



Cybersecurity and Information Security Policy

July 2026

ID	CYBERSECURITY AND INFORMATION SECURITY POLICY	CLASSIFICATION	VERSION	DATE
IS_PL_01		FCC_INTERNAL	5.0	July 2026

Version History				
Version	Date	Author	Details	Approved by
1.0	March 2009	IS	Creation of the document	FCC Group Board of Directors
2.0	February 2023	IS	Document revision. Format unified with the rest of the Standards and new information classification structure	FCC Group Board of Directors
3.0	May 2023	IS	Document review. Adaptation to ISO/IEC 27001:2022 regulations	FCC Group Board of Directors
4.0	January 2024	IS	Charts standardised and document templates updated according to the new identifier convention	FCC Group Board of Directors
5.0	July 2026	IS	Document review and formatting changes	FCC Group Board of Directors

ID	CYBERSECURITY AND INFORMATION SECURITY POLICY	CLASSIFICATION	VERSION	DATE
IS_PL_01		FCC_INTERNAL	5.0	July 2026

INDEX

1. Introduction	4
1.1 Purpose.....	4
1.2 Scope.....	4
2. Development.....	5
2.1 Principles of Information Security Management.....	5
2.2 Criteria	6
2.2.1 Information Security Regulatory Framework.....	6
2.2.2 Classification of Information	7
2.2.3 Prior authorizations	7
2.3 Actions	8
2.3.1 Interconnection Agreements	8
2.3.2 Risk Analysis.....	9
2.3.3 Audit and Information Systems Control	9
2.3.4 Configuration management	9
2.4 Organization.....	10
2.4.1 Organizational Structure.....	10
2.4.2 Information Security Areas	11
3. Responsibilities	12
4. Normative reference	13
4.1 Regulatory controls ISO27001:2022 and ENS.....	13

ID	CYBERSECURITY AND INFORMATION SECURITY POLICY	CLASSIFICATION	VERSION	DATE
IS_PL_01		FCC_INTERNAL	5.0	July 2026

1. Introduction

This document is part of the FCC Group's Information Security Regulatory Framework, which outlines the mandatory precepts of the Group regarding Information Security.

The Security Regulatory Framework is reviewed and updated periodically by the Information Security department (hereinafter IS department), in accordance with the provisions of the Regulatory Framework Management and Maintenance Document. This document contains information on the version history, revisions and approvals of this Policy, as well as its relationship and dependency with the rest of the regulatory documents.

1.1 Purpose

The purpose of this Policy is to:

- Define the basic principles and minimum requirements for the development of security measures for information systems.
- Establish an organizational scheme that allows managing and controlling Information Security.
- Strengthen the suitability, adequacy, and effectiveness of the leadership and management of Information Security in accordance with commercial, legal, regulatory, and contractual standards.

In order to guarantee, in a proportionate manner, the confidentiality, integrity, availability and auditability of the FCC Group's information.

1.2 Scope

This Policy will apply to:

- All **information** of the FCC Group, regardless of the place or medium in which it is located.
- All **personnel** who process FCC Group information.
- Any internal **regulations** that address some particular aspect of Information Security.

ID	CYBERSECURITY AND INFORMATION SECURITY POLICY	CLASSIFICATION	VERSION	DATE
IS_PL_01		FCC_INTERNAL	5.0	July 2026

2. Development

2.1 Principles of Information Security Management

Information is a strategic resource for FCC, and, therefore, its adequate protection must be guaranteed in the performance of daily activity and in relations with external entities.

The Cybersecurity and Information Security Policy is based on the following basic principles of mandatory compliance, to always be kept in mind in any activity related to the processing of information:

- The Information Security Regulatory Framework is mandatory for all FCC Group personnel.
- The design and management of Information Security must take into account the strategic objectives of the FCC Group.
- Information Security management needs an organizational structure that in turn represents the functional structure that is known by all staff and functions as the main reference.
- The size of the Information Security organization structure will be proportional to the security needs of the FCC Group.
- Protection measures must be applied in proportion to the value of the assets to be protected, the existing risks and the operational, reputational and financial impact of possible security failures.
- The FCC Group must ensure that all risks are identified and that measures are taken against threats to the Information Security it owns.
- The confidentiality, integrity, availability and auditability of the information must be preserved during its life cycle, regardless of the medium in which it is contained and the place where it is located.
- The internal regulations established to protect information must be in accordance with current legal regulations.
- The information that the FCC Group exchanges with other individuals or entities must adhere to the FCC Group's Information Security Regulatory Framework.
- Information Security is the responsibility of all FCC internal staff and collaborators, who must be adequately trained to perform their duties.
- The state of the art of Cybersecurity and Information Security will be evaluated periodically.

