group elecnor

Policy on Information Security and Cybersecurity

INDEX

1. INTRODUCTION 3
2. DEFINITIONS 3
3. OBJECT 4
4. SCOPE OF APPLICATION 5
5. GENERAL PRINCIPLES 5
6. BASIC NETWORK AND INFORMATION SYSTEMS SECURITY REQUIREMENTS 6
7. GOBERNANCE 8
   - 7.1. The Board of Directors and its Committees 8
   - 7.2. Information Security and Artificial Intelligence Committee 8
   - 7.2.1. Principles of action 8
   - 7.2.2. Composition and functions of the Committee 9
8. MONITORING, INTERPRETATION, REVIEW AND UPDATING 10
   - 8.1. Monitoring 10
   - 8.2. Interpretation 11
   - 8.3. Review and updating 11
9. DISEMINATION 11
10. ENTRY INTO FORCE **Error! Bookmark not defined.**

1. INTRODUCTION

As a listed company, the Board of Directors of Elecnor, S.A. ("**Elecnor Holding**" or the "**Company**") is legally vested with the non-delegable power to determine the general policies and strategies of the Company and of the Group of which it is the controlling entity ("**Elecnor Group**" or "**Group**"), a power also set forth in the Corporate Governance Policy and in the Regulations of the Board of Directors.

This Information Security and Cybersecurity Policy (the "**Policy**") assumes the commitment of Elecnor Holding and the companies forming part of the Group to guarantee the security of the networks and information systems on which the different business processes are based, so as to reinforce its Digital Operational Resilience, aligning its practices with the applicable regulations in force, as well as with its corporate values.

In this regard, Elecnor Holding is committed to developing the Group's maximum Cybersecurity capabilities, thereby reducing the threats to the network and information systems used to provide essential services in key sectors, so that its products and services generate sustainable benefits and are aligned with the highest ethical and legal standards.

This Policy forms part of Elecnor Holding's security strategy as the parent company of the Group, with the aim of ensuring that the use of networks and information systems is consistent with respect for the right of all interested parties to the highest standards of Cybersecurity and privacy, taking into account the Group's activities and structure and, in particular, its presence in critical sectors such as infrastructure development and renewable energy.

Pursuant to the aforementioned objectives, the Board of Directors of the Company has approved this Policy, which applies to the Group and which forms part of the Company's Corporate Governance System.

2. DEFINITIONS

For the purposes of this Policy, the following definitions shall be taken into consideration:

- **Risk analysis:** systematic process aimed at identifying, analysing and assessing risks that may affect information in any of its security dimensions.
- **Information Security and Artificial Intelligence Committee:** an interdisciplinary committee with supervisory and regulatory responsibilities for adopting any resolution with relevance in matters of Cybersecurity and Artificial Intelligence at Elecnor Holding and its Group, with the aim of ensuring that the measures for managing information security risks are suitable and that any activity of the organisation that has special relevance is aligned with the values and policies that are projected on the Elecnor Group (the "Committee").
- **Cybersecurity:** all activities necessary to ensure the security of information, the protection of networks and information systems, the users of such systems and other persons affected by cyber-threats.
- **Personal Data:** any information about an identified or identifiable natural person. This includes any data that, directly or indirectly, can be used to identify an individual such as names, photographs, email addresses, bank details, social media information, location, medical information or computer IP address, among others. Personal Data are protected by various legislations and good practices for their collection, processing and storage must be followed in order to respect the privacy rights of the individuals involved.

