SCOTTISHPOWER SECURITY POLICY

8 July 2026

The Board of Directors of Scottish Power Limited (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 "**SP Group**"), decide to approve in the exercise of their autonomy.

In exercising these powers and within the framework of legal regulations, the *Articles of Association* and the *Purpose and Values of the Iberdrola Group*, the Board of Directors hereby approves this *ScottishPower 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 SP Group in this area in the exercise of their powers and in accordance with their autonomy.

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

For companies that do not form part of the SP 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 *ScottishPower 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 SP 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, and of information, to proactively manage risks in all phases of their life cycle, ensuring that they have an appropriate level of both security, including cybersecurity in any of the dimensions of confidentiality, integrity and availability, and resilience, applying the most advanced standards for those that support the operation of critical infrastructure in accordance with, in particular, the *ScottishPower Digital Technology Policy*, the *General Risk Control and Management Foundations of the Iberdrola Group* and with the *Security and Resilience 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 with effective coordination mechanisms, which integrates security and proactive risk management into decision-making processes and endeavours to ensure compliance with applicable legal provisions in terms of security, particularly reinforcing cybersecurity and the protection of essential services as priorities.

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, as well as 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 *ScottishPower Operational Resilience Policy*, contributing to the definition, planning and implementation of tests and drills aimed at managing incidents and crises arising from security risks; as well as to the systematic analysis and evaluation of the causes and impacts of incidents, identifying lessons learned and driving the corresponding corrective measures.

j) Foster an inclusive culture and awareness regarding security, in all dimensions thereof (physical, cybersecurity and resilience), 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 by default and by design into the management of Company 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 initial phases 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) Promote the appropriate management of security incidents by endeavouring to ensure their detection, analysis, containment and recovery and the reporting of significant incidents to the competent authorities and, if applicable, to the affected Stakeholders of the Company.

o) Define standards for the secure use of artificial intelligence capabilities, and endeavour to ensure and oversee the implementation thereof.

p) Establish security requirements and standards applicable to the suppliers and partners in the Company's supply chain, in order to manage the security risks associated with the supply chain, that are equivalent to and consistent with the

provisions of this *Policy*, as well as endeavour to ensure and oversee the implementation thereof.

q) 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.

r) Promote best practices, continuous improvement and innovation in the area of security.

s) 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. Iberdrola Group-level Coordination

The Company's Security, Resilience and Digital Technology Committee shall coordinate with the Security, Resilience and Digital Technology Committee of Iberdrola, S.A. (or such committee as assumes the powers thereof at any time) regarding security matters at the Iberdrola Group level.

5. Implementation and Monitoring

For the implementation and monitoring of the provisions of this *Policy*, the Board of Directors is assisted by the Corporate Security 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 as the *Corporate Security Policy* and was last amended on 8 July 2026.