FCC Group Configuration and Change Management 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 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 earlier revision.

1.1 Purpose

The purpose of this Standard is to define the requirements necessary for the management and control of the configuration and change of the components that make up the FCC Group’s information systems.

1.2 Scope

This Standard applies to the processes of identification, control, inventory, and status verification of all components of the FCC Group’s information systems during their design, development, and operation.

The Standard applies to all internal personnel and collaborators of the FCC Group who have assigned responsibilities in the management, control, and use of these processes.

Configuration and change management shall be established, documented, maintained, and applied across all FCC information systems.

2. Development

2.1 Principles

- All information systems used by internal personnel and collaborators of the FCC Group, regardless of ownership, shall have the necessary support and resources for their proper maintenance. The FCC Group shall ensure the implementation of the processes and tools required to comply with the configurations defined in this Standard (including security configurations) for hardware, software, services, and networks, both for newly installed systems and for systems in operation throughout their lifecycle. The acquisition and installation of software, hardware, services (such as cloud services), and network components that have not been previously approved by the Information Systems and Technology Division (hereinafter ISTD) is prohibited.
- The installation of any component within FCC information systems shall be conducted in accordance with the security specifications recommended by the manufacturer and the Information Security Department.
- Configuration and change management for the information systems of internal personnel and collaborators of the FCC Group shall consider the Group-approved Privacy by Design and by Default Procedure.
- Configuration and change management for the information systems of internal personnel and collaborators of the FCC Group shall ensure appropriate segregation of duties and functions in all related activities. For this reason, roles associated with the configuration and administration of components shall be clearly segregated.
- Changes to information systems shall be conducted with the necessary security measures, including the proper deletion/blocking of data in compliance with the GDPR.
- Configuration settings and changes shall be duly verified and validated by qualified FCC Group personnel.
- Configuration and change management shall ensure the availability of all components of the information systems used by internal personnel and collaborators of the FCC Group.
- The established configuration shall be properly documented, and a record of all changes shall be maintained. These records shall be securely stored in accordance with the guidelines of the Physical Security Standard.

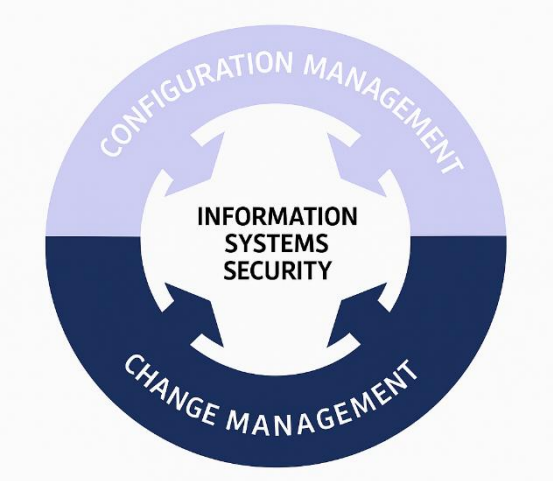

Figure 1: *Configuration and Change Management*

2.2 Configuration Management

One of the key measures to preserve the integrity and availability of information systems is the establishment of strict configuration and change management procedures.

Configuration management procedures shall document the security requirements and the justification for any exceptions that may arise.

The security measures of information systems shall be configured in the most restrictive manner possible and in alignment with the functional requirements established for each system.

2.3 Change Management

- Security modifications, updates, or patches shall only be applied once their needs have been approved. These changes shall originate from trusted sources and shall be evaluated prior to deployment of production systems.
- The components that make up an information system, along with their versioning, shall be documented.
- The use of production data in non-production environments is not permitted. Its use may be approved by the Information Security Department (IS Department) provided that the implemented security controls ensure a level of protection appropriate to the classification level of the information processed.
- If it is not possible to guarantee the required level of security, the execution of tests shall require the approval of the corresponding information owner, and the reasons for non-compliance shall be explicitly recorded in the approval log.
- If a testing environment has been established and it is determined that the required level of security cannot be guaranteed, FCC Group information shall be properly sanitized, and the security requirements necessary to ensure that the controls provide the appropriate level of protection shall be defined.
- Testing procedures for FCC Group information systems shall include a period of parallel operation prior to their transition to production.
- The replacement or withdrawal of information systems and/or assets containing data or information shall require the formal acceptance of the information owner and subsequent approval by ISTD.
- Information systems and/or assets containing data or information that have been replaced or withdrawn shall be disposed of in accordance with media destruction procedures.
- Modifications made to FCC Group information systems shall follow the sequence below:
    - Each change shall begin with a formal request. This request may be submitted by the information owner or by ISTD.
    - Before approving the changes, their potential impact on other systems shall be assessed. This may be conducted through a process-based analysis rather than solely on specific systems.
    - The change shall be authorized by the owner or responsible party of the affected FCC Information Service and by ISTD.