- **Risk Management:** coordinated activities to manage and control identified Cybersecurity risks in the Elecnor Group.
- **Incident Management:** set of measures and procedures aimed at preventing, detecting, analysing and limiting a Cybersecurity Incident, as well as resolving it and incorporating performance assessment measures that make it possible to know the quality of the protection system and detect trends before they become relevant problems.
- **Cybersecurity Incident (or Cyberincident):** an unexpected or undesired event that may compromise the availability, authenticity, traceability, integrity or confidentiality of data stored, transmitted or processed, or the services offered by or accessible through network and information systems.
- **Professional:** members of the Elecnor Group's management bodies, executives, workers, employees, collaborators, trainees and interns, regardless of the legal status of their employment or service relationship, their hierarchical level, their geographical or functional location and the Group company for which they provide their services.
- **Manager:** directors, middle management or any other person with decision-making responsibility in terms of Cybersecurity.
- **Digital Operational Resilience:** the entity's ability to build, secure and review its operational integrity and reliability by ensuring, directly or indirectly, through the use of services provided by third party information and communications technology ("ICT") service providers, the full range of ICT-related capabilities necessary to preserve the security of the networks and information systems used by the Elecnor Group that underpin the continued provision of services and their quality, including in the event of disruptions.
- **Data Processing:** any operation or set of operations which is performed upon Personal Data, or sets of Personal Data, by automated processes or otherwise, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, storage, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
- **Vulnerability:** any weakness, susceptibility or defect in an asset, system, process or control that can be exploited.

Unless expressly provided otherwise in any section of this Policy, definitions in the singular include the plural and vice versa.

3. OBJECT

The purpose of this Policy and the basic principles set forth herein is to enable the Group to deploy the Cybersecurity strategies, procedures, technologies and standards necessary to develop an appropriate operational and control framework, in line with the business objectives and the security of the Elecnor Group's data, networks and information systems.

This is done in accordance with the applicable regulations and taking into account the various stakeholders.

4. SCOPE OF APPLICATION

This Policy is applicable to all divisions and subsidiaries that make up the Elecnor Group, as well as to suppliers and partners that provide services for or relate to the Group.

Without prejudice to the provisions of the preceding paragraph, in those investee companies in which this Policy does not apply, the Company shall promote as far as possible, through its representatives on their management bodies, the alignment of their own policies with those of the Company, within the framework of respect for the decision-making autonomy of the investee companies.

In addition, this Policy shall also be applicable, as applicable, to temporary joint ventures (UTEs), joint ventures, and other equivalent associations, whether domestic or foreign, when any of the companies that make up the Elecnor Group have control over their management and always within the legally established limits.

It is the responsibility of all Professionals and subjects bound by the Policy to read and understand the contents of the Policy, as well as to observe and comply with its guidelines, principles and processes in the performance of their work, insofar as understanding and adherence to the definitions and principles set forth therein is essential to ensure that the Cybersecurity objectives are achieved throughout the Elecnor Group.

5. GENERAL PRINCIPLES

The Elecnor Group understands Cybersecurity as a fundamental element for protecting business assets, considering it to be an integral process based on risk management and control in order to achieve its objectives and fulfil its mission.

In this regard, Elecnor Holding undertakes to provide the different areas of the Group with the necessary technical, human, material and organisational resources to guarantee adequate security management of the Elecnor Group's networks and information systems.

To this end, the Elecnor Group shall guide its actions in accordance with the following principles:

I. **Define, develop and maintain an integrated framework of controls:** The Elecnor Group shall promote the development of an integrated framework of technical, legal and management controls for Cybersecurity in accordance with its objectives and strategies, and which guarantee compliance with applicable legal, regulatory and contractual requirements at all times.

II. **Promote a culture of Cybersecurity:** the Elecnor Group undertakes to actively promote a "culture of Cybersecurity" among all its Professionals and other parties bound by this Policy, and therefore internally and among its customers and suppliers. In particular, it will promote the integration of this Cybersecurity culture in all areas of the Group as the basis of its activities and in relation to the products and services that the Elecnor Group offers its customers.

III. **Permanently manage security:** the Elecnor Group is committed to protecting the security of its networks and information systems, designing robust security measures aligned with the needs of the different stakeholders, as well as with the applicable regulations in force in this area, for which purpose the Elecnor Group shall approve the specific policies and procedures that will develop the basic security principles and requirements established in this Policy. The purpose of all of the above is to identify risks and correct all Vulnerabilities detected in order to prevent the occurrence of Incidents that compromise the Elecnor Group's business continuity.

