

Digital Technologies Policy

Approved on June 18, 2026

NEOENERGIA S.A.'s (the "**Company**") Board of Directors has the power to prepare, evaluate and consistently review the Company's Governance and Sustainability System, as well as approve and update policies that contain guidelines that govern its performance. They may also provide notice of, as applicable, the policies that they autonomously decide to approve at companies that are part of the group where the controlling company by law is the Company (the "**Subsidiaries**" and "**Neoenergia Group**").

In exercising these powers and in accordance with applicable law, the Company's *Articles of Incorporation*, and the *Iberdrola Group's Purpose and Values* (the "**Purpose and Values**"), the Board of Directors hereby approves this *Digital Technologies Policy* (the "**Policy**"), which respects, builds upon, and adapts in relation to the Company the *Iberdrola Group's Ethical and Basic Principles of Governance and Sustainability* (the "**Ethical and Basic Principles of Governance and Sustainability**" and the "**Group**," respectively).

1. Scope

This *Policy* shall apply to the Company. Nevertheless, it includes principles that complement, within the scope of sustainable value and, in particular, for innovation and digital transformation strategy, the *Ethical and Basic Principles of Governance and Sustainability*. To this extent, the principles of this *Policy* inform the specific actions and regulations of the Subsidiaries, observing their powers and autonomy in this matter.

These principles must also guide, when applicable, the performance of the Neoenergia Institute, which is linked to the Neoenergia Group.

The Company will ensure regulations at the companies in which it holds an ownership interest, but which are not part of the Neoenergia Group, as well as joint ventures, temporary company associations and other entities it manages, are aligned with the principles contained in this *Policy*.

2. Purpose

The purpose of this *Policy* is to establish an overall framework for the governance and proactive management of processes and actions related to digital technologies, including information technology and operational technology, recognizing their importance as an essential resource for achieving the Company's objectives, as well as for ensuring the effective and efficient operation of business processes. This *Policy* promotes a coordinated approach to architecture, security and possible convergences with other

technologies, seeking to minimize operational and security risks and ensure the continuity of systems.

For the purposes of this *Policy*, the following definitions apply:

- (i) **Information technology ("IT")**, a series of physical elements or materials that constitute a computer or a computer system ("**Hardware**") and the series of computer programs, instructions, data and rules for performing certain tasks on a computer ("**Software**") used for data manipulation. IT focuses on the management and protection of digital information, including communication networks in general, data storage and processing and management systems and is limited to Hardware and Software that are approved by the Systems Board.
- (ii) **Operation Technologies ("OT")** are the Hardware and Software used to control and interact with physical industrial processes in real time, including local control systems, SCADA (*Supervision, Control and Data Acquisition*), remote operation and telecommunications systems, among others.

3. Principles of action

The Company assumes and promotes the following principles of action, which must guide activities related to the use of digital technologies:

- (i) **Operational Continuity:** Ensure the continuity of operations aimed at providing services by applying criteria of high availability and resilience, and by developing business continuity, contingency, and disaster recovery plans, all in accordance with the *Security Policy*, the *Operational Resilience Policy*, the *Iberdrola Group's General Principles for Control and Risk Management*, and the *Risk Guidelines and Limits for Digital Technologies*, as approved or adopted, as applicable, by the Board of Directors.
- (ii) **Operational efficiency:** promote the operation of IT and OT assets at maximum efficiency, optimizing human and material resources and their costs during the asset life cycle, based on reliable processes and technologies that will ensure the high availability of facilities. Best practices and recognized standards must also be applied.
- (iii) **Risk management:** promote the identification and proactive management of risks in devices, systems and processes associated with digital technologies and ensure that identified risks are within the limits considered appropriate. This will in particular include risks related to safety, natural capital, business continuity and those associated with facilities considered critical in accordance with applicable regulations. These processes include, in particular, the planning, implementation and use of solutions that enable the identification, protection, detection, response

and recovery of cybersecurity risks in coordination with the *Security Policy* and the *Operational Resilience Policy*, as well as with the *Cybersecurity Risk Guidelines and Limits*.

- (iv) Technological innovation and life cycle: promote guidelines for the safe design, planning, implementation, operation, renewal, decommissioning and replacement of IT and OT equipment and systems.
- (v) Sustainability and social responsibility: promote the selection of technologies that optimize energy efficiency and reduce energy consumption and loss and greenhouse gas emissions. In particular, special attention must be paid to ensure that the devices, systems and processes associated with digital technologies do not affect the health of professionals, users, customers and society in general.
- (vi) Training and awareness: promote the proper preparation and training of planners, developers, maintenance professionals and users of digital technologies, depending on their profile, so that they are able to understand the risks associated with these technologies.

4. Coordination of the Group's digital governance model

The Digital Technology Governance Model must be established within the Group, in accordance with the provisions of the *Ethical and Basic Principles of Governance and Sustainability*, the *Basis for the definition and coordination of the Iberdrola Group* and this *Policy*, with the objective of defining the methodologies, procedures and tools necessary for the Group's companies to operate under a common model that allows compliance with the principles of action.

The Resources Executive Board (or the board that may eventually assume its responsibilities), through the Company's Security, Resilience, and Digital Technologies Committee (or the committee that may eventually succeed it), oversees the implementation process of the aforementioned Digital Technology Governance Model.

Similarly, the Resources and Services Board of Iberdrola, S.A. (or the board that, at any given time, assumes its powers), through the Security, Resilience, and Digital Technologies Committee (or the committee that, at any given time, assumes its functions) and together with the corresponding departments of the Subsidiaries that, in due course, assume such responsibilities, in order to ensure an adequate and consolidated level of maturity for the Digital Technology Governance Model.

5. Implementation and development

For the implementation and monitoring of the provisions of this *Policy*, the Board of Directors will have the support of the Resources Executive Board (or the board that may eventually assume its duties), which will be responsible for developing the necessary procedures for this purpose.

The Resources Executive Board (or the board that, from time to time, assumes its functions) will review this *Policy* at least once a year, in order to ensure that its content remains aligned with the continuous advances, innovations, risks and regulatory changes applicable to the matter.

* * *

This Policy was initially approved by the Board of Directors on June 18, 2026 and last updated on June 18, 2026.