Cyber Security

In the era of digital transformation, cyber security takes on a key role in ensuring the normal operations of businesses, in a context characterized by increasingly sophisticated cyber threats and by laws and regulations requiring the adoption of rigorous measures to guarantee the security of data and IT infrastructures (especially critical ones), with heavy fines and criminal penalties in cases of non-compliance. In such a scenario, collaboration between the public and private sectors becomes essential to prevent cyber threats and to strengthen the protection and resilience of national critical infrastructures. To address these challenges, it is necessary to adopt a systemic and proactive approach, providing for the definition of a clear and shared strategy, the identification and continuous assessment of risks, the implementation of adequate preventive measures and response to cyber incidents, together with the creation of a culture of cyber security.

In particular, Enel is committed to:

- **Ensuring integrity and protection of data:** Enel, in order to ensure the rights and freedoms of all those involved are respected, adopts high standards of security and management of personal data for its employees, customers, and stakeholders. Enel has implemented policies and procedures to ensure the protection of personal data being processed and to enhance the security of our information systems and applications.

- **Monitoring and responding to information security threats**: Enel reserves the right to prevent incorrect and inappropriate uses of its assets and infrastructure through the implementation of accounting systems, reporting, financial control, and risk analysis and prevention, while adhering to applicable laws. As part of Cyber Security unit, Enel has its own CERT (Cyber Emergency Readiness Team), a global unit, active H24 7/7, whose mission is to protect Enel's employees and assets (instrumental to our business that could be compromised by cyber threats in IT/OT/IoT environments) by managing and responding, in a proactive manner, to cyber incidents, through sophisticated data monitoring and correlation systems.

- **Establishing individual responsibilities for information security for the entire workforce:** Every individual at Enel is responsible for the protection of the resources entrusted to them and has the duty to promptly inform the appropriate business units in the event of any threats or harmful incidents affecting Enel. The organization of Enel is tasked with clearly categorizing information based on the responsibility for specific processes, in order to standardize and raise awareness of the actions taken for the protection, processing, and dissemination of such information. Enel personnel must understand and implement the provisions outlined in company policies and procedures regarding information security in order to ensure its integrity, confidentiality, and availability.
- **Establishing information security requirements for third parties:** Enel requests that each stakeholder acts towards the Company in accordance with principles and rules inspired by a similar idea of ethical conduct. The performance of suppliers, in addition to ensuring the necessary quality standards, must go hand in hand with the commitment to adopt best practices in terms of, among all the others, respect for by design and by default privacy and information security.
- **Continuously improving information security systems:** Enel ensures continuous improvement of information security systems through a structured approach based on systematic risk assessments, advanced technological tools and solutions to ensure adequate protection of company resources against cyber threats, regular review of security policies and procedures, and technical security controls to identify any vulnerabilities. Finally, awareness-raising and continuous training activities are promoted, with mandatory content, for all Enel employees, to develop a culture of cyber security.

These principles are more extensively described in **Enel's internal Cyber Security policies**, which also disclose the operating procedures that guarantee the implementation of the actions needed to achieve Enel's commitments.

Furthermore, **it's crucial that any cyber security issue** (e.g., theft or loss of Company devices; suspected fraud, suspected cyber-attacks, data leakage and credential theft) **is promptly reported to the relevant channel** in order to activate as soon as possible the remediation and preventive activities. The role of employees is of the utmost importance for efficient and effective detection and reporting of cyber security issues.

Internal technical security controls are constantly carried out, also with the support of appropriately selected independent external suppliers, in all the Group's environments (IT, OT and IoT) in order to identify any vulnerabilities and mitigate the associated risks.

Enel has seized on the growing interest in the market for **ISO 27001** Information Security Certification. Indeed, it has initiated certification paths to this ISO standard by achieving it already for several Legal Entities. This important achievement certifies the information security management system for core processes, with a view to delivering trusted products and services to customers. Given the Group's complexity, beginning from the experiences gained in leading the path to certification to ISO 27001 standard of the Group's various Legal Entities, a digital management tool was designed that makes the achievement of certification efficient, repeatable, scalable and sustainable.

In addition, Enel cyber management processes are examined through the ISAE3402 Type 2 Report, released annually by the **external auditor KPMG**, which evaluates in detail the maturity, design, implementation, and operating effectiveness of our controls.

Finally, the company has an internal procedure that implements a **comprehensive and structured approach to ensure business continuity**. This is achieved through the IT Service Continuity Management (ITSCM) process, which includes both proactive and reactive strategies to mitigate and recover from severe IT service outages. A key component of this process is the Disaster Recovery Plan (DRP) test, scheduled by the Service Continuity Manager that defines the annual test plans and verify their effectiveness, while Service Continuity Agents support execution and continuous improvement. These tests outcomes are monitored and reported to executive management to maintain readiness and resilience.