IV. **Proactively protect information assets and ensure resilience:** the Elecnor Group shall actively undertake the commitment to safeguard the established levels of confidentiality, availability, authenticity, traceability and integrity of the Group's information assets, as well as to ensure the Elecnor Group's Digital Operational Resilience.

V. **Continuously improve risk management:** the Elecnor Group pursues constant progress in all processes linked to risk management in the area of Cybersecurity, as well as controls for the security of networks and information systems, analysing vulnerabilities, cyber-threats and Cybersecurity incidents to identify their causes and the necessary improvements in the Elecnor Group's operations and business continuity.

6. BASIC NETWORK AND INFORMATION SYSTEMS SECURITY REQUIREMENTS

All Cybersecurity documentation developed in execution of the requirements established in this section is managed, structured and maintained in accordance with the documented policies and procedures developed by the Elecnor Group, taking into account the national and international regulations and standards applicable in each case.

In order to carry out the day-to-day management of Cybersecurity, all Elecnor Group Professionals and other parties bound by this Policy must know, understand and, where appropriate, always act in accordance with the following basic network and information system security requirements:

Prevention, detection, response and preservation

Processes, policies and procedures for the prevention and Management of Cybersecurity Incidents shall be established, documented and implemented to ensure that they are known by all Elecnor Group Professionals and other parties bound by this Policy, in order to detect, analyse, contain or respond to Incidents, recover from them, document them and notify them in a timely manner.

Risk analysis and management

Risk assessments shall be conducted and documented on the basis of continuous monitoring and periodic reassessment of risks and, based on the results, a risk treatment plan shall be established, implemented and supervised.

Differentiation of responsibilities

The functions and responsibilities in Cybersecurity matters shall be clearly established, so that all Elecnor Group Professionals and other parties bound by this Policy are aware of them and understand them.

Organisation and implementation of the Cybersecurity process

An appropriate risk management framework shall be established and maintained to identify and deal with the risks posed to the security of networks and information systems.

Management and training

The objective shall be to ensure that all Professionals and, where appropriate, other persons bound by this Policy understand and are committed to their Cybersecurity responsibilities by conducting the necessary background checks and requirements for their role, responsibilities and authorisations.

In turn, awareness and training programmes will be carried out so that all Professionals, including members of management bodies, as well as direct suppliers and service providers, and other subjects bound by this Policy, are aware of the risks, are informed of the importance of Cybersecurity and apply cyber hygiene practices.

Authorisation and access control

Logical and physical access control procedures and policies shall be established, documented and implemented for access to its network and information systems, based on business requirements and the security requirements of the network and information systems, managing access rights to same, as well as to privileged and system administration accounts that are enabled, based on the principle of least privilege.

Protection of facilities

Controls and measures shall be adopted to prevent the loss, damage or compromise of facilities where network and information systems and other assets are located, as well as to prevent the disruption of their operations due to the failure and interruption of support services.

Information system integrity and updating

Processes shall be established and implemented to manage and update both the risks and the content of the associated Management System. In particular, requirements shall be established for security updates applicable to the Management System during its lifetime.

Protection of information in storage and in transit

Appropriate controls shall be established, implemented and applied to ensure the appropriate and effective use of cryptography to protect the confidentiality, authenticity and integrity of information, both stored and in transit, in line with the asset classification and the results of the risk assessment performed.

Prevention against other interconnected information systems

Measures shall be taken to segment systems into networks or zones (both in-house and those provided by third parties) in accordance with the results of the risk assessment.

Recording of activity and detection of malicious code

Procedures shall be established and tools shall be used to monitor and record activities on the Elecnor Group's networks and information systems in order to detect events that may be considered incidents and respond accordingly to mitigate their impact, ensuring that the results of these assessments are taken into consideration in the learning and improvement processes.

Business continuity

A business continuity and disaster recovery plan shall be established and maintained to be applied in the event of Incidents, establishing, among other issues, activation conditions, key contacts, roles and responsibilities, and necessary resources, in order to ensure that operations are re-established in accordance with said plan, as well as business continuity in the Elecnor Group.

