Global Information

Security Policy

TABLE OF CONTENTS

1. Background

The Board of Directors of Cellnex Telecom, S.A. (hereinafter, "Cellnex Telecom", the "Company" or the "Organization") has, among its functions as the highest governing body, that of determining the Company's general policies. In exercising this function, it has established this Global Information Security Policy for all companies in the Cellnex Group.

This policy is implemented through an Information Security Management System (hereinafter, “ISMS”) designed to ensure the systematic management of information security risks, the protection of assets, and the continuous improvement of security controls in a unified and structured manner.

2. Frame of reference

This policy provides guidelines and principles to ensure the proper implementation and management of **security** within the framework of the **Information Security Management** System and the requirements of the ISO standards under which the Company is certified in terms of **Information Security.**

The Policy is aligned with international reference standards and voluntary initiatives to which Cellnex Telecom adheres, including the following:

- ISO 27001 standard.
- ISO 22301 standard.
- Esquema Nacional de Seguridad (ENS)
- NIST (National Institute of Standards and Technology)

The Policy supports and should be interpreted in conjunction with, among others, the following corporate policies:

- Sustainability Policy
- Occupational Health and Safety Policy
- Environment and Climate Change Policy
- Energy Policy
- Quality and Integrated Management System Policy
- Anti-Bribery, Gifts and Hospitality
- Global Risk Management Policy
- Stakeholder Engagement Policy
- Procurement Polic
- Human Rights Policy

3. Purpose and scope

Purpose: This policy sets out the guidelines and lines of action for Information Security that will govern how **Cellnex Telecom** will manage and protect its information and service, as well as its communication to stakeholders and implementation in all companies and functional areas within the Cellnex Group.

Scope: This policy applies to all the companies that make up the **Cellnex Telecom** group and is the responsibility of its entire team. It also applies to all individuals, regardless of their Company affiliation, who operate Company resources to conduct Company business or interact with internal networks and business systems, whether owned or leased by the Company, the employee, country within the **Cellnex Telecom** group is responsible for guaranteeing compliance with this policy and implementing it in accordance with local laws and regulations.

This policy is aligned with and complementary to the rest of Cellnex Telecom's corporate policies and internal regulations.

4. Basic principles

Information is a critical asset for **Cellnex Telecom**, and it is necessary to guarantee the confidentiality, integrity, availability, authenticity and traceability of the same in accordance with the recognized standards of management of Information Security in the provision of the service as operator of Telecommunications infrastructures to Operators, Broadcasters, Public Administrations and Corporations.

Cellnex Telecom is committed to protecting people, facilities, businesses, and brand through the following principles:

Protecting Information Assets:

Steps are taken to identify and prevent unauthorized access, modification, disclosure, or destruction of information assets, ensuring that they are used only for purposes approved by Management.

Resource Allocation:

The **Cellnex Telecom** team has the material resources, continuous training in technologies and skills, as well as development processes to detect individual needs in accordance with this policy and to achieve business objectives.

Team Responsibility:

Involvement in the protection of these assets and the implementation and maintenance of appropriate security controls is the responsibility of both management and the entire **Cellnex Telecom** team.

Continuous improvement:

Operating within a Management System guided by ISO 27001 standards, focusing on people management, process management, and continuous improvement to ensure effectiveness and efficiency.

5. Commitments and strategic lines

Information Security Commitment

Information is one of the most valuable assets for Cellnex, and protecting it is crucial. The protection of information follows the principles of **confidentiality**, **integrity**, **availability**, **authenticity** and **traceability**, ensuring that information is only accessible to authorized individuals, safeguarded against unauthorized changes, and available when needed. The organization is committed to implementing information security measures.

The entire security model is centralized within the **Corporate Security** department, responsible for defining general guidelines for local compliance in each country. Each country has an Information Security representative, with the **Global SOC** in Spain with CSIRT capabilities providing support to all business units.

Risk Management and Security by Design

The organization is dedicated to managing **information security risks** through a **risk-based approach**. These risks are identified, evaluated, and treated by implementing appropriate controls. Furthermore, **security by design and by default** is applied in all business processes, services, and technologies, ensuring that security is an integral part of every development from its inception.

Human Resource Security and Training

Understanding that human resources are pivotal to information security:

Raise Awareness:

Provide continuous training to employees and collaborators to protect information effectively.

Educate Employees:

Ensure that employees are aware of security expectations upon joining and receive ongoing education to detect and respond to potential threats.

Promote Ethical Behavior:

Embed information security into daily activities and encourage staff to act ethically and responsibly regarding security.

Asset and Access Control Management

Asset management is a priority, with Cellnex Telecom implementing:

Asset Classification and Inventory:

Ensuring that all information assets are classified and adequately protected according to their sensitivity and importance, following internal classification guidelines and data protection regulations.

Access Control Mechanisms:

Access to these assets is controlled through **strict access control mechanisms** that only allow authorized personnel to interact with sensitive information.

