



---

# **FCC Group Information Management Policy**

July 2026

|          |                                          |                |         |           |
|----------|------------------------------------------|----------------|---------|-----------|
| ID       | <b>INFORMATION MANAGEMENT<br/>POLICY</b> | CLASSIFICATION | VERSION | DATE      |
| IS_PL_02 |                                          | FCC_INTERNAL   | 5.0     | July 2026 |

| <b>Version History</b> |               |               |                                                                                                             |                              |
|------------------------|---------------|---------------|-------------------------------------------------------------------------------------------------------------|------------------------------|
| <b>Version</b>         | <b>Date</b>   | <b>Author</b> | <b>Detail</b>                                                                                               | <b>Approved by</b>           |
| <b>1.0</b>             | April 2009    | IS            | Document creation                                                                                           | FCC Group Board of Directors |
| <b>2.0</b>             | February 2021 | IS            | Document review. Format unified with the rest of the Standards and new information classification structure | FCC Group Board of Directors |
| <b>3.0</b>             | May 2023      | IS            | Document review. Adaptation to ISO/IEC 27001:2022 regulations                                               | FCC Group Board of Directors |
| <b>4.0</b>             | January 2024  | IS            | Charts standardised and document templates updated according to the new identifier convention               | FCC Group Board of Directors |
| <b>5.0</b>             | July 2026     | IS            | Document review and formatting changes                                                                      | FCC Group Board of Directors |

|          |                                          |                |         |           |
|----------|------------------------------------------|----------------|---------|-----------|
| ID       | <b>INFORMATION MANAGEMENT<br/>POLICY</b> | CLASSIFICATION | VERSION | DATE      |
| IS_PL_02 |                                          | 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 Management .....5
  - 2.2 Classification of information.....6
    - 2.2.1 FCC Group Information Classification Model..... 7
  - 2.3 Labeling of Information .....9
  - 2.4 Information Storage Management ..... 10
    - 2.4.1 Specific management of the storage of Restricted information .....10
    - 2.4.2 Audit and Information Systems.....10
- 3. Responsibilities .....11**
- 4. Normative reference .....12**
  - 4.1 Regulatory controls ISO27001:2022 and ENS..... 12

|          |                                          |                |         |           |
|----------|------------------------------------------|----------------|---------|-----------|
| ID       | <b>INFORMATION MANAGEMENT<br/>POLICY</b> | CLASSIFICATION | VERSION | DATE      |
| IS_PL_02 |                                          | 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 history of versions, 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 achieve information management of the FCC Group that:

- Is efficient and effective.
- Provides support to business activities.
- Facilitates decision making.
- Ensures the confidentiality, integrity, availability and auditability of information.
- Serves as a commitment to continuous improvement of information management systems.
- Complies with the regulations and applicable legislation.

### 1.2 Scope

This Policy will apply to all FCC Group information, including information existing prior to its coming into effect.

|          |                                          |                |         |           |
|----------|------------------------------------------|----------------|---------|-----------|
| ID       | <b>INFORMATION MANAGEMENT<br/>POLICY</b> | CLASSIFICATION | VERSION | DATE      |
| IS_PL_02 |                                          | FCC_INTERNAL   | 5.0     | July 2026 |

## 2. Development

### 2.1 Principles of Information Management

- Access to the information will be allowed only to Group personnel who need to know it for the correct performance of their duties and always under the principle of "least privilege".
- The information will be distributed respecting the FCC's principles of action and the limitations imposed by security, legality and/or privacy criteria.
- FCC information will be managed as a corporate resource that supports business objectives and activities.
- Information management will be governed by policies, standards, procedures and guides that ensure its confidentiality, integrity, availability and auditability.
- The organisation and control of information will be carried out throughout its life cycle, regardless of the format and medium in which it is dealt with.
- The protection measures applicable to the information will be included in the agreements that regulate the relationships between FCC and external entities that require access to it.
- Information will be classified and labelled in accordance with the FCC Information classification scheme laid down in this document and the Document Security Standard.
- Information that is not labeled will by default be considered of level Restricted Internal Information.
- The information owner will guarantee the security conditions required according to its classification level, when distributing and storing information.
- The potential impact of an incident will define the need to encrypt information. Information classified as Restricted (Internal, Confidential, Secret) must be protected by encryption when sufficient protection cannot be guaranteed through other controls; the characteristics of the encryption will be dictated by the Encryption Standard.
- Before distributing or exchanging any information outside the FCC Group, the information must be assessed by its owner to identify any type of restricted-level asset and protect it by applying the measures stipulated in the Secure Information Management Guide.
- Once the information has been reviewed and the protection measures appropriate to its classification level have been applied, the information may be reclassified as Public Use to be shared outside the FCC group.
- In the event that a Restricted level asset is mistakenly disclosed or shared with third parties without the asset having the appropriate classification level, the Information Security department will be immediately notified of the event.