The FCC Group has created a Security Management Model to ensure compliance with the security requirements established in its information systems, based on the following sections.

ID	CYBERSECURITY AND INFORMATION SECURITY POLICY	CLASSIFICATION	VERSION	DATE
IS_PL_01		FCC_INTERNAL	5.0	July 2026

2.2 Criteria

2.2.1 Information Security Regulatory Framework

Starting from this Policy, the Information Security Regulatory Framework will be developed, structured in the following four levels:

- **The Policies** will define the principles, objectives and protection criteria that describe the operations involving Information Security. They will be applied to all companies that make up the FCC Group.
- **The Standards** will establish the requirements that must be met to satisfy and achieve the security objectives established in the Policies. They determine what needs to be protected and what is the appropriate level of protection in each case. They will apply to all the companies that make up the FCC Group and will collectively ensure the protection of all the environments of the organisation's information systems.
- **The Procedures** will specifically describe who, how, where and when specific tasks will be performed to protect information assets, in accordance with the Standards. They will therefore contain, above all, technical specifications for compliance with the different services or security aspects.
- **The Technical Guides** will document explicitly and in detail the tasks and actions to be carried out during the execution of a procedure.

The Policies and Standards will be developed by the Information Security department, while the Procedures and Technical Guidelines, due to their operational nature, will be developed by the departments that implement them in each case.

ID	CYBERSECURITY AND INFORMATION SECURITY POLICY	CLASSIFICATION	VERSION	DATE
IS_PL_01		FCC_INTERNAL	5.0	July 2026

2.2.2 Classification of Information

FCC classifies the information it processes, taking as its main criterion the potential harm that could be caused by its dissemination to unauthorized personnel.

The Information Management Policy establishes four levels of classification:

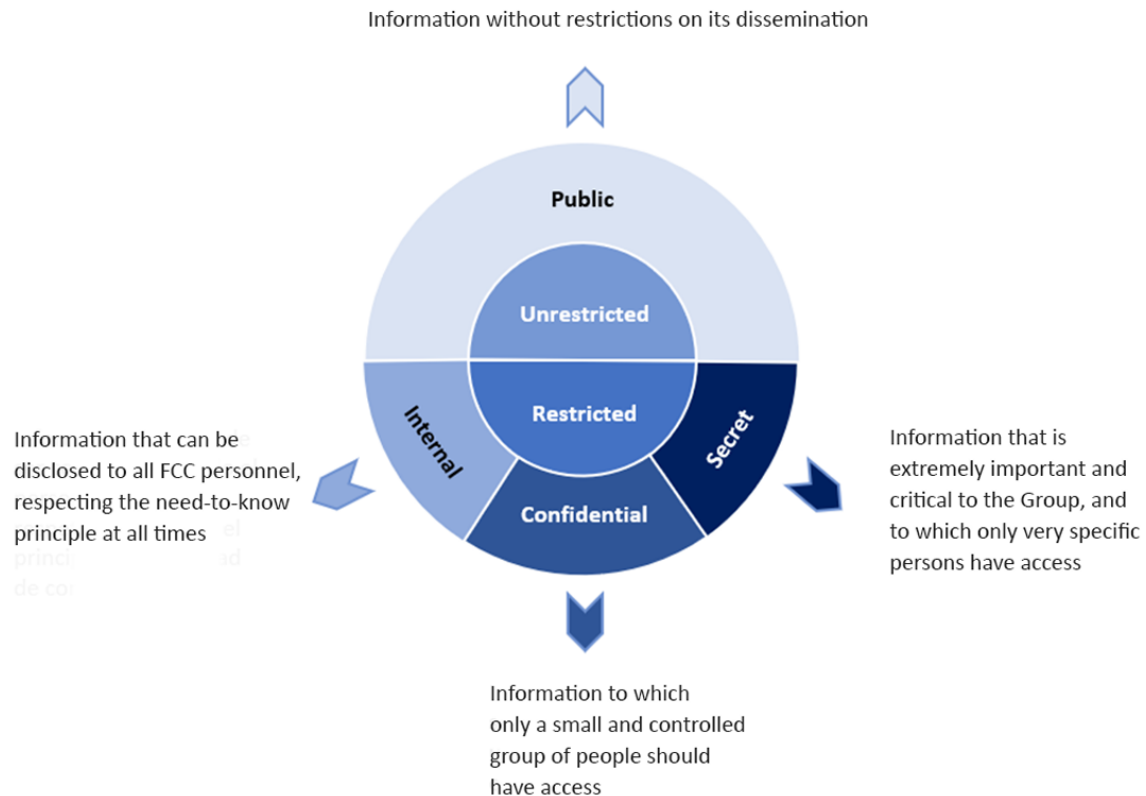


Figure 1. FCC Group information classification scheme

2.2.3 Prior authorizations

Access to information is justified through two means:

- **The need to be familiar with information:** FCC's staff will have access, exclusively, to the information they need to know for the performance of their professional duties.
- **Personal authorization to access Restricted information:** FCC will enable access to Restricted information based on personal trust.

Both access routes will take the form of profiles that will allow you to view, modify or reproduce the appropriate information in each case.

ID	CYBERSECURITY AND INFORMATION SECURITY POLICY	CLASSIFICATION	VERSION	DATE
IS_PL_01		FCC_INTERNAL	5.0	July 2026

2.3 Actions

The Information Security management model will be based on a series of actions that ensure the confidentiality, integrity, availability and auditability of the information, as well as compliance with applicable legal regulations.

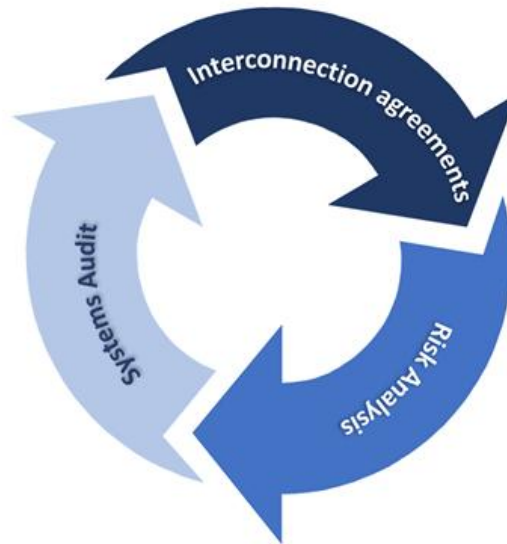


Figure 2. Security model actions

2.3.1 Interconnection Agreements

When FCC information systems are interconnected with different technologies, levels of trust or implementation of security policies, a prior certification process must be carried out to guarantee the appropriate level of Information Security for the new information system created after the interconnection.

The IS department will establish the interconnection criteria, conditions and requirements based on a risk analysis of the respective systems.

ID	CYBERSECURITY AND INFORMATION SECURITY POLICY	CLASSIFICATION	VERSION	DATE
IS_PL_01		FCC_INTERNAL	5.0	July 2026

2.3.2 Risk Analysis

The analysis and risk management of information systems will be carried out to:

- Assess the risks and determine, based on these, what measures shall be applied.
- Categorize and prioritize actions regarding Information Security.
- Consolidate a scheme of priorities and consequences in the event of a security incident.
- Continuously improve the group's security maturity level in order to reinforce the effectiveness and response capacity in the event of a security emergency.
- Comply with the responsibilities established in the Regulatory Framework of the FCC group.
- Prepare businesses to comply with their legal obligations before the authorities and operational and/or contractual obligations before their clients and suppliers regarding Information Security.

The analysis and treatment of risks will be reviewed periodically.

2.3.3 Audit and Information Systems Control

System auditing will allow us to know whether information protection is provided and complies with the FCC Group's Information Security Regulatory Framework.

As a result of the conclusions reached in the audit, the person in charge must develop appropriate actions to improve security management.

The audits will be periodic and will be based on risk criteria.

2.3.4 Configuration management

As an important measure, it is necessary to define precise procedures regarding security configurations that include: Hardware, software, services (e.g. Cloud Services) and networks. To guarantee compliance with this measure, the Configuration and Change Control Standard must be used as a reference.

