

SECURITY POLICY

Updated on October 13, 2026.

The Board of Directors of NEOENERGIA S.A. (the “**Company**”) is empowered to prepare, assess and continuously review the Company’s Governance and Sustainability System, as well as to approve and update the policies containing the guidelines governing the Company’s activities. Such policies also inform, where applicable, the policies that the companies comprising the group whose controlling entity, as defined by law, is the Company may approve in the exercise of their corporate autonomy (the “**Subsidiaries**” and the “**Neoenergia Group**”).

In the exercise of these powers and within the framework of applicable legislation, the Company’s *Bylaws* and the *Purpose and Values of the Iberdrola Group* (the “**Purpose and Values**”), the Board of Directors approves this *Security Policy* (the “**Policy**”), which observes, develops and adapts to the Company the *Ethical and Basic Principles of Governance and Sustainability of the Iberdrola Group* (the “**Ethical and Basic Principles of Governance and Sustainability**” and the “**Group**,” respectively).

Through this *Policy*, the Company affirms its commitment to excellence in security, which plays a central role in the day-to-day activities of the Company and its Subsidiaries, enabling them to remain secure, resilient and reliable in a continuously evolving digital environment in which increasingly sophisticated physical, cybersecurity and hybrid threats are emerging. This environment is driving higher expectations from regulators, customers and the other Stakeholder groups with which Neoenergia Group companies engage regarding compliance with increasingly stringent security standards, thereby supporting the development and consolidation of long-term, trust-based relationships.

1. Scope of application

This Policy applies to the Company. Nevertheless, it includes principles that, with respect to security, supplement the *Ethical and Basic Principles of Governance and Sustainability*. Accordingly, the principles set forth in this *Policy* inform the actions and specific internal regulations of the Subsidiaries, with due regard for their respective powers and autonomy in this area.

Where applicable, these principles shall also inform the activities of the Neoenergia Institute, which is affiliated with the Neoenergia Group.

The Company shall promote the alignment of the internal regulations of companies in which it holds an interest but which are not part of the Neoenergia Group, as well as those of *joint ventures*, temporary associations and other entities under its management, with the principles set forth in this *Policy*.

2. Purpose

The purpose of this Policy is to establish the operating principles that shall govern security matters at the Company, as the Group's *subholding* company in Brazil, and at its Subsidiaries, in order to ensure the effective protection of people; physical and cybersecurity assets, including critical infrastructure; information; knowledge; and control and communication systems, as well as the confidentiality of processed data. Security activities shall at all times be fully compliant with applicable law and strictly observe the provisions of the Company's *Human Rights Policy*.

3. Operating principles

The Company adopts and promotes the following operating principles, which shall guide its security activities:

- a) Safeguard the professionals of the Company and its Subsidiaries, both in the workplace and while traveling for business purposes, as well as individuals present at the Company's facilities or at any of its corporate events.
- b) Ensure appropriate protection of physical, cyber and information assets by proactively managing risks throughout all stages of their life cycle and ensuring appropriate levels of security—including cybersecurity across confidentiality, integrity and availability—and resilience. The most advanced standards shall be applied to assets supporting the operation of critical infrastructure, particularly in accordance with the Digital Technologies Policy, the *General Risk Control and Management Framework of the Iberdrola Group* and the *Security and Resilience Risk Guidelines and Limits* adopted by the Board of Directors.

