FCC Group Document Security 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 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 establish the protection measures applicable to documents containing FCC Group information, in order to ensure the confidentiality, integrity, availability, authenticity, traceability, and auditability of such information throughout their life cycle.

1.2 Scope

This Standard applies to all documents that contain information belonging to the Group, regardless of their location and medium.

Hereinafter, the term “document” refers to those that contain information owned by the FCC Group.

2. Development

2.1 Principles

- Documents must be protected from a comprehensive perspective, covering all stages throughout their life cycle, regardless of the format, medium, or means used.
- The organizational and technical protection measures applied to the documents shall be proportional to the risk level of the information they contain and to its classification level, in accordance with the Information Management Policy of the FCC Group.
- Every document must be accessible only to individuals who have a need to know the information contained within it. If the information is Restricted, a Personal Security Clearance shall be required.
- Any document containing Restricted information—specifically, Confidential or Secret—must be encrypted in all states in which it exists, whether at rest and/or in transit, following the measures indicated in the Cryptography Standard.
- The handling of documents by external collaborators must be carried out in accordance with the External Companies Standard of the Group.
- For documents containing information with different classification levels, the specific measures for each level must be applied. If this is not possible, the security measures associated with the highest (most restrictive) classification level must be applied.

2.2 Labelling

- All documents containing FCC Information, regardless of their format or medium, must identify the classification level assigned to the information they contain by clearly and visibly incorporating one of the following mutually exclusive labels:
    - FCC_SECRET
    - FCC_CONFIDENTIAL
    - FCC_INTERNAL
    - FCC_PUBLIC
- Documents labelled “FCC_SECRET” must include a cover page clearly indicating this classification level and the authorized distribution list, in such a way that the content of the document cannot be viewed without opening it.
- Documents that are not labelled with the classification level of the information they contain shall be considered Internal Use, except for those that were archived prior to the entry into force of this Standard. In such cases, they shall be classified when they are retrieved from the archive.

2.3 Storage

- Only those documents containing information necessary for achieving the FCC Group's business objectives may be stored.
- Documents that contravene applicable legislation, public order, morality, or good practices may not be stored.
- Information must be stored on media or devices that ensure its proper handling within the technological environment used by the FCC Group, thereby preventing technological obsolescence or any leakage of content from causing information unavailability.
- When information is stored externally, the agreement between the FCC Group and the provider must specify the security measures to be applied by the provider, the liability framework, and the criteria established in the FCC Group External Companies Security Standard.
- Access to data shall be based on the principle of least privilege and follow the measures described in the Access Control Standard.
- The person responsible for documents containing Restricted Information must maintain an up-to-date list of individuals with authorized access. All restricted information must be safeguarded, stored, and preserved separately from other information.
- Restricted information must be kept in locations with appropriate security measures; unprotected cabinets, unlocked rooms, or public shared network folders for digital media are not permitted.
- Restricted information must not be exposed or left unattended; it must always remain under the custody of an authorized individual or be properly destroyed when no longer needed. Any loss of information must be reported to the Information Owner.
- Restricted information stored on digital media must be encrypted whenever possible.

2.4 Distribution

- Documents containing Non-Restricted Information may be distributed to all individuals who have a need to know, without requiring prior authorization from the responsible party.
- In accordance with the FCC Group External Companies Standard, when document management is outsourced, the agreement governing such service provision must include a confidentiality and non-disclosure commitment applicable to all personnel of the external provider involved in the service.
- When distributing documents to any third party outside the Group, the agreements must include the recipient's obligation to implement the security measures deemed appropriate by the FCC Group, based on the classification level of the information contained in those documents.
- Document distribution shall be carried out through means that ensure:
    - Unequivocal receipt by the recipient or their authorized personnel.
    - Confidentiality, integrity, authenticity, and traceability of the information.
- Any restricted document distributed through a digital channel must use encryption methods. Whenever possible, the use of email for such distribution should be avoided.
- The use of printers should be avoided; only FCC Group-owned and designated printers may be used, and documents must be collected immediately after printing.
- Restricted information contained in properly labelled documents must be distributed on media that do not include labels explicitly indicating the classification level of the information.
- Certified mail with acknowledgment of receipt and hand delivery shall be used whenever restricted information is distributed on physical media. An opaque envelope must be used, and the acknowledgment of receipt must be obtained and archived.
- All additional information contained in hidden fields, metadata, comments, previous revisions, etc., must be removed, except in cases where such information is relevant to the document's recipient.

