# FCC Group Access Control Standard

January 2026

| Document Version Control | | | | |
|---|---|---|---|---|
| **Version** | **Date** | **Author** | **Detail** | **Approved by** |
| **1.0** | April 2009 | IS | Document creation | FCC Executive Committee |
| | September 2019 | IS | Document Review | FCC Executive Committee |
| **2.0** | January 2026 | IS | Document Review<br>ISO/IEC 27001:2022<br>ENS | Chief Information Security Officer (CISO) |

# INDEX

# 1. Introduction

This document is part of the FCC Group's Information Security Regulatory Framework, which establishes the Group's mandatory requirements on Information Security.

The Security Regulatory Framework is periodically reviewed and updated by the Information Security Department (hereinafter, the 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 Standard, as well as its relationship and dependence on the rest of the regulatory documents.

This Standard will be reviewed at least once a year unless circumstances recommend or require earlier revision.

## 1.1 Purpose

This Standard aims to define the mechanisms that enable the management of access to the information processed within the FCC Group’s information systems, through controls that ensure such information is only available to duly authorized users.

## 1.2 Scope

This Standard applies to all users, both internal personnel and external collaborators of the FCC Group, who access the information contained in FCC’s information systems, as well as the resources associated with them, as a result of their management and/or use, regardless of:

- The type of access (logical or physical).
- The location from which such access is performed (local or remote).

# 2. Development

## 2.1 Principles

- Access control is justified by the “need-to-know” principle, which requires ensuring that users only access the information or resources for which they have been authorized and that are essential for the performance of their duties.
- By default, defined access profiles shall not be able to access any FCC Group resource until the corresponding permissions have been granted. Profiles constitute specific access-rights groups that reflect the permissions that one or more job positions must have over an information resource or system.
- As a general rule, there must be logical consistency between access permissions and the classification level of the information being accessed.
- Access control mechanisms shall manage access to FCC Group information or resources regardless of the format in which they are presented or the location where they reside.
- Access control shall comply with the minimum-security requirements determined according to the classification level of the information processed, in accordance with the Information Management Policy.
- When an information system processes information classified under several of the levels defined in the FCC Group’s Information Classification Model, the security measures corresponding to the highest classification level shall be implemented.
- Physical access to FCC Group facilities where information systems are located shall be managed in accordance with the Physical Security Standard for facilities.
- When external companies process FCC Group information, both physical access to the facilities where information systems are located and physical or logical access to such systems shall be managed in accordance with the External Companies Standard.
- Access controls to information shall comply with the applicable legislation in force.
- FCC Group access control shall be based on the principle of least privilege, which establishes that each user, process, or system must have only the privileges necessary to perform its specific function and nothing more, thereby minimizing risks associated with unnecessary access to data and resources.

## 2.2 Access Management

- All FCC Group information systems and facilities that process their information shall have access control mechanisms in place that allow activity logging.
- Access shall be based on access profiles that enable the unequivocal and personalized identification of users or entities (e.g., logical items such as robots, machines, devices, or services).
- Access control lists shall be defined for system resources or functions. These lists shall include the different access profiles that have been established.
- Access rights shall be based on reading, writing, and executing permissions.
- Information Owners shall specify who is entitled to use the profiles that process the information for which they are responsible.
- The multiple assignment of identities to a single user or entity shall be formally justified and aligned with business needs or operational requirements.
- FCC has identified three types of access accounts:
    - User Account: An access account granted to an individual for business reasons.
    - Service Account: A user account used by an application or system to automatically access another system.
    - Generic Account: An account with a shared password used by a group of people to access a system. The use of generic accounts shall only be authorized for access to workstations, and a second nominative authentication shall always be required to access any application or production environment.
- The nominal owners of these accounts shall be:
    - The individual to whom the User Account has been assigned.
    - The person designated as responsible for the service in the case of a Service Account.
    - The Information Owner or the person responsible for the accessed application in the case of Generic Accounts.
- The following are prohibited, except in cases duly justified and approved by the IS Department:
    - Service Accounts with system administrator privileges.
    - Generic Accounts.
- When, due to business needs, the creation and use of any of the above account types is required, the parties responsible shall conduct an assessment of the associated risks.
- Activity performed using privileged service accounts or Generic Accounts shall be monitored, and their access shall be recorded in the system audit logs.
- Generally, the application owner should review the access rights granted to users at least once a year. A different period may be established if there is a clear business need; in such cases, it should be documented in the procedures that implement this Standard.
- Each Information Owner shall conduct a review of existing rights, considering:
    - Their continued necessity.
    - The appropriateness of such rights.

