Operational Resiliency Policy

25 March 2025

The Board of Directors of IBERDROLA, S.A. (the "**Company**") has the power to design, assess and continuously revise the Company's Governance and Sustainability System, and specifically to approve and update policies, which contain the guidelines governing the conduct of the Company, and furthermore, to the extent applicable, inform the policies that the companies belonging to the group of which the Company is the controlling entity, within the meaning established by law (the "**Group**"), decide to approve in the exercise of their autonomy.

In exercising these powers and within the framework of legal provisions, the By-Laws and the Purpose and Values of the Iberdrola Group, the Board of Directors hereby approves this Operational Resiliency Policy (the "**Policy**"), which respects, further develops and adapts the Ethical and Basic Principles of Governance and Sustainability of the Iberdrola Group with respect to the Company.

1. Scope of Application

This Policy applies to the Company. Without prejudice to the foregoing, it includes basic principles that, in the area of the sustainable value chain, and particularly operational resilience, complement those contained in the Ethical and Basic Principles of Governance and Sustainability of the Iberdrola Group and, to this extent, must inform the conduct and standards-setting implemented by the other companies of the Group in this area in the exercise of their powers and in accordance with their autonomy.

To the extent that listed country subholding companies form part of the Group, they and their subsidiaries, under their own special framework of strengthened autonomy, may establish principles and rules that must have content consistent with the principles of this Policy.

To the extent applicable, these principles must also inform the conduct of the foundations linked to the Group.

For companies that do not form part of the Group but in which the Company holds an interest, as well as for *joint ventures*, temporary *joint ventures* (*uniones temporales de empresas*) and other entities in which it assumes management, the Company shall also promote the alignment of its regulations with the basic principles regarding the sustainable value chain, and particularly operational resilience, contained in this Policy.

2. Purpose

The purpose of this Policy is to establish the principles of conduct as regards operational resiliency, that is, to provide a consistent, planned and coordinated response to internal or external disruptive events or incidents or crises, of any nature, that might unexpectedly involve a significant disruption or loss in the normal operations of the Company, or, to the extent applicable, of the Group's companies, in order to maintain its critical business operations and processes and key structures at previously established levels, and, if applicable, to recover operational capacity with the minimum impact and within the shortest possible period.

The Policy also includes the principles that the operational resiliency model of the Company and the other companies of the Group (the "**Operational Resiliency Model**") must follow, and the Company confirms, as a provider of essential services and as the owner of any critical infrastructure, its firm link to excellence as regards the continuity of the business and activities, ensuring at all times that its operational resiliency activities are fully in accordance with applicable legal provisions and with the Governance and Sustainability System.

3. Main Principles of Conduct

The Company adopts and promotes the following main principles of conduct that must inform all of its activities in the area of operational resilience:

a. Define the continuity strategies and plans, endeavouring to ensure continuity of operational capacity and strengthening resilience, in order to minimise the impact of disruptive events or crises that might affect business continuity, to be regularly tested to improve and validate their capacities and response.

b. Establish a comprehensive management process to lead, direct and supervise the activities of the Group's companies in response to disruptive incidents or crises that might have an impact on the Company or at the Group level as a whole.

c. In relation to the external and internal context, including the political environment, assess the social, economic, legal and cultural aspects, the technological and competitive context, internal capacities, resources and decision-making processes to address disruptive incidents or crises.

d. Promote the continuous improvement of processes by measuring, evaluating and reporting on the performance and effectiveness of the results of the operational resiliency plans of the Company and at the Group level.

e. Allocate appropriate resources for the performance of the duties and responsibilities corresponding thereto established in the Operational Resilience Model and in the operational resiliency plans.

f. Develop, provide and continuously improve the education and training of the staff assigned to the duties defined in the Operational Resilience Model.

g. Promote a culture of operational resiliency and awareness within the Group, through an updated and continuous training programme.

h. Via the Operational Resilience Model, implement a formal, documented and measurable management system that defines the framework of activities for the operational resiliency plans of the Group's companies, endeavouring to ensure continuous improvement in order to achieve its goals.