2.5 Destruction

- Document destruction shall be carried out using methods that ensure the information becomes unrecognizable and unrecoverable, while maintaining the confidentiality of the information throughout the entire process.
- If document destruction is outsourced to specialized providers, the agreements signed must include a confidentiality and non-disclosure commitment applicable to all personnel of the external collaborator who, directly or indirectly, participate in the service, regardless of any additional requirements imposed by applicable legislation based on the nature of the information contained.
- When information destruction is outsourced, the agreement between both parties must require the service provider to issue a destruction certificate guaranteeing that the information contained in the documents has been completely eliminated.
- For each information classification level, procedures must be developed detailing the secure destruction criteria applicable to that level.
- Transport of documents to the location where destruction will take place must be carried out in a manner that ensures no theft, loss, or leakage of information occurs during transit.
- When dealing with electronic documents containing personal data, distribution must be performed by encrypting such data or by using any other mechanism that ensures the information cannot be read or manipulated during transport.

3. Responsibilities

The Information Security Department shall:

- Develop the security criteria for document labelling.
- Approve and/or define the means for distributing and destroying documents.
- Verify document security procedures.
- Ensure the existence of security measures appropriate to the classification level of the information and the type of medium used.
- Guarantee the availability of informational resources regarding document labelling levels and document security.

The Information Systems and Technology Division shall:

- Ensure that information stored in electronic documents is available for use through the processing systems in place at any given time.

Information Owners shall, for their systems:

- Verify access identification and authentication procedures.
- Be aware of the controls implemented for document security.

Users shall:

- Report, with as much detail as possible, any incidents detected related to information documents.

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
5.9	Information and Associated Asset Inventory	[op.exp.1] Asset Inventory; [op.pl.2] Security Architecture
5.10	Acceptable Use of Information and Associated Assets	[org.2] Security Policy; [org.3] Security Procedures; [mp.si.3] Custody
5.11	Asset Return	[org.2] Security Policy
5.12	Information Classification	[mp.info.2] Information Qualification
5.13	Information Labelling	[mp.si.1] Media Marking
7.10	Storage Media	[mp.si.1] Media Marking; [mp.si.2] Cryptography; [mp.si.3] Custody; [mp.si.4] Transport; [mp.si.5] Erasure and Destruction
8.10	Information Disposal	[mp.si.5] Erasure and Destruction

ANNEX I - Recommended Actions by Information Classification

General Information		PUBLIC	INTERNAL	CONFIDENTIAL	SECRET
1. CREATION					
1.1 Marking/Labeling of information					
1.1.1	Change history Document name Summary of changes Date of changes	X	X	X	X
1.1.2	Audit trail table Author (Department + creation date) Approval responsible (Committee + creation date)		X	X	X
1.1.3	Classification and document status	X	X	X	X
1.1.4	Document owner / administrator	X	X	X	X
1.1.5	Distribution control		X	X	X
2. STORAGE					
2.1 Access control					
2.1.1	Reading: no restrictions	X			
2.1.2	Reading: internal users and third parties		X		
2.1.3	Reading: internal users and authorized third parties			X	X
2.1.4	Writing: authorized users	X	X	X	X
2.1.5	Access: all public	X			
2.1.6	Access: user ID + password		X	X	
2.1.7	Access: user ID + password + possibility of requiring MFA				X
2.1.8	Access control audit			X	X
2.2 Storage					
2.2.1	Encryption			X	X
2.2.2	Backups	X	X	X	X
3. DISTRIBUTION					
3.1 Transmission over internal networks					
3.1.1	Intranet (all personnel)	X	X		
3.1.2	Intranet (with access restrictions)			X	
3.1.3	Corporate email without protection	X	X		
3.1.4	Corporate email with encryption protection			X	
3.1.5	Explicit authorization from the owner for its transmission				X
3.1.6	Mandatory document encryption			X	X
3.1.7	Document encryption when necessary		X		
3.1.8	Confidentiality notice in email signature			X	X

ANNEX II - Good Practice Guide for the Use of Information Media

Whenever practical and necessary, authorization shall be requested for the removal or disposal of the Group's media, and an entry-and-exit log shall be maintained.

The Group's media shall always be stored in a secure environment, following the requirements specified by the manufacturer. Such storage must be aligned with the classification of the information contained within the media.

Cryptographic techniques shall be used whenever the integrity, confidentiality, or authenticity of the information stored on the media is considered important.

The Group shall keep the ports intended for removable storage media blocked unless there is an organizational need for their use. If such a need exists, the transfer of information to these storage media shall be controlled.

To prevent unauthorized access, the use of postal or courier services for sending storage media shall be avoided.