FCC Group Cryptography 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)
	August 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

This Standard establishes the necessary measures to ensure the confidentiality, integrity, authenticity, traceability, and non-repudiation of information, to provide a higher level of security against unauthorized access, disclosure, or use when information is transmitted or stored. These measures include:

- An information encryption strategy for the entire FCC Group.
- A standardized and appropriate management of information system keys.
- An inventory of permitted cryptographic methods, along with their characteristics and use cases.

Together with this, it defines the assignment, implementation, maintenance, monitoring, and enforcement of the appropriate encryption measures within the Group’s information systems.

1.2 Scope

This standard applies to all digital information of the FCC Group, whether at rest or in transit, whose confidentiality level advises the need to protect it through cryptographic mechanisms, and any deviation must be recorded.

Any implementation that requires the use of cryptography based on information technologies must comply with and adhere to this Standard. This includes:

- Information systems, applications and services, infrastructures, and on-premises platforms.
- User workstations and corporate mobile devices.
- Corporate portable or removable storage devices.
- Information systems, applications, services, and/or storage media (SaaS, IaaS, PaaS) in on-premises or cloud infrastructures.

2. Development

2.1 Principles

The fundamental principles on which this FCC Group Standard is based are the following:

- Information encryption shall be governed by the risk or potential impact of an incident, rather than by the likelihood of such an incident occurring.
- The encryption measures applied to information shall be proportional to the level of risk associated with the information they protect and to its confidentiality level, thereby establishing the type and required quality level of the cryptographic algorithm.
- The products and algorithms selected to encrypt information must:
    - Be certified at an industry level.
    - Be used and managed only by authorized personnel.
    - Be periodically evaluated, approved, and inventoried by the IS Department.
- The implementation strategy must consider the effect of using encryption mechanisms on the performance of the technologies and/or information systems involved, ensuring that their deployment does not degrade the availability of these systems.
- The impact and performance implications of using encrypted information must be assessed in relation to controls whose ultimate purpose is malware content inspection or content filtering.
- The application of encryption measures must be comprehensive and consider:
    - All information requiring protection.
    - All locations where information is stored.
    - All information flows during transitions between systems.
    - The entire lifecycle management of cryptographic keys.
- All cryptographic solutions must be protected against modification and loss. In addition, secret and private keys require protection against unauthorized use as well as against disclosure.
- Appropriate management of cryptographic keys must be conducted through secure procedures for generating, storing, archiving, distributing, recovering, retiring, and deleting cryptographic keys.
- All solutions used for cryptography must be approved by the IS Department.

2.2 Information Identification

All information covered by this Standard is considered sensitive information and therefore must be encrypted before its distribution and/or storage. The encryption solutions used are selected based on the processing and classification level of the information. In general, depending on how the information is handled, it is divided into two main groups:

2.2.1 Information at Rest

Information at rest is information stored in information systems, whether physical or logical.

This category includes, for example, information hosted in databases, files, records, and backups, stored on devices such as servers, cloud services, laptops/desktops, external storage devices, etc.

2.2.2 Information in Transit

Information in transit is information transmitted through networks or communication channels, whether public networks (e.g., the Internet) or private networks (e.g., the corporate LAN). It also includes information moving between different information systems, devices, or applications.

2.3 Encryption Strategy

The purpose of this section is to establish the controls for the proper management of cryptographic processes and the correct management of keys, to protect the confidentiality, availability, integrity, authenticity, traceability, and non-repudiation of information, as well as authentication across all FCC Group systems, services, and/or applications.

The information encryption strategy shall be based on the following technical and organizational measures:

- Encryption may be conducted through hardware and/or software techniques.
- The storage and transmission of information must be encrypted according to the risk and classification level of the information.
- The information and media to be encrypted, using the approved cryptographic methods, shall include:
    - Credentials stored or transmitted by any information system.
    - Especially sensitive personal data (such as data relating to ideology, race, religion, health, etc.) or any personal data that must be encrypted because of the risk assessment of the processing activity.
    - In the case of information classified as Secret or Confidential, the following must be encrypted:
        - Backup copies.
        - Emails.
        - Transmissions sent through the corporate internal network, as well as outside the FCC Group information systems.
        - Communication and access from remote systems or devices.
        - Information stored on any server, workstation, or device when its protection cannot be guaranteed through physical or logical controls and the information is at risk of being compromised or stolen.

