Corporate Security Policy

Updated July 15, 2021

The Board of Directors of NEOENERGIA S.A. (the "**Company**") is vested with the powers to prepare, assess and review the Company'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 Company and of the companies that comprise the Group, for which the Company 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 this *Corporate Security Policy (the "Policy").*

1. Purpose

The purpose of this *Policy* is to establish the main principles of conduct that shall govern the Group to ensure the effective protection of people, hardware and software assets and information, as well as the privacy of the processed data, ensuring a reasonable level of security, resilience and compliance.

This *Policy* confirms the firm commitment of the Group to excellence in the security of people, hardware and software assets, the critical infrastructure and the information, at all times ensuring that security activities are fully compliant with the law and strictly comply with the provisions in the Company's Human Rights Respect Policy.

2. Scope

Within the limits established by law, this Policy is applicable to all companies comprising the Group and investees not comprising the Group, over which the Company has management influence.

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

This Policy shall also apply, as the casa may be, to the joint ventures, temporary joint ventures and other equivalent associations, when the Company is responsible for their management.

3. Main principles of conduct

For achieving these goals, the Group takes on and promotes the following main principles of conduct that govern all of its activities in matters of corporate security:

a) design a preventive security strategy, with a comprehensive overview, for the purpose of minimizing hardware and software security risks, including consequences resulting from an act of terrorism, and allocate the resources required for its implementation;

b) develop specific defensive plans to protect critical infrastructure and to ensure the continuity of the essential services provided by Group;

c) ensure the protection of the Group's professionals, both in their workplace and in their professional displacements, for professional reasons;

d) ensure proper protection for information, as well as for the Group's systems of control, information technology and communication, pursuant to the provisions of the *Cybersecurity Risk Policy*;

e) adopt procedures and tools that allow the active fighting against fraud and attacks on the brand and reputation of the Group and its professionals;

f) ensure the right to protection of personal data for all natural persons who establish relations with the companies belonging to the Group, ensuring respect for the rights to reputation and privacy and the processing of different types of personal data, in compliance with the provisions of the Personal Data Protection Policy;

g) implement security measures based on efficiency standards and contribute to the normal course of the Group's business activities;

h) avoid the use of force when exercising security, using it solely and exclusively when strictly necessary and always in compliance with law and in a manner proportional to the threat faced, to protect life;

i) promote a culture of security within the Group by means of communication and training activities in this area.

j) ensure the proper qualification of all security personnel, both own and outsourced employees, establishing rigorous training programs and defining hiring requirements and standards according to the established plan. Particularly, train all security personnel in the area of human rights, or ensure that such personnel have received proper training in this area;

k) convey these principles to contracted security providers and periodically review their compliance;

l) collaborate with public security authorities in charge of security matters and not interfere in the performance of their legitimate duties; and

m) act at all times in compliance with applicable law and within the framework established by the Code of Ethics and the other regulations of the Governance and Sustainability System.

* * *

This Policy was initially approved by the Board of Directors on July 19, 2018 and was last reviewed and updated at the Board of Directors' Meeting held on July 15, 2021.