Information Security Policy

INTRODUCTION

One of FiberCop's most important assets, on which its business is based, is information, understood as any aggregation of data that has business value and relevance, regardless of its form or the technology used for its processing.

The protection of information and all related assets is therefore a fundamental element in safeguarding and ensuring the continuity of business processes and must be managed through an organizational and regulatory system that defines roles, responsibilities, strategies, and rules to be adopted within FiberCop.

PURPOSE AND SCOPE

The purpose of this document is to:

- Define information security objectives;
- Express FiberCop's commitment, through its management, to meet information security requirements through a process of continuous improvement;
- Specify the information security requirements that FiberCop intends to adopt.

The scope of this document extends to all corporate assets (processes, people, technologies) that process information on behalf of FiberCop.

FiberCop Functions shall adapt and specialize, each within its area of responsibility and through appropriate documentation, the guidelines expressed in this policy in order to achieve the defined security objectives.

PROCESS DESCRIPTION AND RESPONSIBILITIES

Security Objectives

FiberCop's information assets consist of all information managed through the use of corporate assets such as people, processes, and technologies, physically located at specific sites, based on cloud services, or operating in a fully mobile environment, whether owned by FiberCop or by Third Parties (e.g., Suppliers, Partners, External Contractors, Customers).

The objectives defined by FiberCop for information protection are proportionate to:

- Applicable regulations and standards;

- The business value of the information.

Therefore, FiberCop undertakes to:

- Establish rules, priorities, develop plans, and make available the necessary resources for the full adoption of this document;
- Define processes, roles, and responsibilities for information security;
- Ensure a level of confidentiality, integrity, and availability of information proportional to its business value, as well as to the direct or indirect losses that a security incident may cause to services provided to customers;
- Ensure the security of services delivered to customers as defined in contractual agreements;
- Protect the confidentiality of strategic information and business development plans;
- Safeguard its reputation against damage caused by information security incidents;
- Comply with legal, regulatory, and internal requirements in line with its own Code of Ethics and Conduct;
- Ensure the security of employees' personal information in compliance with applicable regulations and for the protection of employees;
- Raise awareness and provide training to personnel on information security;
- Record, analyze, and manage any actual or suspected information security incident;
- Cooperate with Competent Authorities and Institutions in managing security incidents with national or international impact;
- Cooperate with Competent Authorities and Institutions to ensure the secure management of strategic information processed on its assets;
- Cooperate with Competent Authorities and Institutions to share methodologies and best practices for the continuous improvement of security policies;
- Fulfill contractual obligations related to information security.

Achievement Strategy

To achieve the objectives described in previous section, FiberCop has established an Information Security Management System (ISMS) with the following characteristics:

- It identifies an appropriate governance model for processes and activities related to the protection of information assets, defining roles and responsibilities within FiberCop;

- It includes a reference framework that supports the organization in identifying areas of focus, intervention priorities, and allocation of resources necessary for the effective implementation of security policies;
- It enables the establishment of policies and identification of security requirements based on risk analysis, providing awareness of the organization's exposure to threats and the impact of security incidents on business operations;
- It enables the formalization of all security measures in compliance with international standards and applicable regulations;
- It allows the evaluation of residual risk levels with the objective of continuously improving the security level of information assets and corporate resources;
- It ensures verification of the effective implementation of identified security measures and monitors their ongoing maintenance.

The ISMS must be designed and implemented in such a way as to enable management to periodically evaluate, including through performance indicators, the results of the risk management process, in order to direct preventive, corrective, or improvement actions and allocate the necessary resources for their implementation.

GENERAL REQUIREMENTS FOR THE IMPLEMENTATION OF THE ISMS

Within the ISMS, FiberCop assets are classified into two categories:

- **Primary:** this category includes information of any type, as well as business processes;
- **Secondary:** this category includes all assets on which information is processed, namely hardware, supporting infrastructures, software, networks, workstations (WS), mobile devices, paper or digital media, personnel, suppliers, physical locations, and the organization.

The general security requirements that FiberCop intends to adopt are defined based on security standards and best practices. These requirements are grouped by topic as follows:

- Information Security Policies and Procedures
- Information Security Organization
- Third-Party Relationships
- Risk Management
- Asset Analysis, Classification, and Handling

- Access Management, Authorization, and Logging
- Operational Security and Communications Management
- Asset Acquisition, Development, and Maintenance
- Security of Facilities, Infrastructure, and Information Processing Resources
- Information Security Incident Management
- Business Continuity
- Compliance with Applicable Requirements, Contractual Obligations, and Security Standards
- Information Security in Personnel Management
- Security Audits and Assessments

As confirmation of the strategic importance attributed to information security, FiberCop has achieved certification under ISO 27001 for its ICT Risk Management process.