- c) Define a security management model with clearly assigned roles and responsibilities and effective coordination mechanisms, integrating security and proactive risk management into decision-making processes and ensuring compliance with applicable security regulations, with particular emphasis on cybersecurity and the protection of essential services as priority elements.
- d) Promote the identification of non-public information deemed, or potentially deemed, to constitute a trade secret, as well as information whose unauthorized disclosure or alteration could cause serious harm to the Company's interests.
- e) Define criteria for the appropriate protection of information and knowledge, as well as control, information and communication systems, and oversee and ensure their implementation.
- f) Actively combat fraud and attacks against the brand, image and reputation of the Company and its professionals.
- g) Safeguard the right to personal data protection of the individuals with whom the Company engages, in accordance with the *Personal Data Protection Policy*.
- h) Adopt the measures required to prevent, mitigate, minimize or remediate damage caused by physical, cybersecurity or hybrid threats to the normal conduct of operations, based on criteria proportionate to the potential risks and to the criticality and value of the affected assets and services.
- i) Comply with the operating principles set forth in the *Operational Resilience Policy*, contributing to the definition, planning and execution of tests and simulations for managing incidents and crises arising from security risks, as well as to the systematic analysis and assessment of the causes and impacts of incidents, identifying lessons learned and promoting the corresponding corrective actions.
- j) Foster an inclusive culture and awareness of security in all its dimensions—physical security, cybersecurity and resilience—both internally and externally among third parties and contractors, through appropriate communications, awareness and training initiatives tailored to each audience and conducted with sufficient frequency to ensure that they have the necessary knowledge, skills, experience and capabilities.

- k) Promote appropriate security training for all internal and external personnel and define recruitment and contracting requirements and criteria that take such training into account.
- l) Embed security by design and by default into the management of Company projects that may involve potential security risks, ensuring that such risks are appropriately identified and addressed from the project's initial stages and that the necessary controls are established throughout its term.
- m) Promote the secure use of assets in a manner that strengthens detection, prevention, defense, response and recovery capabilities in the event of security attacks or incidents, ensuring their effectiveness and focusing particularly on cybersecurity threats.
- n) Promote appropriate security incident management, ensuring the detection, analysis, containment and recovery of incidents and the notification of significant incidents to the competent authorities and, where applicable, to the Company's affected Stakeholder groups.
- o) Define criteria for the secure use of artificial intelligence capabilities and oversee and ensure their implementation.
- p) Establish security requirements and standards applicable to the Company's suppliers and supply-chain partners to manage supply-chain security risks. Such requirements and standards shall be equivalent to and consistent with those established in this Policy, and their implementation shall be overseen and ensured.
- q) Monitor the organization's current context and operating environment, as well as the development of events that may help identify the most relevant security threats, with a view to anticipating their potential impact.
- r) Promote best practices, continuous improvement and innovation in security.
- s) Collaborate with the relevant Stakeholder groups, including the supply chain and customers, in relation to security risks affecting the organization, in order to strengthen a coordinated response to potential security risks and threats.

4. Group-level coordination

With respect to the specific scope of activities of each Neoenergia Group company, the Corporate Security and Resilience Department (or the area that assumes its responsibilities from time to time), through the Security, Resilience and Digital Technologies Committee (or the committee that assumes its responsibilities from time to time), shall coordinate with the Security and Resilience Department of Iberdrola, S.A. (or the department that assumes its powers from time to time) and with the Security, Resilience and Digital Technologies Committee of Iberdrola, S.A. (or the committee that assumes its responsibilities from time to time). It shall also establish a coordination framework with the Subsidiaries to ensure an appropriate consolidated level of security maturity and risk management across the Group.

In addition, the Corporate Security and Resilience Department (or the area that assumes its responsibilities from time to time), through the Security, Resilience and Digital Technologies Committee (or the committee that assumes its responsibilities from time to time), shall identify, implement and assess the actions required to prepare and oversee a strategic security program in accordance with the principles and guidelines set forth in this *Policy*, and shall develop the internal standards, methodologies and procedures required to ensure its proper implementation.

5. Implementation and monitoring

For the implementation and monitoring of the provisions of this Policy, the Board of Directors is supported by the Executive Resources Department (or the department that assumes its responsibilities from time to time), which shall develop the procedures required for this purpose.

* * *

This *Policy* was initially approved by the Board of Directors on July 19, 2018, and was most recently reviewed and updated at the meeting of the Board of Directors held on October 13, 2026.