Corporate Security Policy

C

20 February 2024

NOTICE. This document is a translation of a duly approved Spanish-language document, and is provided for informational purposes only. In the event of any discrepancy between the text of this translation and the text of the original Spanish-language document that this translation is intended to reflect, the text of the original Spanish-language document shall prevail.

The Board of Directors of IBERDROLA, S.A. (the "**Company**") has the power to design, assess and continuously revise the Governance and Sustainability System, and specifically to approve and update the corporate policies, which contain the guidelines governing the conduct of the Company and of the companies belonging to the group of which the Company is the controlling entity, within the meaning established by law (the "**Group**").

In fulfilling these responsibilities, in order to lay down the general principles that are to govern all aspects of the corporate security activities and in compliance with the provisions of the *Purpose and Values of the Iberdrola Group*, the Board of Directors hereby approves this *Corporate Security Policy* (the "***Policy***").

1. Purpose

The purpose of this *Policy* is to establish the main principles of conduct that are to govern security at the Group's companies, to ensure the effective protection of people, of physical assets (including critical infrastructure), of information and of knowledge and of the control and communications systems, as well as of privacy of processed data, at all times endeavouring to ensure that security activities are fully in accordance with the law and scrupulously comply with the provisions of the *Policy on Respect for Human Rights*.

Through this *Policy*, the Company states its commitment to excellence in terms of security, which plays a leading day-to-day role at the companies of the Group, so that they remain secure, resilient and reliable in a continuously transforming digital community, where increasingly sophisticated hardware, cybersecurity and hybrid threats are arising, causing increased levels of demands from regulators, from customers and from the other Stakeholders with which the companies of the Group have a relationship, with respect to compliance with increasingly high security standards that allow for the construction and consolidation of long-lasting relationships of trust.

2. Scope of Application

This *Policy* applies at the Company and at all companies of the Group, as well as at all investees not belonging to the Group over which the Company has effective control, within the lawfully established limits.

Without prejudice to the provisions of the preceding paragraph, listed country subholding companies and their subsidiaries, based on their own special framework of strengthened autonomy, may establish an equivalent policy, which must be in accord with the principles and guidelines set forth in this *Policy* and in the other environmental, social and corporate governance and regulatory compliance policies of the Governance and Sustainability System.

At those companies in which the Company has an interest and to which this *Policy* does not apply, the Company will promote, through its representatives on the boards of directors of such companies, the alignment of their own policies with those of the Company.

This *Policy* shall also apply, to the extent relevant, to the joint ventures, temporary joint ventures (*uniones temporales de empresas*) and other equivalent associations, if the Company assumes the management thereof.

This *Policy* is developed and supplemented by the following specific policies, also approved by the Company's Board of Directors: the *Personal Data Protection Policy* and the *Cybersecurity Risk Policy*, with regard to said areas.

3. Main Principles of Conduct

To realise the commitment set forth in Section 1 above, the following main principles of conduct that must inform all of the corporate security activities of the Group are established:

a. Define a comprehensive security strategy with a preventive and proactive approach to guarantee a reasonable level of risk.

b. Ensure the appropriate protection of assets (including critical infrastructure), to proactively manage risks.

c. Guarantee the protection of the professionals of the companies of the Group, both in their workplace and in their professional travel, as well as the protection of persons when they are at the facilities or at any institutional event of the Group's companies.

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

e. Ensure the adequate protection of information and knowledge, as well as of the control, information technology and communication systems, to proactively manage risks pursuant to the provisions of the *Cybersecurity Risk Policy* (or such regulation as may replace it at any time).

f. Promote the identification of non-public information classified (or that could be classified) as confidential or secret, as well as the information considered (or that could be considered) to be a trade secret, and define standards for the appropriate protection thereof, ensuring their implementation.

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

h. Guarantee the right to the protection of personal data for all natural persons who establish relations with the companies belonging to the Group, in accordance with the provisions of the *Personal Data Protection Policy* (or such regulation as may replace it in the future).

i. Adopt the measures necessary to prevent, neutralise, minimise or restore the harm caused by hardware, cybersecurity or hybrid security threats to normal business operations, based on criteria of proportionality to the potential risks and the critical nature and value of the affected assets and services.

NOTICE. This document is a translation of a duly approved Spanish-language document, and is provided for informational purposes only. In the event of any discrepancy between the text of this translation and the text of the original Spanish-language document that this translation is intended to reflect, the text of the original Spanish-language document shall prevail.

j. Comply with the main principles of conduct established in the *Operational Resilience Policy.*

k. Foster an inclusive culture and awareness regarding security within the Group, through appropriate dissemination, education and training activities adapted to each recipient and with sufficient regularity to guarantee up-to-date knowledge in this area.

l. Promote appropriate security training for all staff, both internal and external, defining hiring requirements and standards that take this training into account.

m. Monitor the current organisational and environmental context, as well as the evolution of events that permit the identification of the most significant security threats in order to anticipate their potential impact.

n. Promote best practices and innovation in the area of security.

o. Collaborate with relevant Stakeholders (including the supply chain and customers) on security risks that affect the Group's companies, to strengthen the coordinated response to potential security risks and threats.

p. Provide all assistance and cooperation that may be requested by the competent security institutions and bodies, including but not limited to regulators, security forces and bodies and governmental agencies, both domestic and international, in those countries in which the Group carries out its activities.

q. Endeavour to ensure effective compliance with the obligations imposed by the Governance and Sustainability System and by applicable security regulations at any time, always acting in accordance with applicable law and the provisions of the *Code of Ethics* and the other rules of the Governance and Sustainability System.

4. Strategic Security Programme

The Corporate Security Division (or such division as assumes the duties thereof in the future) shall identify, implement and evaluate the actions necessary to prepare a Strategic Security Programme (the "**Programme**") in accordance with the principles and guidelines defined in this *Policy*, and it shall develop the internal rules, methodologies and procedures to ensure the appropriate implementation of the Programme by the Company and by the other companies of the Group, which shall adapt it to the particular features applicable in each of their territories and businesses.

The corporate security divisions (or such divisions, areas or functions as assume the powers thereof at any time) of each of the Group's companies shall endeavour to guarantee, with respect to their corresponding company, a level of maturity at the organisation at all times in terms of security, in accordance with the highest existing standards at any time, in view of the territory and of the business carried out by the corresponding company.

In turn, the Corporate Security Division (or such division as assumes the duties thereof at any time) shall also endeavour to ensure the appropriate coordination of practices and the management of security risks among the various companies of the Group, as well as the maintenance of an appropriate level of maturity at Group level in terms of security.

5. Supervision and Control

The Corporate Security Division (or such division as assumes the duties thereof at any time) shall supervise compliance with the provisions of this *Policy*.

The foregoing shall in any event be without prejudice to the responsibilities vested in other bodies, areas, functions and divisions of the Company and, if applicable, in the management decision-making bodies of the companies within the Group.

Regular evaluations and audits shall be performed with internal or external auditors in order to verify compliance with this Policy.

***

This *Policy* was initially approved by the Board of Directors on 23 September 2013 and was last amended on 20 February 2024.

NOTICE. This document is a translation of a duly approved Spanish-language document, and is provided for informational purposes only. In the event of any discrepancy between the text of this translation and the text of the original Spanish-language document that this translation is intended to reflect, the text of the original Spanish-language document shall prevail.