|          |                                          |                |         |           |
|----------|------------------------------------------|----------------|---------|-----------|
| ID       | <b>INFORMATION MANAGEMENT<br/>POLICY</b> | CLASSIFICATION | VERSION | DATE      |
| IS_PL_02 |                                          | FCC_INTERNAL   | 5.0     | July 2026 |

## 2.2 Classification of information

The purpose of the classification of information at FCC is to catalogue the information owned by the Group or stakeholders (clients, partners, collaborators of the Group, etc.) according to its level of confidentiality, as determined by the sensitivity of the information and its potential for disclosure, in order to achieve business objectives.

All information owned by FCC Group or interested third parties must be classified and labeled at the time of its creation, following the Secure Information Management Guide.

Notwithstanding the foregoing, given that the sensitivity and/or criticality of the information may vary during its life cycle as the need or objective for which it was originally created changes, any information may be reclassified at any time, also following the procedure for information reclassification described in the Secure Information Management Guide.

The person responsible for the information will expressly classify the information or, where appropriate, subsequently reclassify it, based on the FCC classification model, which is described below. When the information comes from an external source, the person at FCC responsible for that information must reclassify the information received in accordance with the classification model of the FCC Group, unless there is an express obligation to apply the other party's classification levels or the information has already been previously classified by the other party.

|          |                                          |                |         |           |
|----------|------------------------------------------|----------------|---------|-----------|
| ID       | <b>INFORMATION MANAGEMENT<br/>POLICY</b> | CLASSIFICATION | VERSION | DATE      |
| IS_PL_02 |                                          | FCC_INTERNAL   | 5.0     | July 2026 |

