FCC Group Development Security

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	Chief Information Security Officer (CISO)
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 precepts on Information Security.

The Security Regulatory Framework is periodically reviewed and updated periodically 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 other 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 ensure that the development and maintenance processes of applications and programs that handle FCC Group information are carried out in a secure environment that incorporates the attributes of confidentiality, integrity, authenticity, traceability, and availability throughout their entire life cycle. A secure environment is understood as the set of people, processes, technologies, and infrastructures involved in the development and integration of systems.

1.2 Scope

This Standard applies to application development and maintenance projects, as well as to programs used within the FCC Group (hereinafter FCC), regardless of where they take place or the personnel involved. Throughout this Standard, the expression “information system development project(s)” refers indistinctly to the development of new information systems for FCC, as well as to the maintenance of existing information systems within the Group.

2. Development

2.1 Principles for Secure Development

- The security measures applied to FCC Information processed in information system development projects must be proportional to the classification level required for such information.
- Projects involving software development must use an appropriate methodology to implement the necessary security measures, whether carried out by internal personnel or external collaborators of the FCC Group, with the aim of producing applications and programs that meet the required security level.
- Those responsible for the development of an information system must properly manage the controls derived from the implementation of the FCC Group's Cybersecurity and Information Security Policy, as well as the needs defined by the business.
- Information system development projects must take place exclusively within development, pre-production, and testing environments.
- When it is necessary to use production data during development or testing, the security measures of these environments must comply with the requirements established in the Password Security Standard, the Access Control Standard, the Cryptography Standard, and all applicable legal regulations.
- The development of information systems and/or software by the FCC Group must take into account the Group-approved Privacy by Design and by Default Procedure, as well as all applicable data protection regulations.
- Production environments must be properly segregated, through logical means, from development and testing environments, ensuring the confidentiality of FCC Information hosted in operational environments.
- Applications must be updated in accordance with:
    - Technological conditions defined by manufacturers.
    - Changes in functionalities related to information security.
    - Applicable legal requirements at any given time.
- Freely available information systems must be acquired only from official and secure sources.
- All changes made to information systems must:
    - Be duly authorized by the information owner.
    - Have properly documented internal functionality, application interfaces, the location of incorporated source code, and records of the operations performed.
- Those responsible must provide FCC personnel only with the information strictly necessary to perform their work within the development project.
- Temporary and test files generated during these projects must comply with the security measures required by the classification level of the FCC Group Information they contain.
- The development of any software must follow the corresponding secure development guidelines applicable to the programming language used.

2.2 Information Security in Development Activities

In general, information system development projects carried out within the FCC Group must:

- Use sufficiently proven methodologies for analysis, design, implementation, documentation generation, and development testing, enabling the creation of information systems that meet the security requirements established by the FCC Group's Information Security Regulatory Framework.
- Keep development tools and integrated development environments (IDEs) up to date.
- Properly ensure the security of FCC Group Information throughout the entire project life cycle.
- Apply best programming practices during the development of information systems and document the code to eliminate defects and prevent the exploitation of vulnerabilities.
- Provide adequate technical and functional training to users on the use of new applications.
- Comply with the Information Security Regulatory Framework during the migration of information systems from a development environment to an integration or production environment. The migration of developments to a production environment must be carried out in a way that does not interfere with information availability.
- Ensure that all proposed developments for an information system are reviewed to verify that they do not compromise the security of the system or the operational environment. These reviews must be performed periodically during development and upon completion.
- Perform proper change management and software version control in accordance with the Configuration and Change Control Standard.
- Ensure that any modifications made to commercial applications used by the FCC Group take into account technical and post-sales maintenance implications and are sufficiently documented to facilitate the installation of future versions of the application.
- Once information system development projects are completed, access to the source code must be safeguarded to protect it from unauthorized access and any manipulation.

