CORPORATE RISK MANAGEMENT AND CONTROL POLICY

The Euskaltel Group is the Business Group made up of those companies that, in a legal sense, form part of a commercial Group whose parent company is Euskaltel S.A. In this policy, the references made to the Euskaltel Group or to Euskaltel should be understood to apply to each and every one of the individual companies that make up the Group.

This document, which forms part of the Euskaltel Group's Corporate Governance system, sets out the risk management and control and internal control policy set by the Board of Directors of the Euskaltel Group, hereinafter referred to as the Corporate Risk Policy.

Purpose of the Corporate Risk Policy

The purpose of this policy is to lay down the guiding principles that must govern the Euskaltel Group's actions to control and manage all kinds of risks it faces or could face in the future and the key figures in charge of managing these risks.

This policy is implemented and complemented by the Group's Corporate Governance System, which includes policies, manuals, instructions and any other document.

The Corporate Risk Policy, which as a whole comprises the Group's General Framework of Action with regard risk management issues, is structured as follows:

- Definitions and types of risk
- Guiding principles
- Risk management system
- Roles and responsibilities
- Corporate risk map and
- Risk tolerance level

Definitions and types of risk

For the purposes of this policy, an Event is an incident or occurrence, from sources inside or outside the Euksaltel Group, which affects or may affect the achievement of its objectives and which may have a positive or negative impact, or both at the same time, on the fulfilment of these objectives. Risk is defined as the probability that an Event may occur and adversely affect the achievement of the Group's objectives.

Corporate risk management is the process designed to identify potential events that may affect the Group and to manage possible risks within accepted thresholds so as to provide reasonable assurance with regard achieving the Group's objectives.

Internal Control is defined as a set of activities performed by the Group to provide reasonable assurance in terms of the efficiency and effectiveness of operations, the reliability of financial information, compliance with applicable standards and the safeguarding of its assets, which is why it is therefore a comprehensive part of Corporate Risk Management.

Risk Management is global, although each Risk can be dealt with individually based on the nature of the event causing it, but taking into consideration the possible effects on all Group objectives, whether short or long-term. The Risk subject to analysis and management is the Inherent Risk, prior to the actions adopted to manage it, i.e. before the actions adopted to change or reduce the probability of occurrence and/or impact on the Group's objectives.

For the purpose of managing the risk, the following types of Euskaltel Group Risk are defined based on the possible source of the event:

- Strategic risks: risks that affect the Group's strategic objectives contained in its current Strategic Plan and Business Plan. These are high level risks that reflect the option chosen with regard to how value will be created for Stakeholders. By contrast, the source of the other types of Risk (the non-strategic risks) is the strategy implementation.

- Financial risks: risks via financial instruments that have an impact on the Group's financial results (as defined in the accounting regulations). They are broken down as follows:

    - Credit or counterparty risk, linked to one of the parties to the financial instrument causing the other party a financial loss due to failure to comply with an obligation;
    - Liquidity risk, linked to a difficulty in meeting obligations relating to financial liabilities that are settled through cash or another financial asset; and
    - Market or cash flow risk, linked to the financial instrument's fair value or future cash flows fluctuating as a result of changes to market prices, the issuer of the financial instrument or to factors that affect all financial instruments with the same characteristics.

- Regulatory risks: risks arising from requirements and limitations set out in specific legislation and regulations that affect the Group's business practice and include risks arising from a failure to comply with contractual obligations, whatever their nature, both by the Group itself and by the counterparty (whoever this is: customer, supplier, employee, bank, etc.).

  For the purposes of Group Risk Management, these Risks are structured into Criminal risks, Data protection risks, Tax risks, Industry risks, Entity of Public Interest risks and Other regulatory and regulatory compliance risks.

- Sustainability-related risks: risks linked to the Group's environmental, social, ethical and corporate governance objectives.

