FCC Group Systems Laboratory Standard

January 2026

Document Version Control				
Version	**Date**	**Author**	**Detail**	**Approved by**
1.0	April 2009	IS	Document creation	FCC Executive Committee
	October 2019	IS	Document Review	FCC Executive Committee
2.0	January 2026	IS	Document Review ISO/IEC 27001:2022 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 an earlier revision.

1.1 Purpose

The purpose of this Standard is to establish the guidelines that ensure the integrity, confidentiality, authenticity, and traceability of FCC Group Information when carrying out configuration, testing, maintenance, repair, or destruction activities on assets or information systems.

1.2 Scope

This Standard applies to any FCC Group asset or information system on which configuration, testing, maintenance, repair, or destruction activities are performed, regardless of the information it processes or the laboratory in which these activities take place.

2. Development

2.1 Principles

Information security in the FCC Group system laboratories is based on the following principles:

- Laboratories shall provide services exclusively to FCC Group information systems and assets, unless the Information Security Department authorizes support for assets owned by other parties.
- Any task performed on an asset or system in a laboratory shall require an authorization and access process, prior to its execution, by the information owner of the asset. When one or more of the tasks referred to in this Standard are conducted by external collaborators to the FCC Group, the security measures established in the External Companies Standard must be complied with.
- The security measures to be applied in configuration, testing, maintenance, repair, or destruction operations on IT assets shall be proportional to the classification level of the information they contain.

2.2 Systems Laboratories

Systems laboratories must implement a controlled working environment aligned with the protection levels established for the IT resources they operate with. Regardless of their location, systems laboratories must:

- Adopt the principles set out in the Physical Security Standard, the Access Control Standards, and the Configuration and Change Control Standard, with the aim of preventing alteration, loss, processing, and/or unauthorized access to FCC Group information handled by the IT assets used in daily operations.
- Ensure that all assets located in the laboratories are properly identified and recorded. Additionally, all entries and exits of IT assets managed in the systems laboratory must be logged, including those disposed as a result of laboratory operations.
- The entry/exit log must contain at least the following fields regarding the asset or group of assets:
    - Type of asset
    - Date and time
    - Sender
    - Recipient
    - Department/area/company that owns the information
    - Number of assets
    - Method of delivery
    - Authorized person responsible for receipt/delivery
- If any type of security incident occurs while an IT asset is in the laboratory, the associated measures established in the Incident Management Standard must be followed. The security incident must be fully recorded in accordance with the guidelines of the Incident Management Standard and reported to the corresponding information owner.

- When configuration, testing, maintenance, repair, or destruction operations on IT assets are carried out by FCC Group personnel or collaborators outside FCC facilities, measures must be adopted to ensure the protection of information, in accordance with the External Companies Standard and the Policy on the Use of Technological Resources, as well as the Remote Work Security Guide.
- Adopt the necessary measures to prevent any improper recovery of data or information contained in IT assets that leave these facilities as a result of maintenance or destruction operations.

3. Responsibilities

The Information Security (IS) department must:

- Approve and oversee the logical and physical controls established for the management of FCC's IT systems laboratory.
- Analyze any breaches of this Standard that may constitute a security incident.
- Stay informed about and analyze the latest global trends in real vulnerabilities, guide the organization through continuous improvement, and actively contribute to the dissemination of knowledge and best practices.

The Information Systems and Technology Division must:

- Implement operational procedures that ensure the required levels of information security in the laboratories and in the activities conducted within them.
- Record the entry, exit, and destruction movements of IT resources managed in the systems laboratory.
- Inform the IS department of any indication, attempt, or execution of an action contrary to this Standard, or of any anomalous behavior in the access control of applications and systems.

The Information Owner is responsible for:

- Authorizing the configuration, testing, maintenance, repair, or destruction of IT resources that process FCC Information for which they are accountable.

FCC internal personnel and collaborators must:

- Apply the "Zero Trust" methodology as an operating principle in the systems laboratories, ensuring that any access, modification, or creation of assets within them is verified and formally processed.

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
5.8	Information security in project management	[op.pl.3] Acquisition of new components
8.25	Security in the development lifecycle	[mp.sw.1] Application development
8.26	Security requirements in applications	[mp.sw.1] Application development; [mp.s.2] Protection of web services and applications
8.27	Secure systems architecture and engineering principles	[op.pl.2] Security Architecture; [mp.sw.1] Application Development
8.28	Secure coding	[mp.sw.1] Application development
8.29	Security testing in development and acceptance	[mp.sw.2] Acceptance and commissioning
8.30	Outsourced development	[op.ext.1] Contracting and service level agreements; [mp.sw.1] Application development; [mp.sw.2] Acceptance and commissioning; [op.ext.3] Supply chain protection
8.31	Separation of development, testing, and production environments	[mp.sw.2] Acceptance and commissioning