FairConnect

# QUALITY POLICY AND INFORMATION SECURITY POLICY

The management of Fair Connect adopts a quality policy to adequately respond to market needs and to increasingly pursue customer satisfaction.
Our company has always aimed at customer satisfaction in terms of the quality of the products and services provided.
The company is strongly committed to continuous quality improvement to promptly respond to all market demands.
To this end, management aims to achieve this goal through:

- Ensuring a prevention-oriented approach to problems and service disruptions, and continuous improvement.
- Considering quality as a determining factor in meeting regulatory requirements.
- Pursuing constant innovation of know-how and its organization, in order to capitalize on projects, methods, and experiences.
- Continuously focusing on customer satisfaction by regularly measuring their satisfaction.
- Carefully controlling the service delivery phases, to optimize the use of existing and/or potential resources, which can significantly impact the company's performance.
- Pursuing continuous improvement of the quality management system.
- Managing the company's commercial development aimed at strengthening relationships with customers and increasing market presence, also through correct commercial and technical approaches with clients, in full transparency of communication.

The organization is aware that guaranteeing quality requires continuous commitment from all operational personnel, and it can only be successfully achieved through a systematic approach to quality issues.

Having assessed the context in which the organization operates and the needs of the stakeholders, FAIRCONNECT SPA has deemed it appropriate to develop, maintain, control, and continuously improve an Information Security Management System (ISMS), in compliance with the ISO/IEC 27001:2022 standard.
The management attaches strategic importance to the handling of information and concretely aims to protect the confidentiality, integrity, and availability of data.
The main objectives of the ISMS are:

1. **Confidentiality of the managed information assets**: ensuring information is not made available or communicated to unauthorized individuals, entities, or processes.
2. **Integrity of the managed information assets**: protecting the accuracy and completeness of assets, meaning any information or asset to which the organization attributes value.
3. **Availability of the managed assets**: ensuring information is accessible and usable upon request by an authorized entity.
4. **Compliance with mandatory, regulatory, and contractual requirements.**
5. **Adequate training of personnel on information security.**

Further details on the objectives are outlined in the company’s improvement plan for the reference year.

**The implementation of the Information Security Management System involves:**

- Identifying a risk assessment methodology suitable for the ISMS, the identified business requirements, mandatory and regulatory requirements, and managing risks at an acceptable level, aligned with the broader organizational risk management context.
- Identifying, through appropriate risk analysis, the value of the information assets within the scope of the ISMS to understand vulnerabilities and potential threats that could expose them to risks.
- Managing confidentiality, availability, and integrity of information while respecting the principles of privacy by design and privacy by default, as well as mandatory regulations.
- Protecting data against unauthorized access based on their criticality, value, and sensitivity.
- Increasing internal awareness of information security risks.

- Ensuring operational continuity of business processes.
- Providing customers with effective and efficient communication channels for information exchange and support them in any event that might compromise information security, especially personal data, in compliance with the applicable regulations.
- Defining and enforcing operational guidelines for a security architecture, including rules, functions, tools, objects, and controls, designed and implemented to ensure compliance with the standards defined by FAIRCONNECT SPA across every organizational structure, IT environment, and individual computer.
- Monitoring the implemented ISMS system, capturing any improvement opportunities.

**Applicability**

All internal staff and collaborators of FAIRCONNECT SPA involved in processing information within the scope of the ISMS.

**Responsibility**

This policy is formulated and reviewed by the management of FAIRCONNECT SPA.

The RSQ (Quality and Security Responsible) facilitates the implementation of this policy through appropriate standards and procedures.

All staff and collaborators must adhere to the policies and procedures established by FAIRCONNECT SPA in support of this policy.

All personnel, based on their knowledge, are responsible for reporting any vulnerabilities to the RSQ.

Any action, whether intentional or due to negligence, causing damage to FAIRCONNECT SPA, may be pursued in appropriate forums.

**Review**

This policy is reviewed annually (during the Management Review) and in the event of changes that affect it, to ensure that it remains suitable for the strategies of FAIRCONNECT SPA and the expectations of stakeholders.

**Issue Date: 10-01-2024**

**Signature Management**

________________________