Supply chain security

Supply chain security procedures and policies governing relations with direct suppliers and service providers shall be established, implemented and applied, and the appropriate measures and controls shall be established in order to

mitigate the risks detected arising from these third parties for the security of the Elecnor Group's networks and information systems.

7. GOBERNANCE

Cybersecurity governance in the Elecnor Group is essential both to guarantee decision-making based on the real risk of the materialisation of Cybersecurity threats in the Group, and for the continuity of business operations, and this Policy is a fundamental tool for establishing appropriate Cybersecurity governance bases.

7.1. The Board of Directors and its Committees

The Board of Directors of Elecnor Holding is responsible for establishing the strategy and management guidelines of the Elecnor Group regarding the Cybersecurity, through this Policy and, if applicable, other corporate rules approved to implement it.

In turn, the Appointments, Remunerations and Sustainability Committee, in accordance with its supervisory and control functions, is responsible for ensuring the implementation and development of this Policy and the measures adopted in application thereof, as well as for reviewing and, if appropriate, proposing to the Board of Directors the updating of this Policy.

The Audit Committee is responsible for supervising the effectiveness of the control and risk management systems related to the Cybersecurity of the Company and its Group, as well as supervising the reporting process of such risks.

In order to perform their supervisory duties, both the Appointments, Remunerations and Sustainability Committee and the Audit Committee shall periodically receive from the Information Security and Artificial Intelligence Committee, through the Head of Information Security, information on the actions and management carried out by the Committee and the Head of Information Security and Artificial Intelligence, within the scope of their respective competences.

7.2. Information Security and Artificial Intelligence Committee

7.2.1. Principles of action

Elecnor Holding, through the Committee, shall observe and promote the following principles in the Elecnor Group in relation to the governance of Cybersecurity:

a) Principle of strategic alignment and vision of the future

Cybersecurity is understood as another part of the business, constituting a tool that helps the Elecnor Group to achieve its objectives, aligned with the Group's mission and vision.

In this regard, the Committee shall promote a holistic approach in the Elecnor Group so that Cybersecurity is not seen as an obstacle, but as part of a broader whole that is suitable for the development of its business.

b) Principle of ethics and compliance

Cybersecurity governance includes not only compliance with applicable regulations, but also good security practices and the ethical use of the Group's resources.

In order to encourage ethical and responsible action, the Committee shall promote alignment with best practices in this area, among others, in the management of Cybersecurity risks, both within the Elecnor Group and in each of the markets in which it operates and in its relationship with the various stakeholders.

c) Reliability principle

The networks and information systems used in the Elecnor Group shall be robust and function reliably, so that they are capable of supporting business operations continuously and effectively.

The Committee shall ensure the implementation of the principle of reliability in information systems and networks, as well as business continuity in the Elecnor Group, in order to foster the trust of customers and other stakeholders.

d) Principle of responsibility and accountability

Cybersecurity is a complex and transversal discipline that affects all of an organisation's activities. This is why it requires adequate leadership and a structure that, in order to be properly implemented and managed, must be made up of professionals with appropriate training and experience.

The Committee assumes the function of defining, promoting and controlling Cybersecurity and participates in decision-making and strategies in this area. The Committee must also ensure that Cybersecurity-related risks are reported appropriately and at the appropriate levels, as well as the necessary mitigation and control mechanisms.

e) Principle of security and resilience

Networks and information systems must operate in a secure and digitally resilient manner.

One of the goals pursued by Cybersecurity is to ensure the continuity of the Elecnor Group's operational capacity in the interest of the Group and the stakeholders that may be affected by its activities (Digital Operational Resilience), and therefore capacities must be developed to contain or recover from Cyber Incidents.

To this end, the Committee shall promote the approval of procedures and policies that ensure the effective management of Cyber Incidents, identifying the operational groups in charge of their management (both at technical and tactical level, as well as strategic) to minimise the impact on the business and to ensure regulatory compliance and adequate internal or external communication, as well as having capabilities that allow the Group to be resilient to ensure the continuity of operations and the full recovery of services within an appropriate period of time to be determined in the business continuity plan.