4. Group-level Coordination: the Operational Resilience Model

The Security and Resilience Division (or such division as assumes the powers thereof at any time), through the Security, Resilience and Digital Technology Committee (or such committee as assumes the powers thereof at any time) shall establish and regularly review an Operational Resiliency Model, which shall be prepared in accordance with the Ethical and Basic Principles of Governance and Sustainability of the Iberdrola Group and this Policy, and in which the methodologies, procedures and tools required for the Group's companies to have the appropriate operational resilience capabilities shall be defined.

The Operational Resilience Model allows the Company and the other companies of the Group to, whilst ensuring compliance with, among other things, their responsibilities as providers of an essential service such as that of electricity supply and, if applicable, the owner of critical infrastructure, to support the strategic goals of the Iberdrola Group, protect their reputation and credibility, reduce the costs of disruptive shutdowns, protect life, property and the environment, improve their capacity to remain effective during disruptions, and maintain proactive and efficient control of risks.

The Operational Resilience Model must include at least the following aspects:

- Include a description of the organisational structure, procedures and plans related to operational resiliency and to the management of disruptive incidents or crises and recovery thereafter, as well as the allocation of resources and the clear attribution of duties and responsibilities to specific persons in this area.

- Define the range of measures and procedures necessary to increase the resilience of the Group's companies, their scope and priorities.
- Evaluate the risks to which the Group's companies are exposed by using methodologies based on market standards and good practices, analysing potential impacts on business operation, and determining on that basis the critical processes and activities for continuity of their activities, identifying priorities and establishing target recovery times in each case.
- Describe the processes that must be used to identify the interested parties that are significant for the operational resiliency plans, their needs and expectations, to determine their requirements.
- Establish monitoring and control methods, compliance metrics and analysis of evaluation results for the subsequent application of the most suitable corrective measures, all while maintaining appropriate coordination with the relevant risk and internal assurance divisions of the Group's companies.
- Establish rules for the creation of resiliency offices (or such bodies as assume the powers thereof at any time) at the Company and at the country subholding companies, as a mechanism for coordinating and supervising the implementation of the defined resilience plans and, in the case of the Company, the supervision of the effective implementation of the Operational Resiliency Model at the Group level.

Based on the Operational Resiliency Model, each company shall prepare its respective operational resiliency plans, which shall include details of the tasks to be carried out in each financial year within the Company and its subsidiaries, in order to effectively deploy, implement and execute the Operational Resiliency Model, applying it in each area for the defined scope in each case.

For this purpose, the Company's Security and Resilience Division (or such division as assumes the powers thereof at any time) with the support of the resilience office, shall coordinate the preparation of said operational resiliency plans with the corporate and business divisions in each area.

In addition, the Security, Resilience and Digital Technology Committee (or such committee as assumes the powers thereof at any time) shall coordinate with the corresponding committees of the country subholding companies or, in the absence thereof, with the Security and Resilience Division (or such division as assumes the powers thereof at any time) to ensure the creation of their respective operational resilience plans at each company of the Group, as well as monitoring of the definition, review and implementation of their respective resilience plans and operational resilience risk practices and management, in their respective countries or territories and for the specific businesses. The Security, Resilience and Digital Technology Committee (or such committee as assumes the powers thereof at any time) shall monitor the status of the Operational Resiliency Model and its level of implementation at the Group level.

5. Implementation and Monitoring

For the implementation and monitoring of the provisions of this Policy, as well as for the monitoring of the Operational Resiliency Model, the Board of Directors is assisted by the Security and Resilience Division (or such division as assumes the powers thereof at any time), through the Security, Resilience and Digital Technology Committee (or such committee as assumes the powers thereof at any time), which shall establish a procedure for regular monitoring and reporting to the governance bodies.

* * *

This Policy was initially approved by the Board of Directors on 20 February 2024 and was last amended on 25 March 2025.