Corporate Security Policy

C

28 April 2020

The Board of Directors of IBERDROLA, S.A. (the "**Company**") has the power to design, assess and continuously revise the Corporate Governance System, and specifically to approve the corporate policies, which further develop the principles reflected in the *Purpose and Values of the Iberdrola group* and the other rules of the Corporate Governance System, as well as to organise the internal control systems. In exercising these powers, and in order to lay down the general principles that are to govern all aspects of the corporate security activities of the companies belonging to the group of which the Company is the controlling entity, within the meaning established by law (the "**Group**"), the Board of Directors hereby approves this *Corporate Security Policy* (the "***Policy***").

1. Purpose

This *Policy* establishes the main principles of conduct that are to govern the Group to ensure the effective protection of people, of hardware and software assets 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 security of people and of the critical assets and infrastructure of the Group and of information, at all times ensuring that security activities fully comply with law and scrupulously comply with the provisions of the Company's *Policy on Respect for Human Rights*.

2. Main Principles of Conduct

To achieve this commitment, the Group accepts and promotes the following main principles that must inform all of its corporate security activities:

a. Design a preventive security strategy, with a comprehensive overview, the objective of which is to minimise hardware and software security risks, including those 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 sufficient protection of information, as well as the control and information technology and communication systems of the Group, pursuant to the provisions of the *Cybersecurity Risk Policy*.
e. 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.
f. 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*.
g. Implement security measures based on efficiency standards and that contribute to the normal course of the Group's business activities.
h. Avoid the use of force in the exercise of security, using it solely and exclusively when strictly necessary and always in accordance with law and in a manner proportional to the threat faced, to protect life.
i. Promote a culture of security within the Group by means of communication and training activities in this area.
j. 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.
k. Inform hired security providers of these principles and regularly evaluate their compliance herewith.
l. Collaborate with public security authorities having responsibility for public security matters and not interfere in the performance of their legitimate duties.
m. 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 Corporate Governance System.

* * *

This *Policy* was initially approved by the Board of Directors on 23 September 2013 and was last amended on 28 April 2020.