EUSKALTEL GROUP - INFORMATION SECURITY POLICY

Contents

Free translation from the original in Spanish. In the event of discrepancy, the Spanish-language version prevails

1. PURPOSE

The purpose of this Information Security Policy is to establish the guidelines for managing information security that the Euskaltel Group wishes to implement to ensure that access, use and custody of its information assets comply with the legal and regulatory requirements established by and for the Euskaltel Group with regards to the integrity, availability, authenticity, traceability and confidentiality of the information, in accordance with the prevailing legal, regulatory and contractual framework and complying with established security guidelines, procedures and legislation.

2. IMPORTANCE OF INFORMATION AND NETWORK SECURITY

Information is a fundamental asset of the Euskaltel Group, which must be appropriately protected. As a telecoms operator, our network is also a fundamental asset for the Euskaltel Group that must also be protected.

The management of the Euskaltel Group understands that it has a duty to ensure the security of its information and the network as essential elements for correctly undertaking its services and obligations, and it therefore assumes the objectives and principles established in its policies and rules; it is committed to providing the necessary resources; it demands collaboration from all of its employees and contractors; and it takes responsibility for motivating and training them in terms of awareness and compliance with these policies and rules. During their daily activities, every member of the Euskaltel Group must guarantee the confidentiality, integrity and availability of information and the network and their associated assets, thereby ensuring the continuity and security of the services provided to clients.

3. INFORMATION AND NETWORK SECURITY POLICY

The Information and Network Security Policy, in line with the guidelines on good governance, is the reference framework intended to facilitate the definition, management, administration and implementation of the necessary risk management mechanisms and procedures to achieve the appropriate level of protection for the critical nature of the company’s physical and information assets.

The Euskaltel Group has established the following security principles and criteria:

- To make compliance with the applicable prevailing regulatory and legal framework the cornerstone of its policy.
- To provide employees, clients and collaborators with appropriate security measures for buildings, corporate information systems and the network.
- To provide appropriate and proportionate protection of the information that the company collects, processes, stores, generates and transmits in its information systems and on the network, which is essential to ensure its confidentiality, integrity and availability.
- To appropriately restrict access to its information systems, buildings and network, both by people and by physical or logical objects, establishing an access control system for such purpose.
- To train and raise awareness among its employees and collaborators in relation to risk management and security, as the basis for effective compliance with rules and procedures, as risk management is an activity that is everybody’s responsibility and every person must carry out their activities ensuring appropriate protection of the company’s assets; understanding, assuming and applying the security rules and procedures that have been defined.
- To maintain the operational status of buildings, the availability of information, and the systems that collate, process, store and transmit this information, as well as of the network, which are all essential to ensure business continuity, for which our risk management plans, rules, procedures and mechanisms must ensure prevention, crisis management and recovery in relation to disasters.
- To treat security as part of our regular operations, being aware of and engaging in all its processes to minimise the impacts, interruptions and any inefficiencies that may affect the provision of the services offered by the Euskaltel Group to its clients.
- To regularly analyse compliance with this policy and the working methods that implement it, striving for continuous improvement while minimising corporate risks at all times.

This policy applies to all our activities, products and services, across all our work centres. It is communicated to the whole organisation and made available to our clients, shareholders, stakeholders and the general public, and is regularly reviewed to ensure that it is relevant to the Euskaltel Group at all times.

4. INFORMATION AND NETWORK SECURITY OBJECTIVES

Every year, the Euskaltel Group establishes the information and network security objectives within the scope of the Information and Network Security Management System (SGSIR), as established in procedure SGE-00-00-7-32-2 on the definition and monitoring of objectives.

The actions to be carried out together with the necessary resources, the people responsible and deadlines are set for each defined objective. These objectives are approved by the Information and Network Security Management Committee (CGSIR)

The CGSIR regularly monitors the defined actions to ensure compliance with security objectives, establishing new measures if necessary.

5. INFORMATION AND NETWORK SECURITY MANAGEMENT SYSTEM (SGSIR)

The Euskaltel Group has defined an information security management system to implement this policy, which includes the procedures and responsibilities required to ensure its compliance.

