Security Policy

October 15, 2025

The Board of Directors of Avangrid, Inc. ("Avangrid") oversees the management of Avangrid and its business with a view to enhance the long-term value of Avangrid. Avangrid is a wholly-owned subsidiary of Iberdrola, S.A. and a member of the group of companies controlled by Iberdrola, S.A. (the "Iberdrola Group"). The Board of Directors of Avangrid (the "Board of Directors") has approved this *Security Policy* (this "Policy") to assist in exercising its responsibilities to Avangrid and its Stakeholders (as defined in Avangrid's *Stakeholder Engagement Policy*). This Policy is subject to periodic review and modification by the Board of Directors from time to time. This Policy and Avangrid's certificate of incorporation, by-laws, corporate governance guidelines and other policies pertaining to corporate governance and regulatory compliance, risk, sustainable development, and social responsibility (collectively, the "Governance and Sustainability System") form the framework of governance of Avangrid and its subsidiaries (collectively, the "Avangrid Group"). Avangrid's Governance and Sustainability System is inspired by and based on a commitment to ethical principles, transparency, and leadership in the application of best practices in good governance and is designed to be a working structure for principled actions, effective decision-making and appropriate monitoring of both compliance and performance. This Policy aligns with and further develops the principles contained in the *Security Policy*, the *Purpose and Values of the Iberdrola Group*, and the *Ethical and Basic Principles of Governance and Sustainability of the Iberdrola Group* approved by the Board of Directors of Iberdrola, S.A. from time to time.

1. Scope of Application

This Policy applies to the Avangrid Group and reflects the basic principles established by the Iberdrola Group 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 informs the conduct and standards-setting implemented by the other companies of the Avangrid Group in this area in the exercise of their powers and in accordance with their autonomy.

For companies that do not form part of the Avangrid Gorup but in which Avangrid holds an interest, as well as for joint ventures, temporary joint ventures, and other entities in which it assumes management, Avangrid 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

This Policy seeks to protect Avangrid Group people, cyber, and physical assets (including critical infrastructure), information systems, knowledge, communications systems, and privacy of processed data, while at the same time ensuring that security-related actions fully conform to applicable laws and regulations and respect human rights.

3. Main Principles of Conduct

To achieve these goals, the Avangrid Group shall:

a) comply with all applicable laws and regulations regarding physical, cyber, and information security and Avangrid's Governance and Sustainability System;

b) ensure security personnel are qualified and properly trained in security best practices, including, without limitation, privacy, human rights, disclosure requirements, forensic investigation, and the Avangrid Governance and Sustainability System;

c) develop a preventive strategy and implement security programs that seek to protect critical infrastructure and maintain essential services provided by the Avangrid Group and minimize security risks, including, without limitation, operational-, reputational-, financial-, privacy-, and compliance-related risks;

d) implement requirements, practices, and protocols to identify, classify, manage and protect information assets and knowledge, including without limitation trade secrets and other business confidential information;

e) 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 from time to time;

f) actively engage Stakeholders, including customers and the supply chain, to mitigate identified security risks and to strengthen a coordinated response;

g) optimize resources by prioritizing critical security services while complying with all legal and/or regulatory mandates;

h) implement best practices in "threat and incident detection" and "response readiness" to mitigate risk and facilitate the appropriate escalation and reporting of incidents including incidents originating on the systems of our third-party service providers;

i) develop measures to prevent, neutralize, minimize, or restore harm caused by physical, cybersecurity, or hybrid security threats to normal business operations based on proportionality to potential risks and criticality and value of affected assets and services;

j) drive innovation and deployment of technology-related solutions in security and compliance to achieve best-in-class security programs, particularly integrating security into the software development lifecycle including secure coding practices, code reviews, automated vulnerability scanning, and secure baseline configurations for systems, with change management procedures for all modifications;

k) ensure appropriate disclosure controls and procedures are implemented with respect to reporting cybersecurity incidents, including incidents originating on the systems of our third-party services providers;

