Corporate Security Policy

C

20 June 2023

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 within the boundary of the Group to ensure the effective protection of people, of hardware and software assets and critical infrastructure, and of information, as well as of the privacy of the data processed, ensuring a reasonable level of security, resilience and compliance.

This *Policy also* confirms the firm commitment of the Company to excellence in the area of security of people, of the hardware and software assets and critical infrastructure of the Group's companies and of information, at all times ensuring that security activities are fully in accordance with the law and scrupulously comply with the provisions of the *Policy on Respect for Human Rights*.

2. Scope of Application

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

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 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.

3. Main Principles of Conduct

To realize 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 companies that make up the Group are adopted and promoted within the boundary thereof:

a. Design a preventive security strategy, with a comprehensive vision, the objective of which is to minimise hardware and software security risks, including the consequences resulting from an act of terrorism, and allocate the resources required for the implementation thereof.

b. Develop specific defensive plans to protect critical infrastructure and to ensure the continuity of the essential services provided by the companies of the Group.

c. Guarantee the protection of the professionals of the companies of the Group, both in their workplace and in their professional travel.

d. Ensure the adequate protection of information and knowledge and the confidentiality thereof, as well as of the control, information technology and communication systems of the Group, and establish controls and procedures for this purpose, particularly to avoid any unlawful acquisition, use or disclosure of the information or knowledge, pursuant to the provisions of the *Cybersecurity Risk Policy.*

e. Identify non-public information that should be classified as confidential or secret, as well as information or knowledge considered (or that could be considered) to be a trade secret, and implement and develop appropriate and reasonably sufficient security and privacy procedures or protocols, taking into account the risk level of an occurrence thereof, while also endeavouring to ensure that the integrity and availability of such information or knowledge is protected.

f. Have procedures and tools that allow for actively fighting against fraud and against attacks on the brand and reputation of the Group and its professionals.

g. Guarantee the right to the protection of personal data for all natural persons who establish relations with the companies belonging to the Group, ensuring respect for the rights to reputation and to privacy in the processing of the various categories of personal data, in accordance with the provisions of the *Personal Data Protection Policy.*

h. Implement security measures based on efficiency standards and that contribute to the normal performance of the Group's business activities.

i. Avoid the use of force in the exercise of security, using it solely and exclusively when strictly necessary and always in accordance with the law and in a manner proportional to the threat faced, in order to protect life.

j. Promote a culture of security within the Group by means of communication and training activities in this area.

k. Ensure the proper qualification of all security personnel, both internal and external, establishing rigorous training programmes and defining hiring requirements and standards that take this principle into account. In particular, train all security personnel in the area of human rights, or ensure that such personnel have received proper training in this area.

l. Inform security providers who may be hired, as appropriate, of the principles of this *Policy* and regularly evaluate their compliance herewith.

m. Collaborate with public authorities having responsibility for public security matters and not interfere in the performance of their legitimate duties.

n. Act at all times in compliance with applicable law and within the framework established by the *Code of Ethics* and the other rules of the Governance and Sustainability System.

***

This *Policy* was initially approved by the Board of Directors on 23 September 2013 and was last amended on 20 June 2023.