- **Information Assets**:
  - Information and the IT systems that generate, process, store and exchange this information with stakeholders (clients, suppliers and other entities) in the course of their duties and services, shall be considered as information assets.
  - Information and network assets will be appropriately protected according to their value and criticality.
- **Information and Network Security Management System (SGSIR) and Compliance**
  - The confidentiality, integrity, availability, traceability and authenticity of the information and IT systems related to the services offered by the Euskaltel Group must also be safeguarded, using the management framework established by the UNE-ISO/IEC 27001 standard and the best practices set out in the UNE-ISO/IEC 27002 standard (Code of Best Practices for Managing Information Security). The various rules and procedures that are deemed to be necessary to comply with the security principles and the rules defined in this policy shall be developed for such purpose.
  - To ensure continuity and the systematic adaptation and improvement of security to meet the Group's requirements, an information security management system (ISMS) has been implemented in accordance with the UNE-ISO/IEC 27001 standard.
  - The Euskaltel Group shall comply with the security requirements established under prevailing national and European laws.

- **People**:
    - All Euskaltel Group employees shall actively participate in this culture of prevention and asset protection. They must therefore act in accordance with this policy and those security rules and procedures established by the Group.
    - The Euskaltel Group shall raise awareness and provide training for its personnel regarding the importance to the performance of its activities and services of ensuring the security of the information that it handles and processes.
    - Employees of companies and third parties that provide any type of service to the Euskaltel Group that have access to its IT and online resources, as well as to the Group's information, shall also be required to ensure that their actions comply with the security requirements established in this Security Policy and any documents derived from it.

6. DUTIES AND GENERAL RESPONSIBILITIES

The assignment and restriction of responsibilities to ensure that the objectives proposed in this policy are implemented and achieved require certain roles to be established that shall be responsible for the general aspects of managing information security. The Euskaltel Group has therefore established and documented these functions and responsibilities with regards to information security.

Responsibility for the system lies with the head of technology (Chief Technology Officer) and with the head of systems (Chief Information Officer). This responsibility is independent of the responsibility for security, thereby safeguarding the independence of both roles.

7. DECLARATION OF AUTHORITY FOR THE POLICY

The Information and Network Security Management Committee (CGSIR) has the authority to verify compliance with this policy; responsibility to ensure compliance with general guidelines and the corresponding actions contained in them; and the independence to propose the necessary corrective actions to achieve the objectives in the plan for dealing with risks and for continuously improving information security.

Every person and department involved in the processes or services included in the scope of this policy is responsible for complying with it. To achieve this objective, all Euskaltel Group employees must be involved and participate in it.

The Group may also require the participation of suppliers and third parties in applying the minimum-defined security measures.

The Information and Network Security Management Committee (CGSIR) is responsible for this policy and must review this document at least once every year to assess its validity and the need to update it based on new risks that may have appeared or new requirements to ensure information security.

8. GLOSSARY

- **Information Assets**: Elements of the information systems, whether resources or information, that have material value and are necessary for the services of the Euskaltel Group.
- **Authentication**: Feature that enables the identity of people or processes that access or modify information to be verified, or enables their origin to be verified.
- **External collaborators or third parties**: Those people with access to information that the Euskaltel Group is responsible for possessing or administering, but which are not salaried personnel of the Group.
- **Confidentiality**: The information characteristic meaning that it can only be disseminated to authorised people and entities via authorised processes in time and form.
- **Availability**: The characteristic of information and IT systems meaning that they must be accessible and usable in the correct and appropriate way.
- **Information**: Applicable to any storage, communication or receipt of knowledge, such as data, opinions, including figures or graphs, or supported on any media.
- **Integrity**: The information characteristic that means it must be complete and accurate.
- **Information System**: General term that encompasses hardware, software, or organisational or administrative aspects to be taken into account to protect the Euskaltel Group’s IT resources.

Mr José Miguel García Fernández

CEO