7.2.2. Composition and functions of the Committee

The members of the Committee, as well as the Information Security Manager, shall be appointed by the Board of Directors at the proposal of the Appointments, Remunerations and Sustainability Committee. The Committee shall act as an internal support body for the Head of Information Security.

In addition to any other functions attributed or assigned to it by virtue of the internal regulations in force at any given time, the Committee shall be responsible for the following:

- Regularly report to management and different areas in relation to security and control measures adopted in terms of Cybersecurity.

- Address Cybersecurity issues raised by management and the different departments of Elecnor Holding and its Group.
- Develop and update the strategy of Elecnor Holding and its Group with regard to information security.
- Coordinate the efforts of the different areas and subsidiaries in the area of Cybersecurity to ensure that efforts are consistent and are aligned with the agreed strategy in this area and to avoid duplication.
- Develop, approve and promote training and qualification courses and requirements for operators from an information security perspective.
- Monitor the main residual risks assumed by the Group and recommend relevant possible actions.
- Monitor the performance of the security Incident Management processes and recommend relevant possible actions. In particular, to ensure the coordination of the different security areas involved in Cybersecurity Incident management:
- Promote the performance of periodic audits to verify compliance with the organisation's obligations in security matters.
- Approve Cybersecurity improvement plans, as well as ensure coordination of the different plans that may be carried out in different areas and subsidiaries of the Group.
- Prioritise security actions when resources are limited.
- Ensure that Cybersecurity is taken into account in all ICT projects from their initial specification to their implementation. In particular, it should ensure the creation and use of cross-cutting services that reduce duplication and support the seamless operation of all ICT systems.
- Resolve any conflicts of responsibility relating to information security and Cybersecurity that may arise between the different Managers or between different areas of Elecnor Holding and its Group.
- Propose to the Appointments, Remunerations and Sustainability Committee such updates to this Policy as it deems necessary or appropriate.
- Approve internal procedures, rules or protocols aimed at the development and implementation of this Policy at Elecnor Holding and at the Group level.
- Ensure that the necessary human and material resources are available to carry out the functions entrusted to it.

8. MONITORING, INTERPRETATION, REVIEW AND UPDATING

8.1. Monitoring

Compliance with this Policy shall be supervised by the Information Security and Artificial Intelligence Committee. Periodic audit and review mechanisms shall be established to ensure that all Cybersecurity measures established in the Group comply with the requirements established in this Policy and in the applicable regulations.

In the event that a problem arises, or an incident is detected that may affect the operation or security of the information systems, the Committee must be notified immediately, through the channels provided for such purposes and which shall be determined in the internal Procedures.

The results of the Vulnerability management process shall be documented as a metric.

Failure to comply with this Policy may entail legal liabilities of various kinds according to the legislation in force, entitling Elecnor Holding, if deemed necessary, to take the appropriate legal action.

8.2. Interpretation

The contact body for any queries or questions regarding the interpretation and execution of this Policy shall be the Information Security and Artificial Intelligence Committee, which may be contacted through the channels provided for this purpose.

8.3. Review and updating

This Policy shall be reviewed and, where appropriate, updated at least once a year, and whenever significant Incidents or major changes in operations or risks occur. The results of these reviews shall be documented.

The modification and updating of this Policy shall be approved by the Board of Directors of Elecnor Holding, following a report from the Appointments, Remuneration and Sustainability Committee, and shall be disseminated to Professionals through the usual channels.

9. DISEMINATION

This Policy and any amendments thereto shall be published on the Company's corporate website and shall be kept permanently updated, with the consequent knowledge and assumption of its full content by Elecnor Group Professionals and other parties bound by this Policy.

Notwithstanding the foregoing, Elecnor Holding shall carry out communication, training and awareness-raising actions for the understanding and implementation of this Policy, as well as its updates.

In any case, Professionals and Users are recommended to periodically access the content of this Policy through the available channels for a better understanding of the same, and it should be taken into account that their ignorance of all or part of its content does not exempt them from compliance.

10. ENTRY INTO FORCE

This Policy was approved by the Board of Directors of Elecnor Holding at its meeting held on 27 November 2024, coming into force on 1 January 2025.