- Cyber risks: risks arising from threats and vulnerabilities that may affect the Group's control, information and communication systems and the services offered to customers, as well as any other asset that is a part of its infrastructure. This includes risks arising from misleading individuals to access the systems they operate and, where applicable, a lack of diligence on their part. These risks are managed on the basis of four types:

    - Cyber risks linked to the Network/Services, arising from threats and vulnerabilities that may affect the Group's control and communications systems, with an impact on the telecommunications services provided to customers.
    - Cyber risks linked to systems/processes, where it is possible that the Group's control and information systems are affected with an impact on processes.
    - Cyber risks linked to digital services, where the possible impact is on the digital services provided by the Group to customers, and

- Business continuity and contingency risks: are risks arising from possible disasters with a serious impact on services and processes.

- Operating or operational risks: risks that affect the efficiency and effectiveness of operating processes and the provision of services (excluding cyber risks) and customer satisfaction.

  These Risks are structured into Basic supply risks (TV content and traffic from other operators), Technology risks (network and systems), dependency on third party risks, Human Resource risks and others.

- Reputational risks: risks that may adversely impact on the Company's value as a result of conduct by the Group that is below the expectations created in the different stakeholder groups, including conduct or behaviours linked to corruption.

- Information risks: risks linked to the objective of having and providing addresses with reliable, complete data and information, prepared in accordance with applicable legislation, if appropriate, which is fit for purpose and supports decision-making and the monitoring of Group activities and performance.

  These risks are broken down into Official Financial Information Risks, Official Non-Financial Information Risks and Operational Information Risks (unofficial).

The risk of fraud, in all its different meanings, is included in the management of each type of risk.

Guiding principles

The guiding principles within the Group's Corporate Risk Policy framework are as follows:

- Adherence to the law, internal regulations and contractual relations

  Risk management is carried out in strict compliance with current legislation, the Group's voluntarily established internal regulations, its contractual obligations towards third parties, and any binding administrative and judicial rulings. The Group will expressly reject any dishonest or fraudulent behaviour and any acts against the confidentiality, integrity and availability of IT systems, telecommunications networks, computer data, as well as any abuse of such systems, networks and data.

  The standards of the Corporate Governance System and the procedures that govern the Group's activities must be complied with at all times. Behaviours that in any way contravene the values, principles and ethical behaviour laid down in the Ethics Code and its Instructions for Behaviour, under the zero tolerance principle applied to the committing of illegal acts and fraud, must be avoided.

- Organising and separating functions

  The Group's organisational structure must be effective and appropriate in order to apply the Risk Management System and Internal Control, including the necessary policies and procedures. It should ensure that there is adequate separation of operational functions between risk takers and those responsible for their analysis, control and monitoring.

- Transparency

  The Group's Risk Management and Internal Control functions guarantee reliable information for all stakeholders on the Group's inherent risks and the systems developed to prevent and mitigate these risks.

  The control of and relevant information about Risks and the Risk Management System and Internal Control's operation must be treated in a transparent way within the Risk Management System among risk takers and those responsible for their analysis, control and supervision.

- Continuity

  The Group's Risk Management and Internal Control functions are ongoing and are designed and updated regularly to ensure, to the extent possible, and to enable the identification of risks in advance and the adoption of mitigating measures to manage them.

- Monitoring

  The Group's Risk Management System and Internal Control includes and executes sufficient measures to monitor and supervise risks, which provide evidence of compliance with this Corporate Risk Policy.

Risk management system

The Group's Risk Management System is based on recognised international standards (COSO framework and ISO standards), involving an ongoing, iterative process with four key stages:

1. Continuous identification of risks
2. Analysis and assessment
3. Treatment
4. Monitoring and reviewing the system

The Risk Management System's key tools, applied on the basis of the risk assessment, are structured as follows:

- Internal regulations, including this Corporate Policy, other additional policies that implement this one and the processes for drawing up the Group's Risk Map, which include all the kinds of risk defined,

- Information and Reporting, which includes the Strategic Plan, the Business Plan, the Scorecards, the Official Reports and the regular meetings of the Risk Monitoring and Control Bodies,

- Targeted risk management, which includes automatically managing Risks using IT tools, Risk Maps and specific controls, and increasing action depending on operations and risk types,

- Involvement of expert third parties, who provide risk management assurance services.

