Information Security Policy

INDEX

1. 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 services, as well as its communication to stakeholders and implementation in all companies and functional areas of the Group.

Scope: This policy applies to all the companies that make up the **Cellnex Telecom** group, and is the responsibility of its entire team. Stakeholders should be aware of and comply with this policy in accordance with their role when dealing with company or customer information.

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

2. Basic principles

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

Steps are taken to identify and protect Information assets from unauthorised access, modification, communication or destruction, whether intentional or incidental, ensuring that they are used only for purposes approved by Management.

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 in order to achieve the business objectives.

Involvement in the protection of these assets and the implementation and maintenance of

appropriate security controls is the responsibility of the entire Cellnex Telecom team.

Compliance with legal and regulatory standards applicable at all levels, the will to adapt to future standards, as well as customer and social requirements, require a commitment and responsibility from all.

Continuous improvement is developed within the framework of a Management System, which Management undertakes to lead in accordance with the ISO 27001 standard, and which applies to all the Group's Business Units. All of this is based on people management, process management and continuous improvement; guaranteeing its effectiveness and efficiency.

3. Strategic lines and commitments

Based on the above basic principles, **Cellnex Telecom** defines the following strategic areas of action:

Information Security Policy: to provide the necessary support and management for information security in accordance with legal requirements. **Cellnex Telecom's** policy is aligned with the organisation's objectives, which guarantees its commitment to Information Security.

Organization of Information Security: to establish an organisational framework of reference by defining roles and responsibilities of Information Security that allow the definition and implementation of a Risk Treatment Plan and the evaluation of its effectiveness to reduce the identified risks.

Human Resources Security: to inform and raise awareness among personnel as soon as they join the group and on a continuous basis regardless of their activity situation, about the security measures that affect the performance of their functions and the expectations placed on them in terms of security and confidentiality issues. It includes the establishment of the necessary Information Security measures prior to recruitment and at the cessation or change of job.

Asset Management: to adequately protect the assets of the organisation according to their sensitivity.

Access Control: to ensure access to information systems is only provided to authorised personnel.

Cryptography: using cryptographic systems and techniques for the protection of information based on risk analysis, in order to ensure adequate protection of its confidentiality and integrity.

Physical and environmental security: protect **Cellnex Telecom's** physical assets and the sensitive information they manage by establishing security perimeters and protected areas.

Operations Security: to ensure the administration and management of the platforms and services linked to the processing of information.

Communications Security Domain: to ensure the protection of the information communicated by telematic networks and the protection of the supporting infrastructure.

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.

Supplier Relationships: to implement and maintain the appropriate level of information security

and delivery of contracted services in line with third party service delivery agreements.

Information Security incident management: to ensure that information security events and vulnerabilities associated with information systems are communicated in such a way that corrective actions are applied in the shortest possible time.

Business Continuity Management: to ensure the continuity of Business processes through the application of controls that prevent or minimise the materialisation of critical impact risks.

Compliance: to guarantee compliance with legal security requirements applied to the design, operation, use and management of information systems.

4. Monitoring and control

Management undertakes to review the Information Security Policy periodically, adapting it to new organisational, environmental or market requirements that may arise, and to communicate it to the Organization and make it available to interested parties at all times.

The Information Security Objectives are consistent with this policy and are aligned with **Cellnex Telecom's** process model, and are reviewed annually by Management and updated according to their evolution and environment.

5. Changes Control

Version	Elaborate by	Department	Validity	Changes
1	Global Security	Global Security	05/04/2019	Initial version