technologies, and knowledge over the long term, as well as supporting value creation for all stakeholders;

- applying to every process and resource, internal or external, that is relevant to the governance and management of security for all assets — not only IT resources;

- adopting a holistic approach that integrates the various components required to mitigate risk within a unified framework, including:

  o corporate policies, standards, and industry best practices;

- o processes and organizational structures;
- o culture, ethics, and individual behavior;
- o information;
- o services, infrastructures, and applications;
- o people, skills, and competencies;

- ensuring clear segregation of duties, separating the responsibilities for security governance and security management, which involve different types of activities and require a variety of organizational units to meet security objectives.

2 Objectives of the Information Security Policy

The Information Security Policy aims to:

Support Elepro Projects S.r.l. through:

- the integration of security from the design phase;
- compliance with internal and external regulations;
- timely and accurate information on security;
- continuous improvement of security measures.

Defend the Company through:

- a risk-based approach;
- protection of information based on its classification;
- management of security incidents;
- ongoing evaluation of security threats.

Promote security awareness within Elepro Projects S.r.l. through:

- a professional and ethical approach to security management;
- continuous technical training of staff responsible for security,

ensuring the highest standards in the management of corporate protection systems;
- the dissemination of a strong security culture among all stakeholders.

This Policy applies to the entire organization of Elepro Projects S.r.l. and requires employees, shareholders, and relevant third parties to provide the necessary support in achieving the defined objectives. Therefore, all individuals are expected to comply with the information security requirements and report any weaknesses in the protection system.

The Company is also committed to promoting awareness and dissemination of this Information Security Policy to all stakeholders.

3 Monitoring and Review

Elepro Projects S.r.l. continuously monitors and assesses the achieved level of information security and the effectiveness of its management system, with the goal of continuous improvement. This includes obtaining and maintaining certifications according to the most advanced international standards (particularly ISO/IEC 27001), to reinforce the Company's efficiency, quality, and reliability in delivering services and securely protecting data.

The Information Security Policy is regularly updated and reviewed annually, or whenever necessary, to ensure its continual improvement. It is shared within the organization and made available to clients, stakeholders, shareholders, and third parties.

elepro projects