2.3 Development of Information Security Functionalities

Information system development projects carried out within the FCC Group must take into account the need to:

- Introduce security requirements from the functional analysis stage of the application.
- Equip applications with security features such as identification mechanisms, authentication, access control, audit logs, and activity records that safeguard the security of the information they process.
- Include mechanisms capable of maintaining control over the processing of FCC Group Information and reporting any errors that occur during processing, thereby preserving the integrity and availability of such information.
- Ensure the integrity of information both at rest and in transit.
- Prepare the functional and security documentation corresponding to the analysis and design stages of the developments.
- Conduct security assessments to audit the security of applications and address potential vulnerabilities.

2.4 Outsourcing of Software Development

External developments must be carried out under a contract that regulates licensing agreements, code ownership, and intellectual property rights related to the subcontracted content, and must also include specifications on the following aspects:

- Security measures for secure design, coding, and testing practices.
- Execution of quality acceptance tests and validation of deliverables, based on security thresholds and minimum acceptable privacy levels.
- Delivery of evidence demonstrating that tests have been performed to protect the data involved against malicious content—whether intentional or unintentional—and against known vulnerabilities.
- Escrow agreement, for example, if the source code is not available, including contractual rights to audit development processes and controls.
- Accurate documentation of the built environment used to create the deliverables.

In addition, a framework of security requirements and controls must be established, focusing on defining the functional and non-functional security controls required when designing, developing, and testing the compliance of applications and web services. To this end, a standard defining an agile development process shall be used as the framework for specifying the tasks the team must implement to produce a secure product.

This standard must properly define security vulnerabilities and ensure the identification and effectiveness of security controls.

New applications must be registered in the FCC Group’s asset inventory, including the agreed information and the association between the application and:

- The business processes it supports.
- The information system.
- The platform on which it runs.

2.5 Security in Development Testing

2.5.1 Security Testing

During the implementation and coding phase of the application, it is recommended that the development area continuously perform security unit tests on the generated code, with the aim of detecting and correcting potential security vulnerabilities as early as possible.

As a prerequisite for moving applications into production, a defined set of security tests must also be carried out to verify compliance with the previously specified security requirements. These tests shall include blackbox security testing (focused solely on access interfaces) and white-box security testing (at the source code level).

System acceptance testing must include evidence demonstrating the application of secure development practices and compliance with minimum security requirements. Testing must also be performed on received components and integrated systems. The FCC Group may use automated tools—such as code analysis tools or vulnerability scanners—and verify the remediation of identified security weaknesses.

Testing must be conducted in a realistic test environment to ensure that the system will not introduce vulnerabilities into the organization’s environment and that the test results are reliable.

2.5.2 Personal Data Used for Testing

Testing related to the implementation or modification of information systems that process files containing personal data shall not be carried out using real data, unless the security level corresponding to the type of file being processed is fully ensured.

3. Responsibilities

The Information Security Department shall:

- Define the security functionalities that must be implemented in applications and programs.
- Verify that the functionalities of applications and development environments comply with the requirements established in the security standards issued by the Group.
- Monitor real-world threats to advise on and update information regarding software vulnerabilities, guiding the organization through secure coding principles and continuous improvement processes.

The Information Systems and Technology Division shall:

- Implement the necessary technical and organizational measures to protect the security of the information processed in development projects.
- Integrate security requirements into the functionalities of applications and programs.
- Validate the technical tests performed on applications and programs, verifying that the required security functionalities are met.
- Maintain a complete and periodically updated inventory of applications, environments, and software versions.

Information Owners shall:

- Propose measures to improve the security functionalities of FCC's information system developments.
- Validate the testing of applications and programs to ensure that the security functions correspond to those defined in the security requirements analysis.

4. Normative reference

This document has been reviewed by the IS Department, and its wording is based on the international standard ISO27001:2022 and the ENS.

4.1 Regulatory controls ISO27001:2022 and ENS

ID Control ISO	ISO/IEC 27001:2022 control	ENS Correspondence
8.27	Secure system 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; [op.ext.3] Supply Chain Protection; [mp.sw.1] Application Development; [mp.sw.2] Acceptance and Commissioning
8.31	Separation of development, test, and production environments	[mp.sw.2] Acceptance and Commissioning
8.32	Change management	[op.exp.5] Change Management
8.33	Test data	[mp.sw.1] Application Development; [mp.sw.2] Acceptance and Commissioning