### 2.2.1 FCC Group Information Classification Model

**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 FCC Group's information will be classified into four levels:

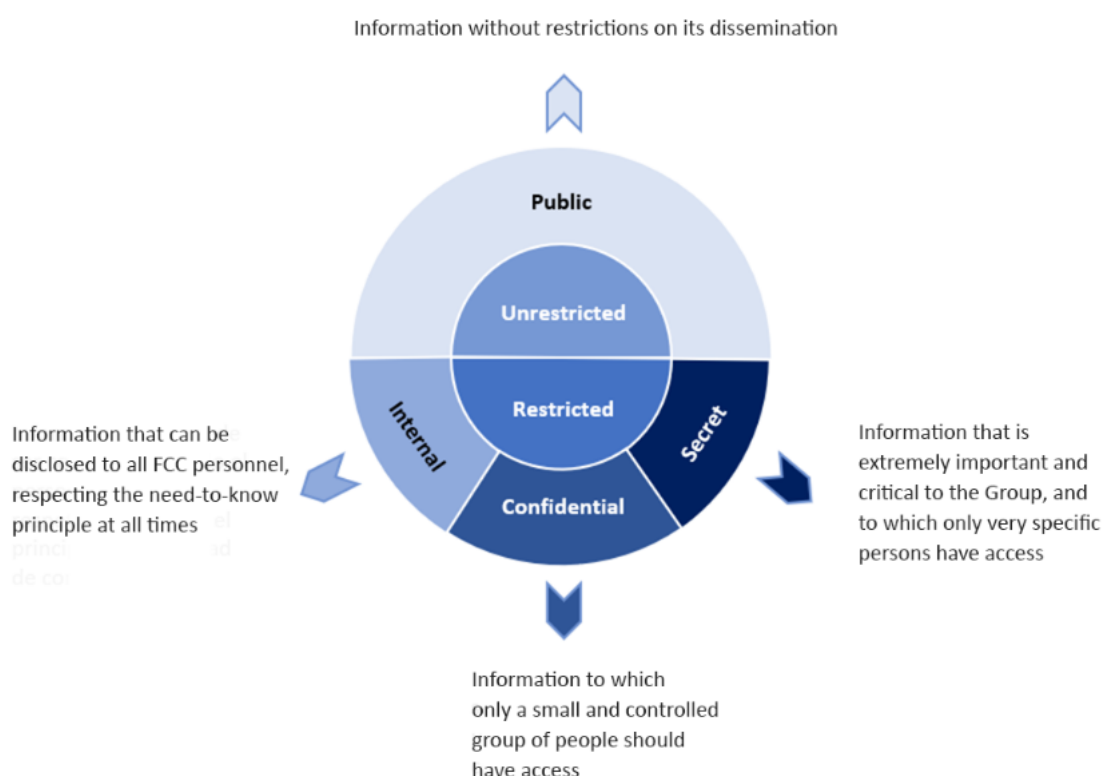


Figure 1. FCC Group information classification scheme

- **Public Use Information:** information that concerns the FCC Group specifically or not, which will be disclosed or published through official channels and, therefore, does not require access limitations. It does not require specific security measures, since the information is intended for publication and/or dissemination without restrictions or limitation of access.
- **Internal Use Information:** information intended solely for use within the organisation, either by FCC Group personnel or interested parties authorised for a limited time for use or access and under the supervision of the person responsible for the information. In general, it is information that if compromised would not cause significant disruption or reputational damage for the FCC Group or interested third parties. It entails security measures that limit its access by personnel unrelated to the FCC Group who do not require said information to meet the objectives of their collaboration with the Group.

|          |                                          |                |         |           |
|----------|------------------------------------------|----------------|---------|-----------|
| ID       | <b>INFORMATION MANAGEMENT<br/>POLICY</b> | CLASSIFICATION | VERSION | DATE      |
| IS_PL_02 |                                          | FCC_INTERNAL   | 5.0     | July 2026 |

This will be the default classification for previously uncatalogued FCC information.

- **Confidential information:** Information intended for a limited and controlled group of people. It is information that, if compromised, could be highly detrimental to the interests of the FCC Group or cause operational difficulties for the organization, its clients or interested parties with whom it collaborates, including sanctions derived from the violation of people's privacy rights. The use and access to this information must be controlled and must be expressly authorised by the information owner. The owner of the confidential information must guarantee adequate security measures that help protect its confidentiality both outside and inside the organisation, limiting its access and distribution to a controlled group of people, who strictly comply with the need-to-know principle.
- **Secret Information:** Information intended for a highly restricted group of people, which, if compromised, could cause an abrupt loss of reputation or competitive advantages. In general, it is information of high value or sensitivity, which must have high security measures to ensure its confidentiality both outside and inside the organization. Access to this information must be highly controlled and must be recorded, periodically verifying that the access and sharing criteria are met.

The FCC Group, through the Information Security department, must guarantee the security of the information by implementing organisational and technical measures that help ensure the privacy and confidentiality of the information, in accordance with its classification

|          |                                          |                |         |           |
|----------|------------------------------------------|----------------|---------|-----------|
| ID       | <b>INFORMATION MANAGEMENT<br/>POLICY</b> | CLASSIFICATION | VERSION | DATE      |
| IS_PL_02 |                                          | FCC_INTERNAL   | 5.0     | July 2026 |

## 2.3 Labeling of Information

All FCC Group information must be properly labeled according to its classification level.

Only the person responsible for the information can label the information for which they are responsible.

When classifying the information, they must include, regardless of the medium where the information is located, one of the following labels, which are mutually exclusive:

- Unrestricted Information Public Use: **FCC\_PUBLIC**
- Restricted Confidential Information: **FCC\_CONFIDENTIAL**
- Internal Use Restricted Information: **FCC\_INTERNAL**
- Restricted Secret Information: **FCC\_SECRET**

Unlabelled information will be considered Internal Use Only, except for information archived prior to the entry into force of this Policy. In this case, it will be classified when it is unarchived.

