FCC Group Backup Management Standard

January 2026

Document Version Control				
Version	**Date**	**Author**	**Detail**	**Approved by**
1.0	April 2009	IS	Document creation	FCC Executive Committee
1.1	July 2014	IS	Document Review	Chief Information Security Officer (CISO)
	September 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 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 preservation and protection requirements necessary to ensure the integrity, confidentiality, and availability of the FCC Group’s information, software and systems throughout the entire lifecycle of backup copies.

1.2 Scope

This Standard applies to the storage devices used by the information systems managed by the FCC Group. Specifically:

- Fixed disks or other non-volatile storage devices, whether operating in isolation or connected to the network.
- Other removable electronic media.

Backup management is understood as the activities of:

- Performing backup copies.
- Conducting recovery and information integrity tests.
- Maintaining and storing the devices.
- Deleting information from backup copies.

The proper execution of these actions will ensure the safeguarding process and the effective recovery of information.

Throughout this Standard, the terms backup copy and backup will be used interchangeably.

2. Development

2.1 Principles

The backup copies performed on the FCC Group's information systems shall be governed by the following principles:

- They shall be documented and planned based on:
  - The criticality of the information processes.
  - The target recovery and restoration times.
  - The retention period of records required by applicable legal provisions.
- They shall be planned considering:
  - The specific measures needed to ensure that information can be recovered in the event of an incident or contingency.
  - Compliance with the requirements defined in this Standard, as well as in related standards.
- They shall be subject, throughout their entire lifecycle, to organizational and technical protection measures proportional to:
  - The level of risk of the information they contain.
  - Their classification level. In this regard, the storage media used for backup copies must be labelled and protected according to the highest classification level of the information they store.
- They shall be stored on devices that:
  - Ensure the availability of the information for as long as it must be retained.
  - Comply, in cases where data must be migrated from one storage medium to another, with the security operating procedures defined for such actions, ensuring that the destination medium provides at least the same level of security as the medium where the information was originally stored.
- They shall be protected, encrypted, labelled, and transported in accordance with the requirements established in the Information Management Policy and in compliance with applicable legislation.

If the FCC Group uses an external service for backup management, it must also be contracted in accordance with the provisions of the External Companies Security Standard.

Figure 1: Backup Management Principles

2.2 Backup Copies

Backup copies of the information systems must be performed ensuring the full recovery of the system in the event of any contingency, safeguarding the confidentiality and integrity of the information processed at every stage of the lifecycle.

Backup copies shall be conducted by authorized personnel trained for the proper performance of such actions.

The frequency for performing backups may be defined in service level agreements, procedures, or user guides of the information systems managed by the FCC Group; in any case, this frequency must always be equal to or less than one week.

Backup procedures shall be automated, in those systems where it is technically possible, to facilitate operational tasks and prevent errors.

During the generation of such copies, as well as any action performed on them, precise and complete audit logs must be generated, indicating who performed the operation, when it was conducted, the reason, and the content of the backup. A code or sequence number must reference the copies.

2.3 Backup Copy Testing

Backup copies and recovery procedures shall be tested at least once a year, ensuring:

- They are capable of correctly recovering the information in case of need or emergency.
- Such restoration meets the target restoration time.
- Recovery tests are conducted in a testing environment where there is no possibility of overwriting the original storage system, thus avoiding irreparable data loss.
- Potential failures during the backup creation process can be detected.

2.4 Information Recovery

Information recovery from backup copies must:

- Be authorized by the information owner or by the person(s) delegated for that action.
- Be conducted, following a formal procedure, by qualified and authorized personnel.
- Be documented in a record detailing the identification of the operation, the storage media used, the information recovered, the results, and any relevant events that may have occurred.

2.5 Backup Copy Retention

Information media containing backup copies must be stored in an appropriate location and at a sufficient distance to protect them from any damage caused by a contingency affecting the site where the primary information systems are located.

A formally documented log of the check-in and check-out of backup copies must be maintained.

Backup copies containing Non-Restricted Information (Public Use) must remain stored for at least one year, with security controls in place to prevent theft and deterioration of the media.

Backup copies containing Restricted Information (Internal Use, Confidential, and Secret) must remain stored for at least two years and be accessible only to properly authorized personnel. Media containing this type of information must be protected against any physical or environmental threat, stored in locked fire-resistant cabinets or in locations with physical or logical access controls that ensure confidentiality and integrity.

Retention periods must comply with applicable legislation or with the needs determined by the information owner.

2.6 Cloud Backup Copies

Cloud backups must:

- Be configured following the recommendations of the cloud service providers contracted by the FCC Group.
- Be monitorable and auditable to identify any type of suspicious activity.

Redundancy in backup copies is recommended. If multiple cloud backups exist, it is advisable to maintain at least one local copy in case errors or issues occur in the cloud.

2.7 Information Deletion

The deletion of backup copies must:

- Be conducted using corporate mechanisms appropriate to the information's classification and the risk associated with its disclosure.
- Result in an irreversible action that prevents the recovery of the information.

If the storage medium does not allow the information to be deleted, its physical destruction must be ensured.

3. Responsibilities

The Information Security Department must:

- Verify the proper implementation of this Standard.
- Verify, where applicable, the encryption method to be used, in accordance with the FCC Information Encryption Standard.

The Information Systems and Technology Division (ISTD) must:

- Manage the security requirements established throughout the entire lifecycle of backup copies.
- Provide the appropriate means for performing backups of the systems managed by ISTD.
- Ensure that all FCC Group information contained in backup copies of systems managed by ISTD can be recovered in any contingency.
- Implement the technical measures necessary to protect the security of the information stored on backup media.
- Configure the audit logs for all actions performed throughout the lifecycle of backup copies.

Information Owners must:

- Classify the information stored on recovery media.
- Authorize the recovery of information contained in backup copies.
- Verify the correct implementation of the controls established in this Standard for the backup copies containing information for which they are responsible.

Users of the information systems must perform backup copies of the information stored in the corporate resources made available to them.

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
5.1	Information security policies	[org.1] Security Policy; [org.2] Security Regulations
5.15	Access control	[op.acc.2] Access requirements
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
8.8	Management of technical vulnerabilities	[op.mon.3] Monitoring; [op.exp.4] Security maintenance and updates
8.12	Data leakage prevention	[mp.com.1] Secure perimeter; [mp.com.2] Confidentiality protection; [mp.si.2] Cryptography; [mp.eq.3] Portable device protection
8.13	Information backup	[mp.info.6] Backup copies
8.17	Clock synchronization	[op.exp.8] Activity logging

ANNEX I - Backup Storage and Transport Procedure

The FCC Group has a procedure that defines the requirements for the transport and storage of Backup Copies. These requirements are included in the contract with the service provider.

ANNEX II - Backup Frequency and Minimum Retention

Information Classification	Minimum Backup Frequency	Minimum Backup Retention
Public Use Information	Weekly	1 year
Internal Use Information	Weekly	1 year
Confidential Information	Weekly	1 year
Secret Information	Weekly	1 year