Cryptographic Protection:

Cryptographic techniques are used where necessary to protect the integrity and confidentiality of critical data.

Security Audits:

Regular audits assess compliance and identify areas for improvement.

Vulnerability Assessments and Penetration Testing:

Periodic scans and tests detect and correct security.

Incident Reporting and Management:

Cellnex Telecom's internal rules and standards, together with formal incident reporting and management processes, ensure timely identification, reporting, and remediation of security incidents and any irregularities in policy compliance. All exceptions to this Policy must be thoroughly documented, follow established procedures, and receive explicit approval from the Board of Directors of Cellnex Telecom, S.A.

Metrics and Reporting:

Continuous monitoring of systems and KPIs related to Operational Risk Control (ORC).

Supplier Relationships and Third-Party Security

Managing information security in collaboration with third parties is essential. The organization implements third-party risk management practices to ensure that external collaborators and suppliers adhere to the same security standards.

Risk Identification and Analysis:

Identifying and analyzing security risks associated with third parties throughout the supplier relationship lifecycle.

Control Implementation:

Enforcing security controls and conducting regular assessments to ensure third parties maintain compliance with **Cellnex Telecom**'s security requirements.

Contractual Obligations:

Ensuring that security requirements, including specific Service Level Agreements (SLAs) for information security, are clearly defined and embedded within contractual agreements with third parties.

Compliance with Legal and Regulatory Standards

Compliance with **legal, regulatory, and contractual requirements** is fundamental. The organization is committed to adhering to the laws and regulations within its scope including, among others, GDPR compliance. This ensures that information security practices align with current and future legal requirements. The DPO team collaborates closely with Global Security to ensure GDPR compliance. Regular audits and assessments are conducted to ensure ongoing compliance.

Incident and Business Continuity Management

Cellnex Telecom maintains robust processes to manage incidents and ensure business continuity:

Incident Management:

Implementing a well-defined process for identifying, reporting, and addressing information security incidents promptly. This includes leveraging a CSIRT team to handle incidents 24/7 and utilizing DFIR capabilities for enhanced incident detection and response.

Business Continuity Planning:

Maintaining comprehensive business continuity plans that outline procedures for maintaining critical operations during and after significant incidents. This includes disaster recovery plans (DRPs) tailored to identified contingency scenarios.

Physical and environmental security

Protect **Cellnex Telecom**'s physical assets and the sensitive information they manage by preventing unauthorized access through established security perimeters and deploying security systems like intrusion alarms and access controls where necessary.

System acquisition, development and maintenance

To guarantee security by default, starting from design in applications developed internally by **Cellnex Telecom** during the software development or implementation stage.

6. Responsibilities

Board of Directors of Cellnex Telecom S.A. and CEO:

Ensure the provision of necessary resources for the execution of security processes and integrate information security into organizational decision-making. This leadership commitment guarantees that information security is prioritized throughout the organization and that all employees understand their roles and responsibilities in maintaining security standards.

Director of Information Security (CISO):

Responsible for the operational management of information security, including the production and maintenance of security standards included in the Information Security Framework as part of the Information Security Management System, the controls to enforce the standards and the provision of advice and guidance on its implementation and maintenance.

CSIRT Security team:

Handles all information security incidents (noc.security@cellnextelecom.com) and all incidents involving personal data to the GDPR Data Privacy Team (personaldata@cellnextelecom.com).

Employees, Contractors, Consultants, and Temporary Staff:

Are fully responsible for adhering to this policy and protecting information assets throughout all stages of information handling.

Country Managing Directors and Country Security Representatives:

Implement the policy within their areas of responsibility and ensure their staff's adherence to the policy.

Information Security Office:

Manages day-to-day information security operations, including monitoring, incident response, and compliance activities.

7. Internal regulatory development

The **Global Security** Department at the Group level, and, where applicable, the corresponding local areas shall be responsible for developing the principles contained in this policy through the preparation and approval of the necessary internal regulations, in accordance with the procedures established for this purpose.

8. Approval, review, control and communication of the Policy

Approval	On the prior recommendation of the Audit and Risk Management Committee, the Board of Directors of Cellnex Telecom, S.A. approved the update of this Global Information Security Policy on 25/03/2026.
Review	The Global Security department will review and propose updates to this Policy whenever deemed necessary or when significant changes occur that may affect its content or application. These reviews ensure that Cellnex remains compliant with actual laws and regulations.
Control	The Global Security Department is responsible for ensuring compliance with this Policy, in collaboration with all corporate and business units within the company. Each area actively contributes to the application of the established principles and commitments, ensuring that operational and strategic practices are aligned with Cellnex Telecom's security objectives.
Communication	The Global Security Department undertakes to periodically communicate its progress in complying with this policy to all internal and external stakeholders, in line with this principle of transparency. It will also promote awareness and compliance with this Policy, which will be permanently available on the company's website.

9. Changes Control

Version	Elaborate by	Validity
1	Global Security	05/04/2019
2	Global Security + Review by Compliance	25/03/2026