ID	CYBERSECURITY AND INFORMATION SECURITY POLICY	CLASSIFICATION	VERSION	DATE
IS_PL_01		FCC_INTERNAL	5.0	July 2026

2.4 Organization

The FCC Group's Information Security management model is based on a governance model made up of clearly defined bodies and roles, responsible for promoting the correct management of its cybersecurity resilience strategy, recognising the responsibilities of personnel at all levels, promoting continuous improvement in the management of this strategy, and demonstrating a full understanding of the risks faced.

2.4.1 Organizational Structure

The FCC Group's information security is based on the recommendations defined by the IS department.

Below are the committees where the IS department has a presence and the role it has:

- **The Board of Directors** is the senior body in charge of approving the security organisation and management model.
- **The Cybersecurity Committee** will act as the highest coordination body for Information Security and is the body in charge of communicating the security strategy to the entire organization. It will be convened quarterly, led by the Director of Information Security.
- **The Security Control Committee** is the body in charge of coordinating and reviewing the security status in the different business units. This committee may have the status of a forum or working group if necessary. It will be convened with each of the business units and will be led by a representative from the Information Security department.
- **The IT Coordination Committee:** Led by the Director of Information Technology. Its objective is to monitor the status of IT projects, ensuring compliance with Information Security recommendations.
- **Privacy Board:** Led by the Data Protection Officer. Its objective is the processing of legal obligations regarding data protection, guaranteeing compliance with information security recommendations.

ID	CYBERSECURITY AND INFORMATION SECURITY POLICY	CLASSIFICATION	VERSION	DATE
IS_PL_01		FCC_INTERNAL	5.0	July 2026

2.4.2 Information Security Areas

The protection of information will take the form of security measures aimed at the following areas:

- Information Security for **Individuals**, who must meet a series of requirements to ensure the correct use of the information.
- Information Security in **Documents**, throughout their entire life cycle, in order to secure the information they contain.
- Information Security in **Information and Telecommunications Systems**, in order to secure the information they contain, handle or process. Before starting to process FCC Group information, the systems must be authorized to do so, in accordance with the Group's Information Security Regulatory Framework.
- Information Security in **Facilities**, in order to ensure the processing and storage of information.
- Security of Information held by **External Companies of the Group**, which must apply the measures specified by FCC to secure the information they process as a result of their participation in programmes, projects or contracts with FCC.

ID	CYBERSECURITY AND INFORMATION SECURITY POLICY	CLASSIFICATION	VERSION	DATE
IS_PL_01		FCC_INTERNAL	5.0	July 2026

3. Responsibilities

The FCC Group is the owner of the information handled within the companies that comprise it. FCC makes certain information assets available to staff and collaborators to meet business objectives.

The roles and responsibilities will be assigned to committees, work groups or organizational units, depending on their functions.

- The committees may partially delegate their duties to those subcommittees or specific working groups that are considered appropriate to adequately carry out the duties that FCC Group management has entrusted to them.
- The person responsible for the Information will be in charge of managing access to the information assets, in accordance with the Information Security Regulatory Framework.

All responsibilities assigned regarding Information Security must be clearly established and avoid any possible ambiguity.

The assignment of responsibilities will be specified in the FCC Information Security Roles and Responsibilities Standard.

ID	CYBERSECURITY AND INFORMATION SECURITY POLICY	CLASSIFICATION	VERSION	DATE
IS_PL_01		FCC_INTERNAL	5.0	July 2026

4. Normative reference

This document has been reviewed by the IS Department, and its drafting is based on the international standard ISO 27001:2022 and the ENS.

4.1 Regulatory controls ISO27001:2022 and ENS

ID Control ISO	ISO/IEC 27001:2022 control	ENS Correspondence
5.1	Policies for information security	[org.1] Security Policy; [org.2] Security Regulations
5.2	Information security roles and responsibilities	[org.6] Roles and Responsibilities
5.4	Management responsibilities	[org.6] Roles and Responsibilities
5.12	Classification of information	[mp.info.2] Information Classification
5.15	Access control	[op.acc.2] Access Requirements
5.18	Access rights	[op.acc.2] Access Requirements
5.19	Information security in supplier relationships	[op.ext.1] Procurement and Service Level Agreements (SLAs)
5.36	Compliance with policies, rules and standards for information security	[org.2] Security Regulations
5.37	Documented operating procedures	[org.3] Security Procedures
8.9	Configuration management	[op.exp.3] Secure Configuration Management; [op.exp.4] Security Maintenance and Updates