Security 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 regulations, the By-Laws and the Purpose and Values of the Iberdrola Group, the Board of Directors hereby approves this Security 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.

In this Policy, the Company states its commitment to excellence in terms of security, which plays a leading role in its day-to-day activities, so that it remains secure, resilient and reliable in a continuously transforming environment, in which increasingly more sophisticated physical, cybersecurity and hybrid threats are arising. All of the foregoing entails an increased levels of demands from regulators, from customers and from other Stakeholders of the Company with respect to compliance with increasingly high security standards that allow for the construction and consolidation of long-lasting relationships of trust.

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 security, 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 enhanced 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 security, contained in this Policy.

2. Purpose

The purpose of this Policy is to establish the main principles of conduct that are to govern security at the Company, in order to endeavour to ensure the effective protection of people, of both physical and cyber 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 legal provisions and scrupulously comply with the provisions of the Policy on Respect for Human Rights.

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 security:

a. Endeavour to ensure the protection of the professionals of the companies of the Group, both in their workplace and in their professional travels, as well as the protection of persons when they are at the facilities or at any institutional event of the Company.

b. Ensure the adequate protection of both physical and cyber assets to proactively manage risks in all phases of their life cycle, ensuring that they have an appropriate level of security, cybersecurity and resilience, applying the most advanced standards for those that support the operation of critical infrastructure in accordance with the General Risk Control and Management Foundations of the Iberdrola Group and with the Cybersecurity Risk Guidelines and Limits approved by the Board of Directors.

c. 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.

d. Promote the identification of non-public information considered (or likely to be considered) as business secrets, as well as information whose unauthorised disclosure or alteration could cause serious damage to the interests of the Company.

e. Define the standards for the adequate protection of information and knowledge, as well as of the control, information technology and communication systems, supervising and ensuring the implementation thereof.

f. Promote the active fight against fraud and against attacks on the brand, image and reputation of the Company and its professionals.

g. Guarantee the right to the protection of personal data for natural persons with whom relations are maintained, in accordance with the provisions of the Personal Data Protection Policy.

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

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

j. Foster an inclusive culture and awareness regarding security, both internally and externally, towards third parties and partners, through appropriate dissemination, awareness-raising and training activities adapted to each recipient and with sufficient regularity to ensure that they have the required knowledge, expertise, experience and skills.

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

l. Promote the integration of security in the management of the Company's projects that may involve a potential security risk, in such a way as to obtain the proper identification and treatment of this risk from the design and initial phases of the project and the establishment of the necessary controls during the life of the project.

m. Promote the secure use of assets to strengthen detection, prevention, defence, response and recovery capabilities against attacks or security incidents, ensuring the effectiveness thereof and paying particular attention to cybersecurity threats.

n. Monitor the current organisational and environmental context, as well as the evolution of events that allow for the identification of the most significant security threats in order to anticipate the potential impact thereof.

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

p. Collaborate with relevant Stakeholders (including the supply chain and customers) on security risks that affect the Company, to strengthen the coordinated response to potential security risks and threats.

4. Group-level Coordination

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 coordinate with any security, resilience and digital technology committees that may be created at the country subholding companies or, in the absence thereof, with the corresponding security and resilience divisions (or such divisions, areas or functions as assume the powers thereof at any time) of each of the Group's companies, in order to seek an appropriate consolidated level of maturity and risks in security matters at the Group level.

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 identify, implement and evaluate the actions necessary to prepare and supervise a Strategic Security Programme in accordance with the principles and guidelines defined in this Policy and shall develop the internal rules, methodologies and procedures to ensure the appropriate implementation of thereof.

5. Implementation and Monitoring

For the implementation and monitoring of the provisions of this Policy, the Board of Directors is assisted by the Security and Resilience Division (or such division as assumes the powers thereof at any time), which shall further develop the procedures required for such purpose.

Regular evaluations and audits shall also 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 25 March 2025.