- The owner of the Generic Account shall review the access rights associated with that account on a quarterly basis.
- Administrators responsible for creating, removing, or modifying access profiles for systems and resources shall retain copies of the requests for such changes and the corresponding reviews for at least one year after they occur.
- The mechanism for granting access permission shall allow the tracing of changes in privileges and their authorizations. A privilege is understood as the right to perform functions that may bypass security controls.
- Procedures that define applicable requirements and circumstances shall consider each phase of the user access lifecycle, from the initial request to its cancellation or revocation.
- Changes in responsibilities or functions shall entail the modification of authorized rights or the removal of granted access authorizations.
- Applications and systems shall maintain an updated record or registry of users and their access profiles.
- Information systems that use passwords as an authentication method shall comply with the provisions of the Password Security Standard.
- Procedures documenting the use and administration of information systems shall include access control measures and profiles according to the type of access (administrative, user, process, etc.).
- Information systems that process Restricted Information shall be continuously monitored to detect any attempt of unauthorized access or the use of access rights other than those authorized.
- Such monitoring shall record all successful and failed access attempts, including at least the date and time, the user performing the action, the accessed resource, the resource through which the access attempt is made, and the result of the action.

## 3. Responsibilities

The IS Department shall:

- Define the access-control needs for information systems.
- Approve and supervise the controls established for managing access control to information systems.
- Review access audit logs to verify that they are up to date and correspond to the actual needs of users.
- Oversee the follow-up and proper implementation of the provisions of this Standard.

The Information Systems and Technology Division is responsible for:

- Managing:
  - The measures established for access profiles and the access accounts assigned to each profile.
  - The procedures for the implementation and management of access-control mechanisms.
- Monitoring the operation of FCC Group information systems under its control.
- Notifying the IS Department of reported security incidents.

Information Owners shall:

- Define the rights associated with access profiles.
- Formally approve access to the information systems under their responsibility.
- Ensure compliance with this Standard and report any discrepancies observed to the IS Department.
- Inform the IS Department of prolonged user inactivity, whether planned or unplanned.

Users are responsible for:

- Properly protecting their access credentials to FCC Group information systems.
- Understanding the consequences that may arise from non-compliance with this Standard.
- Immediately notifying the IS Department of any suspected violation of this Standard.
- Reporting any incident in which personal data may have been or may be compromised to the DPO/Data Protection Coordinator of the corresponding area.
- Immediately informing the IS Department of the loss, theft, or malfunction of any device.

# 4. Normative reference

This document has been reviewed by the IS Department, and its drafting takes as a reference 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 |
|---|---|---|
| **5.15** | Access Control | [op.acc.2] Access Requirements |
| **5.16** | Identity Management | [op.acc.1] Identification |
| **5.17** | Authentication Information | [op.acc.1] Identification;<br>[op.acc.2] Access Requirements |
| **5.18** | Access Rights | [op.acc.4] Access Rights Management Process |
| **7.1** | Physical Security Perimeters | [mp.if.1] Segregated Areas with Access Control |
| **7.2** | Physical Entry | [mp.if.2] Identification of Individuals;<br>[mp.if.7] Equipment Entry and Exit Logging |
| **7.3** | Securing Offices, Rooms and Facilities | [mp.if.1] Segregated Areas with Access Control;<br>[mp.if.3] Premises Conditioning |
| **7.4** | Physical Security Monitoring | [mp.if.1] Segregated Areas with Access Control;<br>[mp.info.1] Personal Data |
| **7.5** | Protection Against Physical and Environmental Threats | [mp.if.3] Premises Conditioning;<br>[mp.if.5] Fire Protection;<br>[mp.if.6] Flood Protection |
| **7.6** | Working in Secure Areas | [mp.if.1] Premises Conditioning;<br>[org.2] Security Regulations |
| **7.7** | Clear Desk and Clear Screen | [mp.eq.1] Clear Workstation;<br>[mp.eq.2] Workstation Locking |
| **7.8** | Equipment Location and Protection | [mp.if.1] Segregated Areas with Access Control;<br>[mp.eq.3] Portable Device Protection |
| **7.9** | Security of Assets Off-Premises | [mp.eq.3] Portable Device Protection |
| **7.10** | Storage Media | [mp.si.1] Media Marking;<br>[mp.si.2] Cryptography;<br>[mp.si.3] Custody;<br>[mp.si.4] Transport;<br>[mp.si.5] Erasure and Destruction |
| **7.11** | Utilities | [mp.if.4] Electrical Power |

| | | |
|---|---|---|
| **7.12** | Cabling Security | [mp.if.3] Premises Conditioning |
| **7.13** | Equipment Maintenance | [op.exp.4] Maintenance and Updates |
| **7.14** | Secure Disposal or Re-use of Equipment | [mp.si.5] Erasure and Destruction |
| **8.2** | Privileged Access Rights | [op.acc.1] Identification |
| **8.15** | Logging | [op.exp.8] Activity Logging |