Grenergy
renovables

INFORMATION SECURITY POLICY

JUNE 2023

INDEX

1. OBJECTIVE

The objective of this policy is to establish the basic principles and general framework for the control and management of Information Security risks to which Grenergy is exposed.

Grenergy's Information Security framework contains the rules and regulations that establish the organizational, procedural and technical requirements to protect Grenergy's information assets and products, solutions and services against internal and external threats.

2. SCOPE

This document applies to all GRENERGY employees, as well as to all Group companies, including investee companies in which it has effective control or the possibility of such control.

It is the responsibility of the above-mentioned individuals and legal entities, regardless of their function within the Group organization(s) to which they belong, to know, respect and comply with this document.

The group's internal regulations are part of the employee's contractual obligations and therefore any failure to comply with them will lead to the appropriate disciplinary sanctions.

3. INFORMATION SECURITY POLICY

3.1.- Information Security

Often only tangible assets such as furniture, machinery, servers, etc. are considered as company assets. However, there are also intangible assets such as customer portfolio, tariffs, commercial knowledge, intellectual property or reputation, among others. **All these elements are part of the information of our company and constitute one of the most important assets of our organization and therefore must be protected.**

Information security is a more general term that covers both the digital (cybersecurity) and physical domains. They are similar concepts but information security is broader and includes cybersecurity.

3.2.- Basic Principles for Information Security

1. Protect the company's critical information and technology assets from potential cybersecurity and physical threats.
2. Raise awareness of security risks among all employees and ensure that they have the necessary training and technological skills to protect the security of the group's information systems.

3. Develop the implementation of adequate security mechanisms following an approach based on the company's specific risks.
4. Promote prevention, detection, reaction, analysis, recovery, response, investigation and coordination capabilities that allow for an agile response to potential threats.
5. Maintain a process of continuous review and improvement of the security management model to keep it up to date with the changing conditions of the technological environment and new threats.
6. Ensure approved regulatory compliance related to information security.

3.3.- Information Security Risks

It is necessary to establish controls that allow us to prevent and mitigate Information Security risks as far as possible. The following is an illustrative classification of the most common information security risks.

Digital risks

Digital risk refers to all unexpected consequences arising from digital systems. Some examples where digital risks can materialize are:

- Risk of cyber-attacks, Malware, phishing, denial of service attacks or ransomware are some of the methods cybercriminals use to try to gain access to a system and use it against the company's interests.
- Lack of digital skills and awareness of the subject.
- Compatibility problems between IT systems and risks arising from failure to update them.
- Adoption risks during the implementation of a new technology, such as loss of information.
- Risks arising from poor data quality, such as errors and poor decision making based on inaccurate information.
- Data privacy risks managed by the company (databases, website cookies, etc.).

Physical risks

These are risks that refer to undesired consequences that may impact physical equipment or its misuse.

- Irregularities in access control: Manipulation of security guards, access control and/or biometric controls
- Device failures caused by deterioration or age of systems that can make information inaccessible, unreliable or even cause a total system crash.
- Deterioration or destruction of assets with sensitive information due to inappropriate use.
- Theft and loss of corporate assets with confidential information.

- Natural disasters such as earthquakes, floods or hurricanes. Especially relevant in areas prone to these types of disasters.

3.4.- Organizational Model

3.4.1 Management Commitment

Grenergy's management, aware of the importance of information security, is committed to:

- Promote the dissemination and awareness of the Information Security Policy among the group's employees.
- Provide adequate resources to achieve information security objectives.
- Consider information security risks in decision making.

3.4.2 Grenergy's Information Security Committee

Grenergy decided to create a security committee whose main objective is to ensure that all employees are aware of and comply with the cybersecurity policy and internal rules that develop it.

The Information Security Committee will consist of the CHRO, Grenergy's IT & Digital Manager and the Compliance Manager.

The Committee should be an adaptable body with a practical focus, so if all members agree, additional members may be included to complement the Committee's knowledge and capabilities. The Committee may also rely on the advice of external experts to ensure its proper and effective functioning.

3.4.3 Risk management

A) Risk assessment and identification

At Grenergy, the Information Security Committee will identify and assess risks related to information security, issuing an annual report or when necessary at the request of the Management Bodies.

Identification and evaluation will be performed:

- Regularly, once a year.
- When there are significant changes in the structure and Information Systems (IT).
- When a serious security incident occurs.

B) Risk management

Once the risks have been identified and evaluated, the Safety Committee will establish the appropriate measures to mitigate them to the extent necessary, so that the residual risk values are considered acceptable values.

4. RESERVATION CLAUSE

GRENERGY expressly reserves the right to unilaterally modify, update and/or eliminate any matter regulated in this policy/regulation/procedure.

5. MAJOR CHANGES COMPARED TO THE LAST REVISION

Version:	Description of change
1.0	Initial version