SECURITY POLICY

Updated on October 16th, 2025.

NEOENERGIA S.A.'s (the "**Company**") Board of Directors has the power to prepare, evaluate and consistently review the Company's Governance and Sustainability System, as well as approve and update policies that contain guidelines that govern the Company's performance. They may also provide notice of, as applicable, the policies that, during the exercise of their autonomy, they decide to approve at companies that are part of the group where the dominant entity is, as established by law, the Company (the "**Group**").

In the exercise of these powers and in order to establish the principles that will govern its actions in matters involving corporate security, the Board of Directors hereby approves, in compliance with the Neoenergia Group's Corporate Purpose and Values of the , this Security Policy (the "**Policy**"). This Policy will respect, develop and adapt the Group's Core Ethical Principles of Governance and Sustainability.

Through this Policy, the Company expresses its commitment to guaranteeing excellence in security-related matters, which plays a leading role in the daily lives of the Group's companies. These commitments will ensure that they remain safe, resilient and reliable in a digital community under continuous transformation, where new and increasingly sophisticated threats arise, both of a physical and cybersecurity or hybrid nature. These threats increase the level of demands from regulators, customers, other Interest Groups with which the Group's companies maintaining relationships while respecting compliance with an increasingly high level of security. This will allows lasting and trusting relationships to be built and consolidated.

1. Scope

This Policy is applicable to the Company. Nevertheless, this Policy describes the actions and regulatory developments that must be carried out within the scope of this Policy by the other companies of the Group while observing their competencies and their autonomy.
These principles must also inform, when applicable, the performance of the Neoenergia Institute, which is linked to the Group.

The Company will promote the alignment of the regulations of the companies in which it holds an ownership interest, but which are not part of the Group, as well as joint ventures, temporary associations and other entities it manages, with the principles contained in this Policy.

2. Purpose

The purpose of this Policy is to establish the principles of action that must govern the Company's security practices to ensure the effective protection of individuals, physical assets (including critical infrastructure), information, knowledge and control systems and communications, as well as the confidentiality of the data processed at all times through means of security initiatives. Such actions must fully comply with the law and scrupulously fulfill the the provisions of the Company's Policy for the Respect of Human Rights.

3. Principles of action

The Company adopts and promotes the following principles of action, which must guide its activities with regards to security-related matters:

a) Ensure the protection of employees of the Group's companies, both in their place of work and during travel for professional reasons, as well as the protection of persons on the Company’s premises or at any institutional event.

b) Ensure the adequate protection of physical and cyberassets to proactively manage risks at all stages of their life cycle, ensuring that they are given an appropriate level of security, cybersecurity and resilience. The most advanced standards must be applied to assets that support the operation of critical infrastructure in accordance with the Neoenergia Group's General Corporate Risk Management Bases and Cybersecurity Risk Guidelines and Limits approved by the Board of Directors.

c) Define a safety management model with clear assignment of roles, responsibilities and effective coordination mechanisms, which must integrate safety and proactive risk management into decision-making processes.

d) Promote the identification of non-public information considered (or likely to be considered) a business secret, as well as information in which unauthorized disclosure or alteration may cause serious harm to the interests of the Company.

e) Define criteria for the adequate protection of information and knowledge, as well as control, information and communications systems and supervise and guarantee their implementation.

f) Promote the active combating of fraud and attacks on the brand, image and reputation of the Company and its employees.

g) Guarantee the right to the protection of the personal data belonging to individuals with whom the Company maintains relationships in accordance with the provisions of the Personal Data Protection Policy.

h) Adopt the necessary measures to prevent, mitigate, minimize or restore the damage caused by security threats, whether physical, cybersecurity or hybrid in nature, for the proper execution of business activities based on proportionality criteria for potential risks and the criticality and value of the affected assets and services.

i) Comply with the principles of action established in the Operational Resilience Policy.

j) Foster an inclusive culture and awareness of security both internally and externally, among third parties and employees by carrying out appropriate dissemination, awareness and training initiatives adapted to each audience at a sufficient frequency to ensure that they have the necessary knowledge, skills, experience and capacities.

k) Provide adequate safety training for all internal and external personnel defining requirements and criteria during hiring that consider such training.

l) Promote the integration of security-related themes in the management of the Company's projects that may imply a specific potential safety risk in order to ensure the proper identification and treatment of this risk starting with the design and initial phases of the project, as well as the establishment of the necessary controls during its effectiveness.

m) Promote the secure use of assets that will strengthen detection, prevention, defense, response and recovery capabilities in the face of attacks or security incidents and ensure their effectiveness while paying special attention to cybersecurity threats.

n) Monitor the current context surrounding the organization and the environment, as well as the development of events that will allow for the identification of the most relevant security threats in order to anticipate their potential impact.

o) Promote best practices and innovation in the field of security.

p) Collaborate with Stakeholders involved (including, among others, the supply chain and customers) in security-related risks affecting the Company, to strengthen the coordinated response to potential security risks and threats .

4. Group-level coordination

With regards to the specific scope of action at each company, the Security and Resilience Directorate (or the management body that may come to assume its competencies), through the Security, Resilience and Digital Technologies Committee (or the committee that comes to assume its competencies), will act in coordination with the persons responsible at Group companies in order to ensure an adequate consolidated level of maturity and risks in terms of security at the Group level.

Additionally, the Security and Resilience Directorate (or the management body that may come to assume its competencies), through the Security, Resilience and Digital Technologies Committee (or the committee that may come to assume its competencies), will identify, implement and evaluate the necessary actions for the preparation and supervision of a strategic security Program in accordance with the principles and guidelines defined in this Policy,. The Directorate will develop the internal standards, methodologies and procedures to ensure their adequate implementation.

5. Implementation and monitoring

As part of the implementation and monitoring of the provisions of this Policy, the Board of Directors relies on the Security and Resilience Department (or the department that may come to assume its powers), which will develop the necessary procedures.

* * *

This Policy was initially approved by the Board of Directors on July 19, 2018 and last reviewed and updated at the Board of Directors' Meeting held on October 16th, 2025.