

OPERATIONAL RESILIENCE POLICY

Updated on October 13, 2026.

The Board of Directors of NEOENERGIA S.A. (the “**Company**”) is empowered to continuously develop, assess and 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 and, where applicable, informing the policies that the companies comprising the group whose controlling entity, within the meaning established by law, is the Company may resolve to approve in the exercise of their corporate autonomy (the “**Subsidiaries**” and the “**Neoenergia Group**”).

In exercising these powers and within the framework of applicable law, the Company’s *Bylaws* and the *Purpose and Values of the Iberdrola Group* (the “**Purpose and Values**”), the Board of Directors approves this *Operational Resilience 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, as a provider of essential services and an owner of critical infrastructure, reaffirms its commitment to excellence in business and operational continuity.

1. Scope

This Policy applies to the Company. Nevertheless, it includes principles that supplement the *Ethical and Basic Principles of Governance and Sustainability* in the area of operational resilience. Accordingly, the principles of this *Policy* inform the specific actions and internal rules of the Subsidiaries, subject to their respective powers and autonomy in this matter.

These principles shall also guide, where applicable, the activities of Instituto Neoenergia, which is affiliated with the Neoenergia Group.

The Company shall promote the alignment of the internal rules of companies in which it holds an interest but which do not form part of the Neoenergia Group, as well as 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 principles of action governing operational resilience, so as to ensure that appropriate capabilities are in place to address, in a

robust, consistent, planned and coordinated manner, unforeseen adverse situations, whether internal or external, that may disrupt or alter the normal operations of the Company and, where applicable, other Group companies. The objective of this response is to minimize, to the greatest extent possible, the impact or adverse effects of such events, maintain priority operations and processes at previously defined levels, restore a stable operating environment as quickly as possible, and draw conclusions that strengthen adaptability and support improvements in responding to future events.

In addition, the Policy establishes the principles to be followed by the Group's operational resilience model (the "**Operational Resilience Model**") and, in its capacity as a provider of essential services and, where applicable, an owner of critical infrastructure, reaffirms its firm commitment to excellence in business and operational continuity, ensuring at all times that operational resilience activities fully comply with applicable regulations and the Governance and Sustainability System.

3. Principles of action

The Company adopts and promotes the following principles of action, which shall govern its activities in the area of operational resilience:

- a) Periodically assess and identify priority business processes across all organizations, together with their associated resources and operational resilience requirements, based on consistent criteria, in order to safeguard them against adverse situations that may affect them.
- b) Maintain appropriate crisis response and management capabilities to address adverse situations and crises that may affect the Company's priority operations in a robust manner, and appropriately manage resilience risks in accordance with the Security Policy, the General Risk Control and Management Framework of the Iberdrola Group, and the Security and Resilience Risk Guidelines and Limits.
- c) Periodically review, update and test response and crisis management plans to verify their effectiveness and validity, identify deficiencies and opportunities for improvement, and capture lessons learned.
- d) Define and implement, through the Operational Resilience Model, a formal, recurring and measurable practice that establishes, for each level of the organization, the appropriate operational resilience capabilities, as well as the roles, responsibilities and resources required to implement such capabilities, in accordance with market standards and best practices.
- e) Periodically assess and monitor the level of implementation and effectiveness of the Operational Resilience Model, identifying deficiencies and opportunities and promoting its continuous improvement.
- f) Promote an appropriate level of education, training and awareness regarding operational resilience at all levels of the organization.
- g) Maintain appropriate coordination among the divisions of Group companies assigned responsibilities for operational resilience, risk and internal compliance.
- h) Regularly monitor the internal and external environment, including developments in threats, vulnerabilities, critical dependencies, internal

- capabilities, and technological, regulatory, social, economic or competitive changes that may affect operational resilience.
- i) Document material incidents, tests and simulation exercises; assess the causes and impacts of incidents; capture lessons learned; and define corrective actions for each of them.
 - j) Identify stakeholders relevant to operational resilience and consider their needs, expectations and requirements in accordance with the Stakeholder Relations Policy and the Operational Resilience Model.
 - k) Allocate adequate resources to perform the functions and responsibilities established in the Operational Resilience Model and the operational resilience plans.
 - l) Promote the integration of operational resilience into Company initiatives from the initial and design stages and by default, in coordination with risk management, security, cybersecurity and digital technologies.

