REWORTH

Version 1.0
Publication Date: April 2023
Classification: Public
ID:SL5.2

INFORMATION SECURITY POLICY

REWORTH recognizes the importance of the data of all our clients, consequently the privacy and security of Information are a business priority, which leads us to work every day to guarantee that our digital platforms and our services maintain high levels of security to become a long-term business ally for all our clients.

This Information Security Policy defines the basis for all guidelines and measures to be considered to manage information security risks on information assets, processes, and to ensure the security of information over all technology services and business activities.

REWORTH has the firm commitment to implement an Information Security Management System, putting the needs and expectations of all our interested parties, this allows us to guarantee that our technology complies with the following principles and objectives:

Principles

Confidentiality: All data in the digital environment of **REWORTH** is protected from unauthorized persons.
Integrity: REWORTH guarantees that all data is complete, accurate and valid, preventing any type of manipulation.
Availability: REWORTH maintains a persistent digital environment in the event of any incident or contingency scenario with the sole objective of not affecting customers.

Objectives

1) Give treatment to 100% of the critical risks present in the business environment
2) Continuously increase our SecOps resilience capabilities
3) Guarantee the protection of critical assets where they are located
4) Establish and maintain a culture of information security

Leadership and Commitment

REWORTH´s Information security policy demonstrates top management’s commitment to information security and the ISMS. This commitment extends to all objectives, processes and controls defined within the scope of the ISMS.

The Senior Management Team is responsible for developing, implementing, and managing the ISMS and that the system is understood and complied with at all levels of the organization ensuring that:

- A policy for information security is established.
- The ISMS is integrated into the organization’s processes.
- Resources are provided to establish, implement, operate, monitor, review, maintain and improve the ISMS.
- The ISMS achieves its intended outcome(s).
- Objectives and plans for the ISMS have been established.
- Responsibilities for specific processes are clearly defined throughout the ISMS and are documented in individual job descriptions or otherwise where necessary.
- The importance of meeting objectives and conforming to the policy, its responsibilities under the law and the need for continual improvement is communicated to the organization.
- Continual improvement is promoted.
- An acceptable level of risk has been decided for accepting risks.
- Internal ISMS audits are conducted.
- Management reviews the ISMS including the policy are conducted

Appropriate records of the above activities are retained.

Note: This Policy will be communicated to all internal and external interested parties within the scope of the ISMS for their consultation and will review every year.