

Information Security Policy

This policy aims to protect the information of ENOMIX from internal and external threats, ensuring the confidentiality, integrity, and availability of data, both for its clients and its business operations.

The policy applies to all employees, partners, and external suppliers who have access to ENOMIX' information systems, data, and infrastructure.

ENOMIX is committed to the following core information security principles:

- Confidentiality: We ensure that our clients' data and our business information are accessible only to authorized individuals.
- Integrity: We maintain the accuracy and completeness of information, preventing any unauthorized changes.
- Availability: We ensure that information and systems are accessible to users when they need them.

ENOMIX implements a continuous risk management process that includes regular identification and assessment of threats to information security, particularly concerning the design and development of information technology services for networks and systems.

ENOMIX' employees have the following responsibilities:

- To follow the information security procedures.
- To immediately report any security incident or suspicious activity.
- To participate in regular training on information security.

This policy fully complies with the ISO 27001:2022 standard, as well as all relevant regulations such as the General Data Protection Regulation (GDPR) and other data security laws.

The information security policy will be reviewed annually or whenever significant changes occur in ENOMIX' business operations, with the aim of continuously improving the Information Security Management System (ISMS).

The company ensures that all employees are properly trained in security procedures through regular updates and training programs on information security threats.

This policy has been approved by ENOMIX' management and will be communicated to all employees and partners for immediate compliance and implementation.

Management Team