l) contribute to the promotion of a culture of security throughout the Avangrid Group through effective education, awareness and training programs;

m) promote the protection of Avangrid people, both in their workplace and in their professional travels;

n) promote the active fight against fraud and against attacks on the brand, image, and reputation of Avangrid and its people;

o) comply with applicable laws regarding the protection of personal data and with the provisions of the *Personal Data Privacy Policy*;

p) comply with the main principles of conduct established in the *Operational Resiliency Policy*;

q) monitor the current organizational and environmental context, as well as the evolution of events that permit the identification of the most significant security threats in order to anticipate their potential impact;

r) promote the integration of security in the management of Avangrid'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;

s) promote the secure use of assets to strengthen detection, prevention, defense, response and recovery capabilities against attacks or security incidents, ensuring the effectiveness thereof and paying particular attention to cybersecurity threats;

t) provide assistance and cooperation that may be requested by the relevant security institutions and bodies, including but not limited to regulators, security forces and bodies and governmental agencies, both domestic and international;

u) promote the identification of non-public information considered (or likely to be considered) as business secrets, as well as information whose unauthorized disclosure or alteration could cause serious damage to the interests of Avangrid;

v) empower its Corporate Security and Resilience Division to identify, implement and evaluate the actions necessary to prepare a strategic security program (the Program) in accordance with the principles and guidelines defined in this Policy and to develop internal rules, methodologies and procedures to ensure the appropriate implementation of the Program by the Avangrid Group;

w) endeavor to ensure effective compliance with the obligations imposed by the Governance and Sustainability System and by applicable security regulations at any time, always acting in accordance with applicable law and the provisions of the *Code of Business Conduct and Ethics* and the other rules of the Governance and Sustainability System;

x) enforce identity and access management practices, including at least privilege, role-based access control, multi-factor authentication, and periodic access reviews for critical systems and sensitive data;

y) conduct regular security assessments of third party vendors and service providers, including due diligence, ongoing monitoring, and inclusion of contractual security requirements such as breach notification timelines, data handling procedures, and audit rights;

z) define a security management model with a clear allocation of roles and responsibilities and effective coordination mechanisms that integrates security and proactive risk management into decision-making processes and as part of such model, maintain a formal incident response plan with defined roles, escalation procedures, and communication protocols, and conduct post-incident reviews to identify root causes, assess impact, and implement corrective actions;

aa) develop and regularly test business continuity and disaster recovery plans to ensure resilience of critical operations, defining and monitoring Recovery Time Objectives and Recovery Point Objectives for essential systems and services;

bb) implement centralized logging and monitoring through a Security Information and Event Management system, defining log retention periods and establishing procedures for regular log review and anomaly detection; and

cc) conduct regular vulnerability assessments and penetration testing to identify and remediate security weaknesses, and establish timelines for applying security patches based on severity and risk exposure.

4. Iberdrola Group Level Coordination

The Corporate Security and Resilience Division of Avangrid (or such division as assumes the powers thereof at any time) ("the Division"), through the Security, Resilience and Digital Technology Committee of Avangrid (or such committee as assumes the powers thereof at any time) (the "Committee"), shall coordinate with the Security, Resilience and Digital Technology Committee of Iberdrola, S.A. in order to seek an appropriate consolidated level of maturity and risks in security matters at the Iberdrola Group and Avangrid Group levels.

The Division, through the Committee, shall implement and supervise the Strategic Security Programme and related internal rules, methodologies, and procedures defined by Iberdrola, S.A.

5. Implementation and Monitoring

For the implementation and monitoring of the provisions of this Policy, the Board of Directors is assisted by the Division, which shall establish a procedure for regular monitoring and reporting to the governance bodies and which shall act in coordination with the appropriate corporate areas at the Iberdrola Group, in accordance with the Iberdrola Group's procedures for such purpose.

Regular evaluations and audits shall also be performed with internal or external auditors in order to verify compliance with this Policy.