4. Group-level coordination: the *Operational Resilience Model*

The Resources Division (or the management body that assumes its powers from time to time), through the Security, Resilience and Digital Technologies Committee (or the committee that assumes its powers from time to time), shall periodically review the Operational Resilience Model, which was developed in accordance with the Ethical and Basic Principles of Governance and Sustainability of the Iberdrola Group and the provisions of this Policy.

The Operational Resilience Model shall establish common criteria and practices for action, coordination, monitoring and oversight, while in all cases respecting the autonomy of the Group companies. This enables them to comply with the principles of action set forth in this Policy by defining the roles and responsibilities, as well as the rules, programs, guidelines and procedures required for Group companies to maintain the capabilities necessary to develop operational resilience on a continuous, formal, consistent, systematic and measurable basis, aligned with generally recognized standards and best practices in the field.

The Operational Resilience Model enables the Company and the other Group companies to support the Group's strategic objectives and brand image, safeguard its reputation and credibility, reduce the impact of disruptive events, protect lives, assets and natural capital, and maintain proactive and efficient risk management, while also ensuring compliance, among other matters, with their responsibilities as providers of an essential service such as electricity supply and, where applicable, as owners of critical infrastructure.

For this purpose, the Operational Resilience Model shall establish, at a minimum, the following:

- a) Regularly analyze the activities and processes of the various corporate and business areas and establish their level of priority from an operational resilience perspective.
- b) Define response plans for adverse situations that are appropriate to their nature and severity, including general incident response procedures and specific business continuity and crisis management plans setting out the required organizational structures, the criteria and procedures to be followed, and the resources needed for their execution.
- c) Define and conduct tests and simulation exercises for the response plans, identifying deficiencies and opportunities and drawing conclusions.
- d) Periodically assess and oversee the level of implementation and effectiveness of the Operational Resilience Model.
- e) Identify legal or regulatory requirements relating to operational resilience and validate their coverage and compliance.
- f) Establish mechanisms to monitor and oversee the implementation of the Operational Resilience Model within the Company and establish resilience functions at those levels.

The Operational Resilience Model shall incorporate monitoring metrics and indicators aligned with the Security and Resilience Risk Guidelines and Limits, including, where applicable, indicators for process assessment, plan definition and testing, crisis exercises, material risks pending mitigation, and material incidents.

Based on the provisions of the Operational Resilience Model, each Group company shall prepare its respective operational resilience plans, detailing the activities to be carried out each year in order to effectively deploy, implement and execute the Operational Resilience Model, applying it within each of its areas according to the scope defined in each case.

Likewise, the Security, Resilience and Digital Technologies Committee (or the committee that assumes its powers from time to time) shall coordinate with the corresponding committees of the companies or, where applicable, with the Corporate Security and Resilience Department (or the management body that assumes its powers from time to time) to ensure that each Group company prepares its respective operational resilience plans, and to monitor the execution of such plans, as well as operational resilience practices and risk management within their respective areas of responsibility.

The Security, Resilience and Digital Technologies Committee (or the committee that assumes its powers from time to time) shall monitor the status of the Operational Resilience Model and its degree of implementation at Group level.

5. Implementation and monitoring

For the implementation and monitoring of the provisions of this *Policy*, as well as for the implementation and monitoring of the *Operational Resilience Model*, the Board of Directors is supported by the Executive Resources Division (or the area that assumes its functions from time to time) and the Security, Resilience and Digital Technologies Committee (or the committee that assumes its functions), which establish periodic procedures for monitoring and reporting to the governance bodies.

* * *

This Policy was initially approved by the Board of Directors on May 29, 2024, and was last amended at the Board of Directors' Meeting held on October 13, 2026.