CYBERSECURITY POLICY

OF SIEMENS GAMESA RENEWABLE ENERGY, S.A.

(Text approved by resolution of the Board of Directors dated September 16, 2021)

CYBERSECURITY POLICY

Pursuant to the provisions of section 529 *ter* of the Companies Act (*Ley de Sociedades de Capital*) and articles 33 of the By-Laws and 6 and 7.3 of the Regulations of the Board of Directors, the Board of Directors of Siemens Gamesa Renewable Energy, S.A. (hereinafter "**Siemens Gamesa**" or the "**Company**", and the group of companies of which Siemens Gamesa is the controlling company, the "**Siemens Gamesa Group**") hereby approves this Cybersecurity Policy of the Company and of the Siemens Gamesa Group.

The purpose of this policy is to establish the basic principles and the general framework for the control and management of the Cybersecurity risks faced by Siemens Gamesa.

The Cybersecurity framework contains the rules and regulations that set the organizational, procedural and technical requirements for protecting Siemens Gamesa's information assets as well as products, solutions and services from internal and external cyber threats and enhance the resilience of the businesses.

1. DEFINITIONS

- **Information Technology (IT):** Includes the full spectrum of information processing technology, including software, hardware, communications technology and related services, as well as the processes implemented for their support and management.
- **Operational Technology (OT):** Includes all hardware, software, processes and policies provided as part of the products, solutions and services, including: hardware and software systems such as DCS, PLC, SCADA, networked electronic sensing, and monitoring and diagnostic systems, as well as associated internal, human, network, software, machine or device interfaces used to provide control, safety, manufacturing, or remote operations functionality to continuous, batch, discrete, and other processes.
- **Cybersecurity:** The protection against harm caused by digital attacks against the confidentiality, integrity, availability, authenticity, reliability of information and assets in cyberspace. It includes and is not limited to the organization, collection of resources, processes, and structures to assure an end to end security across the full supply chain.

2. GENERAL OBJECTIVES

The general objective of the Cybersecurity Policy is to define and formalise general frameworks, which will help Siemens Gamesa to manage Cybersecurity risks in two domains (collectively referred to as the "Cybersecurity domains"):

- **IT Cybersecurity:** Siemens Gamesa considers information to be one of its most important assets to properly and efficiently provide its services and to comply with corporate objectives and laws, thus establishing IT Cybersecurity as a fundamental objective to ensure that the information processed is accurate, is only available to those who need it and is not disclosed without authorization.
- **OT Cybersecurity:** Siemens Gamesa is aware of the changes relating to cyber threats and the regulation of Operational Technology (OT), thus establishing OT Cybersecurity as a fundamental objective to support Siemens Gamesa customers with the protection of critical infrastructure by providing relevant product offerings supporting security

throughout the lifecycle of the asset, customized to meet strategy, internal legislative and regulatory requirements.

3. BASIC PRINCIPLES

The Cybersecurity policy is based on the following basic principles:

- Protect the company's critical information and technology assets from current cybersecurity threats.
- Strive to ensure Siemens Gamesa's Information Systems (IT) and Operational Systems (OT) are able to implement and maintain an appropriate level of security and resilience, based on relevant standards and the requirements of Siemens Gamesa customers and following a risk based approach.
- Promote the implementation of appropriate security and resilience mechanisms for the management of security risks through the supply chain.
- Raise awareness of Cybersecurity risks among employees, contractors and associates.
- Ensure employees, contractors and associates have the necessary knowledge, skills, experience and technological capabilities to support the Cybersecurity objectives of the company.
- Promote prevention, detection, reaction, analysis, recovery, response, research and coordination capabilities against Cybersecurity incidents.
- Provide procedures and tools to adapt quickly to the changing conditions of the technological environment and new threats.
- Ensure regulatory compliance related to the areas of Cybersecurity throughout the company.
- Collaborate with organizations, government agencies and major associations to contribute to the improvement of Cybersecurity at the international level.

4. ORGANIZATIONAL MODEL

4.1. Mandate and Governance

Siemens Gamesa's Board of Directors has decided to grant the oversight of Cybersecurity to the Chief Executive Officer (CEO) with the technical support of the Chief Cybersecurity Officer (CCSO). Oversight is provided through the Holistic Security Board, which is chaired by the CCSO.

The CCSO has the authority to give directives and guidance, including the control and coordination of Cybersecurity work within the domains of the IT Cybersecurity and OT Cybersecurity domains.

Likewise, in consultation with the specialised areas, the CCSO will define the regulations, strategies and binding technical standards required companywide for IT Cybersecurity and OT Cybersecurity as well as the processes, responsibilities, organization, interfaces and control

instruments needed to ensure the implementation and compatibility thereof throughout the company.

4.2. Holistic Security Board

The Holistic Security Board (HSB) is the inter-departmental board for the Siemens Gamesa areas (ON/OF/SE/IT/SEC/CO) that ensures close collaboration, skill sharing and a commitment to common security projects and initiatives and aligns the individual programs and organizations on topics of holistic security. The HSB has a mandate to:

- Ensure alignment across the individual governance functions.
- Decide on common proposals for Holistic Security projects and initiatives.
- Align and define the common Holistic Security strategy.

The board facilitates alignment on strategies and decisions for common security solutions from a holistic perspective and manages future security requirements of the business, partners or outside stakeholders, including overall Cybersecurity, legislative and global market perspectives.

4.3. Cybersecurity Governance Model

In order to support the general objectives of this policy, Siemens Gamesa implements a Cybersecurity Governance Model that is based on an appropriate definition and assignment of governance, management and operational duties and responsibilities, as well as procedures, rules, methodologies and support tools cross the Cybersecurity domains:

a) **Identify** risks, implementing structures and processes to maintain and develop security capabilities, which includes the following objectives:
   - Promote the organisation of Cybersecurity from a holistic viewpoint within the company, based on a continuous identification of risks and reduction of level of exposure, ensuring compliance with commitments to stakeholders (shareholders/regulators/customers/suppliers).
   - Standardise and maintain a risk-based Cybersecurity governance model, clear standards and supervised controls that optimise resource investment.

b) **Protect** against threats, improving measures to protect digital assets before the risk materialises, which contemplates the objective to develop security technologies applicable to the integral protection of the assets throughout their life-cycle, the critical nature thereof, and the progress of the threats.

c) **Detect** threats through the use of multiple intelligence sources in order to be able to proactively manage them, which contemplates the objective to increase the ability to detect internal or external threats with advanced technologies and processes.

d) **Respond** to Cybersecurity incidents, limiting the impact thereof on the company, which contemplates the objective to ensure the continuity of the services supported by the assets that shape the corporate technological and digital infrastructure and reduce the impact of incidents through corporate protocols.

e) **Recover** and restore any capabilities or services that were impaired due to a Cybersecurity event.