

Corporate Security Policy

October 18, 2023

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 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 adopted this Corporate Security Policy (this “Policy”) to assist in exercising its responsibilities to Avangrid and its shareholders. 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.

1. Purpose

This Policy seeks to protect Avangrid Group people, cyber and physical assets and information systems while at the same time ensuring that security-related actions fully conform to applicable laws and regulations and respect human rights. This Policy contributes to the achievement of goal sixteen (Peace, Justice and Strong Institutions) of the Sustainable Development Goals (SDGs) adopted by the member states of the United Nations.

2. Principles

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, treat and protect information assets and knowledge, including without limitation trade secrets and other business confidential information;
- e) actively engage internal and external stakeholders to mitigate identified security risks;
- f) optimize resources by prioritizing critical security services while complying with all legal and/or regulatory mandates;
- g) 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;
- h) drive innovation and deployment of technology-related solutions in security and compliance to achieve best-in-class security programs;

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