2.3.1 Key and Certificate Management

All systems containing encrypted information must have procedures in place for managing cryptographic material, ensuring access to keys, when necessary, segregation of duties, and task rotation. Keys and certificates must be used solely for the purpose for which they were originally issued (for example, document encryption, digital signature, or authentication). This management is based on the following principles:

- Key management, whenever possible, should be conducted using technologies based on directory services, such as Active Directory, with keys stored securely in a location different from where the encrypted information resides.
- The issuance of certificates and keys shall be performed exclusively through authorized and approved certification authorities.
- Possible legal restrictions on the use of cryptographic techniques must be considered before transmitting any encrypted information; for this purpose, the IS Department must be contacted.
- Encryption algorithms and key lengths used shall be reviewed annually to ensure they remain aligned with the latest standards and regulatory requirements.
- The length of encryption keys shall be evaluated in relation to the associated algorithm and the classification level of the information to be protected.
- Encryption, decryption, and key-management functions must be transparent to the user.
- Information Owners shall notify the IS Department of their needs regarding encryption.

3. Responsibilities

The IS Department shall:

- Define the needs for controlling and managing cryptographic techniques.
- Oversee the proper implementation of this Standard.
- Monitor and assess any security incident related to information encryption.
- Define and update an inventory of cryptographic methods.
- Generate intelligence on cryptographic threats and vulnerabilities.

The Information Systems and Technology Division shall:

- Manage:
    - The cryptographic solutions implemented within the FCC Group.
    - The guidelines for the implementation and management of encryption tools, as well as the procedures for the custody and recovery of encryption keys.
- Report to the IS Department any security incidents related to encryption.

Information Owners shall notify the IS Department of their needs regarding encryption.

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
5.1	Information Security Policies	[org.1] Security Policy; [org.2] Security Regulations
5.2	Information Security Roles and Responsibilities	[org.4] Authorization Process
5.3	Segregation of Duties	[op.acc.3] Segregation of Functions and Tasks
5.5	Contact with Authorities	[op.exp.7] Incident Management
5.6	Contact with Special Interest Groups	[org.1] Security Policy
5.7	Threat Intelligence	[op.mon.3] Monitoring
5.8	Information Security in Project Management	[op.pl.3] Acquisition of New Components
5.10	Acceptable Use of Information and Associated Assets	[org.2] Security Regulations; [org.3] Security Procedures; [mp.si.3] Custody
5.12	Information Classification	[mp.info.2] Information Qualification
5.13	Information Labelling	[mp.si.1] Media Marking
5.14	Information Transfer	[org.2] Security Regulations; [org.3] Security Procedures; [op.ext.1] Contracting and SLAs; [mp.s.1] Email Protection
5.15	Access Control	[op.acc.2] Access Requirements
5.36	Compliance with Information Security Policies, Rules and Standards	[org.4] Authorization Process; [op.exp.3] Configuration Management; [op.exp.4] Security Maintenance and Updates
6.7	Remote Working	[org.2] Security Regulations; [mp.per.2] Duties and Obligations
8.1	User Endpoint Devices	[mp.eq.3] Portable Device Protection; [mp.eq.4] Other Network-Connected Devices
8.11	Data Masking	[mp.info.1] Personal Data

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	Backup	[mp.info.6] Backups
8.24	Use of Cryptography	[op.exp.10] Cryptographic Key Protection; [mp.si.2] Cryptography; [mp.info.3] Electronic Signature
8.34	Protection of Information Systems During Audit Testing	[op.exp.2] Security Configuration; [op.exp.3] Configuration Management; [op.exp.4] Security Maintenance and Updates; [mp.s.2] Web Services Protection