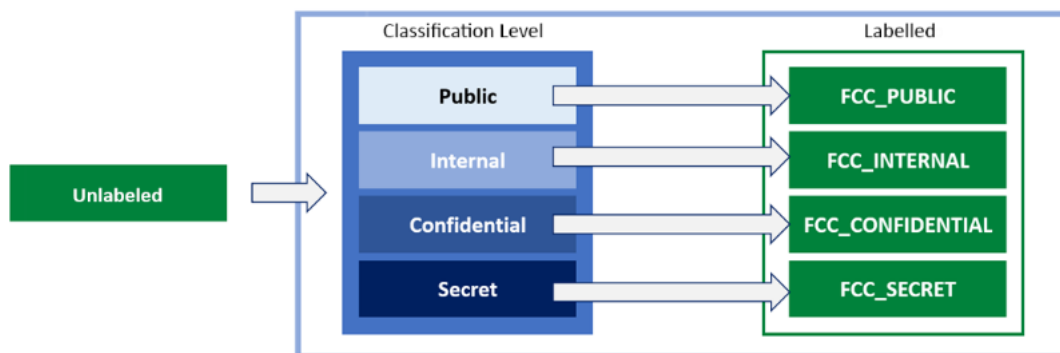


Figure 2. Information labelling scheme of the FCC Group

|          |                                          |                |         |           |
|----------|------------------------------------------|----------------|---------|-----------|
| ID       | <b>INFORMATION MANAGEMENT<br/>POLICY</b> | CLASSIFICATION | VERSION | DATE      |
| IS_PL_02 |                                          | FCC_INTERNAL   | 5.0     | July 2026 |

## 2.4 Information Storage Management

The storage of the information will be carried out in a way that ensures its confidentiality, integrity and availability.

Access to the information will be allowed only to personnel who need to know it in the performance of their duties. In the case of outsourcing the management of information storage, the agreements will establish the minimum applicable security measures and the regime of responsibilities derived from the possible disclosure of said information to unauthorized third parties.

### 2.4.1 Specific management of the storage of Restricted information

The premises, devices and/or media that store **Restricted** information will be equipped with security measures that allow exclusive access to authorized persons.

### 2.4.2 Audit and Information Systems

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

|          |                                          |                |         |           |
|----------|------------------------------------------|----------------|---------|-----------|
| ID       | <b>INFORMATION MANAGEMENT<br/>POLICY</b> | CLASSIFICATION | VERSION | DATE      |
| IS_PL_02 |                                          | FCC_INTERNAL   | 5.0     | July 2026 |

### 3. Responsibilities

**The Cybersecurity Committee** will have the following responsibilities:

- Establish general criteria for the classification and management of information assets.
- Approve the Information Asset Classification and Management Model.

**Information owners** will have the following responsibilities:

- Guarantee the correct classification of the information, and that the people who are under their responsibility and process the information are authorised to do so.

**The FCC staff** will be responsible for:

- Comply with the principles defined in this Policy.

|          |                                          |                |         |           |
|----------|------------------------------------------|----------------|---------|-----------|
| ID       | <b>INFORMATION MANAGEMENT<br/>POLICY</b> | CLASSIFICATION | VERSION | DATE      |
| IS_PL_02 |                                          | 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                                                                                                                                                  |
|----------------|------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>5.1</b>     | Policies for information security                                      | [org.1] Security Policy;<br>[org.2] Security Regulations                                                                                                            |
| <b>5.9</b>     | Inventory of information and other associated assets                   | [op.exp.1] Asset Inventory;<br>[op.pl.2] Security Architecture                                                                                                      |
| <b>5.12</b>    | Classification of information                                          | [mp.info.2] Information Classification                                                                                                                              |
| <b>5.13</b>    | Labelling of information                                               | [mp.si.1] Media Labelling                                                                                                                                           |
| <b>5.14</b>    | Information transfer                                                   | [org.2] Security Regulations;<br>[org.3] Security Procedures;<br>[op.ext.1] Procurement and Service Level Agreements (SLAs);<br>[mp.s.1] Electronic Mail Protection |
| <b>5.34</b>    | Privacy and protection of personally identifiable information (PII)    | [mp.info.1] Personal Data                                                                                                                                           |
| <b>5.36</b>    | Compliance with policies, rules and standards for information security | [org.4] Authorization Process;<br>[op.exp.3] Secure Configuration Management;<br>[op.exp.4] Security Maintenance and Updates                                        |
| <b>8.10</b>    | Information deletion                                                   | [mp.si.5] Deletion and Destruction                                                                                                                                  |
| <b>8.14</b>    | Redundancy of information processing facilities                        | [op.cont.4] Alternative Means                                                                                                                                       |
| <b>8.16</b>    | Monitoring activities                                                  | [op.mon.3] Monitoring;<br>[mp.s.4] Protection against Denial of Service (DoS)                                                                                       |