- Modifications and their scope shall be communicated sufficiently in advance to the personnel involved to ensure they are aware of the tasks they must perform.
- In emergency situations, modifications shall be conducted in accordance with the operational procedures established for such purposes, and change and configuration requests may be submitted after the activities have been completed.
- Documentation produced regarding changes and the installation of system software and hardware shall refer to:
    - The management of the specific change or installation process.
    - The change actions were performed.
- These actions shall be recorded in a document that includes, at a minimum:
    - The origin of the change.
    - The type and scope of the action.
    - The techniques used and the sequence of activities.
    - The tests performed and their results.
- Before any change or modification to information systems is moved into the production environment, the following shall be conducted:
    - Proper testing of business functionalities and processing capabilities.
    - Full backups of the FCC Group information systems affected by the change.
- Information system components may only be replaced by authorized personnel, who will ensure sanitization and the elimination of technical risks.
- Preventive maintenance planning for all components of information systems shall follow a defined periodicity, which may include:
    - Monthly maintenance, including log cleansing.
    - Semi-annual maintenance, including configuration review.
    - Annual maintenance, including equipment cleaning.
- Maintenance procedures shall include, at a minimum:
    - Scope
    - Results
    - Timeframe
    - Designated personnel
    - Procedures for prior notification to users regarding maintenance activities

2.4 Procedures

Configuration and change management procedures shall:

- Define:
  - The personnel responsible for performing configuration and maintenance tasks (segregation of duties).
  - Emergency procedures for conducting configuration and maintenance tasks.
  - Procedures for sanitizing any resources that must leave FCC Group facilities due to configuration or maintenance operations.
  - Procedures ensuring that any failure in information systems is reported and recorded in a timely and appropriate manner.
  - Procedures verifying that, after modifications to information systems, the security characteristics in place prior to the changes continue to function correctly.
  - Procedures ensuring the performance of audit activities are associated with changes to the configuration of information systems.
  - Procedures ensuring that all internal personnel and collaborators of the FCC Group receive the necessary training to perform their duties regarding the functionalities and operations of new components.
  - Controls to ensure that configuration and maintenance operations performed by external companies comply with the FCC Group Information Security Regulatory Framework, and in particular with the External Companies Security Standard.
  - The scope and level of monitoring of changes, which shall be determined based on the requirements established in the Information Management Policy; additionally, baseline patterns of normal behavior shall be defined, and any anomalous behavior shall be monitored.
- Identify:
  - The professional and material resources required for maintenance both within and outside FCC Group facilities.

2.5 Documentation

The documentation related to configuration and change management shall contain, at a minimum:

- Version control, which associates system components with the appropriate version, including the changes made in each version.
- The analysis of the impact of proposed changes on existing security controls.
- Procedures for:
    - Evaluate and/or approve information system components before they are moved to production.
    - Ensure the review of functions, controls, and services that may potentially be removed as a result of the changes made.
    - Ensure that contingency plans and associated documentation are updated to reflect the changes.
    - Manage and resolve potential emergencies or revert to a previous state when a configuration or version-change process must be cancelled.
- Requirements ensuring that all installations and modifications of hardware, software, or firmware are conducted in compliance with applicable intellectual and industrial property regulations.
- Estimated useful life of components, to allow their renewal to be planned sufficiently in advance.
- Error logs derived from management operations shall contain, at a minimum:
    - Name and version of the systems involved.
    - Date and time of the incident.
    - Description of the error and the system components involved.
    - Name of the person responsible for resolving the issue.
    - Corrective actions taken.
    - Date and time of incident resolution.

3. Responsibilities

The Information Security Department (IS Department) shall:

- Define the requirements necessary for proper configuration control of information systems.
- Verify audit logs related to errors, unauthorized use, and activity within the FCC Group's information systems.
- Verify the adequacy of documentation related to hardware, software, and firmware changes.

The Information Systems and Technology Division (ISTD) shall:

- Approve components, their installation, maintenance, and removal.
- Perform impact analysis of changes to information system components.
- Develop procedures related to installation, change control, emergency actions, and rollback.
- Manage:
    - Technical requirements, controls, and test plans.
    - Change requests.
    - Coordination of the implementation of approved changes.
- Monitor FCC information systems to ensure compliance with this Standard.
- Ensure that work teams receive the necessary training to perform configuration and change management functions.
- Investigate, in collaboration with the IS Department, incidents or potential security incidents in FCC Group information systems arising from configuration and change management, assessing their impact and possible causes.

Information Owners shall approve:

- Changes to the configuration of information systems.
- The execution of tests when the required security level cannot be guaranteed.

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
5.28	Evidence Collection	[op.exp.7] Incident Management; [op.exp.9] Incident Management Logging
8.9	Configuration Management	[op.exp.2] Security Configuration; [op.exp.3] Configuration Management
8.16	Activity Monitoring	[op.mon.3] Monitoring; [mp.s.4] Protection Against DoS
8.32	Change Management	[op.exp.5] Change Management