Roles and responsibilities

All members of the Group are responsible for the Risk Management System working in accordance with this Corporate Risk Policy, on the basis of the roles they hold within the organisation. The following responsibilities particularly stand out:

- Board of Directors: approves the Group's general policies and strategies and, specifically, the risk management and control policy, including tax risks. The Board also regularly monitors the internal information and control systems. In addition, the Board approves specific transactions when there is a particular risk due to the amount or nature of the transaction.

- Audit and Control Committee: as part of its core powers over risk management and information systems, the Committee monitors the efficiency of the Group's internal control and its risk management systems. It regularly evaluates the risk management and internal control systems so that key risks are identified, managed and reported on appropriately.

  In terms of risk management and policy, the Committee identifies the different types of risk faced by the Group, including contingent liabilities and other off-balance sheet risks. It determines a risk control and management model based on varying levels. It sets the risk thresholds considered to be acceptable by the Group and the measures planned to mitigate the impact of the risks identified, should they materialise, as well as the information and internal control systems used to control and manage these risks.

- Senior management: ensures the smooth running of the Risk Management System and Internal Control, guaranteeing that all relevant risks impacting the Group are appropriately identified, managed, quantified and reported. Senior management monitors and coordinates the work of Risk Managers within their scope of responsibility, identifies events within their scope of responsibility, reports to the risk coordination and Internal Audit departments and validates, leads and monitors the action plans and work arising from the risk management process.

- Risk managers (or owners): define and execute the action plans, ensuring the measures adopted are efficient and effective. They regularly report on their activities and identify possible events within the scope of their responsibility.

- The Group's Internal Audit function ensures the smooth running of the information and internal control systems, helping to improve risk management, control and governance processes, guaranteeing the Group's Audit and Control Committee effective and independent monitoring of the internal control system and giving recommendations to the Group that help reduce the impact of potential risks to reasonable levels, thus making its objectives easier to achieve. Furthermore, the function coordinates and standardises information on Risks prepared by Senior Management and risk managers, as well as the information needed for the Audit and Control Committee to be able to perform its monitoring work, including the Corporate Risk Map and updates thereto.

  Internal Audit must, at all times, safeguard its independence from the Risk Management System, without taking responsibility for the key operational decisions made.

Corporate Risk Map

The Group includes a list of its key risks in a Corporate Risk Map, which is prepared using the Risk Maps for each of the previously defined types of risk, which are managed by the relevant managers.

The end purpose is to enable the Governing Bodies to regularly reassess existing risks, monitor the measures adopted to manage them, including mitigating their impact should they materialise, and to set out and update, if appropriate, the tolerance level for each risk using the information provided by the members of the Group, in accordance with their roles and responsibilities. The Risk Map is also used to standardise and compare risks of different kinds. The risk map shall be reassessed at least annually, without prejudice to any updating that may be necessary due to other circumstances.

Risk tolerance level

The Euskaltel Group's Risk Management System aims to achieve an average moderate risk profile through cautious risk management. The Group's risk tolerance level is decided using the value assigned to each risk identified in the Risk Map by applying probability, impact and speed of onset criteria.

At least the following factors are taken into consideration to determine expected impact:

- Time and resources needed to resolve situation
- Impact on results after tax
- Short and medium-term impact on turnover
- Media consequences, defined as public exposure time
- Impact on Group's reputation
- Potential sanctions by government entities, and
- Involvement by different organisational levels to manage risk

Risk management is based on the principle of Materiality or the relative importance of the value assigned to the risks identified in the Risk Map.

Entry into force

Euskaltel's Board of Directors approved the Corporate Risk Management and Control Policy at its meeting held on 24 May 2016. In order to adopt the developments and trends in this field set out in the Good Governance Code of listed companies reviewed in June 2020, thus completing the updating process that began in 2019, the Corporate Risk Management and Control Policy was updated and approved by Euskaltel's Board of Directors at its meeting held on 15 December 2020.

* * * * * * * * *