Corporate Security Policy

Updated May 29th, 2024

The Board of Directors of NEOENERGIA S.A. (the "**Society**") is vested with the powers to prepare, assess and review the Society's Governance and Sustainability System on an on-going basis and, specifically, to approve and update, the corporate policies, which contain the guidelines governing the conduct of the Society and of the societies that comprise the Group, for which the Society is the controlling entity, within the meaning established by law (the "**Group**").

In the exercise of its powers and aiming to establish the general principles that shall govern its actions in matters of corporate security, the Board of Directors approves, in compliance with the Purpose and Values of the Neoenergia Group, this *Corporate Security Policy (the "**Policy**").*

1. Purpose

The purpose of this *Policy* is to establish the main principles of conduct that shall govern in matters of security, within the perimeter of the Group's companies in matters of security to ensure the effective protection of people, hardware (including critical infrastructure), information, knowledge and control and communications systems,, as well as the privacy of the processed data, at all times, by security actions, so that they are fully in accordance with the law and scrupulously comply with the provisions of the Society's Human Rights Respect Policy.

Through this policy, the Company manifests its commitment to excellence in security matters, which plays a leading role in the daily lives of the Group's societies, so that they remain safe, resilient and reliable in a digital community in continuous transformation, where new increasingly sophisticated threats emerge, whether physical, cybersecurity or hybrid, which causes an increase in the level of demand from regulators, customers, other Interest Groups with which the Group's societies interact, respecting compliance with increasingly high level of security, which allows building and consolidating lasting and trusting relationships.

2. Scope of application

This Policy is applicable to the Society and other companies that are part of the Group and to subsidiaries that are not part of the Group, over which the Society has management influence, within the legally established limits.

For investees to which this Policy is not applicable, the Society shall promote, through its representatives on the management bodies, the alignment of their own policies with those of the Society.

Furthermore, this Policy shall also apply, as applicable, to the joint ventures, temporary joint ventures, and other equivalent associations, when the Society is responsible for their management.

This *Policy* is developed and complemented through the following specific policies approved by the Company's Board of Directors: The Personal Data Protection Policy and the Cybersecurity Risk Policy, which respect the aforementioned matters.

3. Basic principles of conduct

To materialize the commitment indicated in its “Purpose”, the following basic principles of conduct have been established that must govern the activities of the Group’s societies in matters of corporate security:

a) Design a preventive security strategy, with both a preventive and proactive approach to guarantee a reasonable level of risk.

b) Ensure adequate protection of assets (including critical infrastructures), to proactively manage risks.

c) Ensure the protection of professionals from the Group's societies, both in their workplace and in their professional displacements, for professional reasons, as well as the protection of people when they are on the premises or at any institutional event of the Group's societies.

d) Define a security management model with a clear association of roles and responsibilities and effective coordination mechanisms, which integrates security and proactive risk management into decision-making processes.

e) Ensure proper protection for information and knowledge, as well as control, information technology and communication, to proactively manage risks in accordance with the provisions of the *Cybersecurity Risk Policy*;

f) Promote the identification of non-public information classified (or capable of being classified) as confidential or secret, as well as information considered (or capable of being considered) as commercial secrets and define the criteria for their adequate protection, ensuring their implementation.

g) Promote the active fight against fraud and attacks on the brand, image and reputation of the Group's companies and its professionals.

h) Guarantee the right to protection of personal data of individuals who have relationships with companies that belong to the Group, in accordance with the provisions of the Personal Data Protection Policy.

i) Adopt the necessary measures to prevent, neutralize, minimize or restore the damage caused by security threats, whether physical, cybersecurity or hybrid, to

normalize the development of activities, based on criteria of proportionality to the potential risks and the criticality and value of affected assets and services.

j) Comply with the basic operating principles established in the *Operational Resilience Policy*.

k) Promote an inclusive culture and awareness in matters of security within the Group, by carrying out appropriate dissemination, awareness, and training actions, adapted to each recipient and with sufficient frequency to guarantee the updating of knowledge in this area.

l) Promote adequate security training for all personnel, both internal and external, defining requirements and criteria in hiring that take such training into account.

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

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

o) Collaborate with Stakeholder Groups involved (including the supply chain and customers) on security risks affecting the Group's companies to strengthen the coordinated response to potential security risks and threats.

p) Provide all assistance and cooperation that may be required by institutions and bodies competent in the field of security, including, among others, regulators, security forces and bodies and government agencies, national and international.

q) Ensure effective compliance with the obligations always imposed by the Governance and Sustainability System and applicable standards in terms of safety, always acting in accordance with current legislation and the provisions of the *Code of Ethics* and other standards of the Governance and Sustainability System.

4. Strategic Security Program

The Company's Corporate Security Board (or the management that assumes its functions in the future) will identify, implement and evaluate the actions necessary for the development of a Strategic Security Program ("**Program**"), in accordance with the principles and guidelines defined in this Policy and will develop internal rules, methodologies and procedures to ensure the correct implementation of the Program by the Company and the other companies in the Group, which will adapt it to the particularities of the territories and businesses of each of them.

The corporate security departments (or the departments, areas or functions that assume their responsibilities at any time) of each of the Group's companies undertake, in relation to the corresponding company, that at all times a level of maturity of the organization in terms of security is guaranteed in accordance with the highest existing standards at all times, taking into account the territory and business carried out by the corresponding company.

In turn, the Company's Corporate Security Department (or the area that assumes its functions from time to time) will also ensure the adequate coordination of practices and risk management in the field of security between the different companies of the Group, as well as maintaining an adequate level of maturity in terms of security.

5. Monitoring and control

The Company's Corporate Security Board (or the area that, at any time, assumes its functions) is responsible for monitoring compliance with the provisions of this *Policy*.

The above must be understood, in any case, without prejudice to the responsibilities that correspond to other bodies, areas, functions and management of the Company and, if applicable, to the management bodies of the Group's companies.

To verify compliance with this Policy, periodic assessments and audits will be carried out with internal or external auditors.

* * *

This Policy was initially approved by the Board of Directors on July 19th, 2018 and was last reviewed and updated at the Board of Directors' Meeting held on May 29th, 2024.