FCC Group Network Security Standard

January 2026

Document Version Control				
Version	**Date**	**Author**	**Detail**	**Approved by**
1.0	April 2009	IS	Document Creation	FCC Executive Committee
1.03	December 2011	IS	New chapter “wireless networks” and small changes in some chapters.	Sarto, Magda
1.4	August 2019	IS	Document review, translation update, equivalence with original document	FCC Executive Committee
2.0	January 2026	IS	Document Review ISO/IEC 27001:2022 ENS	Chief Information Security Officer (CISO)

INDEX

1. Introduction 4

1.1 Purpose 4

1.2 Scope 4

2. Development 5

2.1 Network Architecture Design and Development 5

2.2 Network Installation and Configuration 6

2.3 Network Management 7

2.4 Network Interconnection 8

2.5 Wireless Network Security 9

2.5.1 Security Protocols for Wireless Networks 10

2.5.2 Wireless Network for Internal Personnel 10

2.5.2.1 Scope 10

2.5.2.2 Guidelines 10

2.5.3 Guest Wireless Network 10

2.5.3.1 Scope 10

2.5.3.2 Guidelines 10

2.5.4 Wireless Network for Access by Corporate Mobile Devices 11

2.5.4.1 Scope 11

2.5.4.2 Guidelines 11

3. Responsibilities 12

4. Regulatory References 13

4.1 Regulatory controls ISO27001:2022 and ENS 13

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 security requirements for the communication networks of the FCC Group and their interconnection with external networks, in order to ensure the availability, integrity, confidentiality, authenticity, traceability, and auditability of the information transmitted through them, as well as of the information resources connected to them.

1.2 Scope

The Standard applies to all communication networks of the FCC Group and to interconnections with other networks, both public and private. The communication networks include both wired networks and all wireless networks of the FCC Group.

2. Development

2.1 Network Architecture Design and Development

The design and development of the FCC Group's network architecture are fundamental elements for ensuring the security of internal and external information communications. Proper design will support the achievement of security objectives and enable future network growth.

The **principles** that must be considered in the design and development of communication networks to ensure the assigned security levels are as follows:

- Network access must be based on identification, authentication, and authorization criteria prior to connection, complying with the "need-to-know" and "least privilege" principles established in the Access Control Standard.
- The design must consider the availability, integrity, confidentiality, authenticity, traceability, and auditability of the information transmitted through the networks.
- All connections must be blocked unless they have been explicitly authorized (Traffic Control Principle).
- Networks must remain operational and continuously available.
- Technologies used must be market-leading, widely tested in the industry, and based on standards.
- Network segmentation must be carried out into domains according to sensitivity criteria (information classification), business type, functionality (e.g., application servers, databases), and any other necessary criteria.
- All service areas or domains must be protected, both internally and at the perimeter level, through firewall technologies with established security policies and full activity monitoring.
- High availability must be ensured for all components of the perimeter network architecture.
- Services accessible from external networks and/or the Internet must be deployed through an exchange zone commonly known as a Demilitarized Zone (DMZ).
- The security of the FCC Group's communication networks must be multilayered, covering the different types of devices that make up the networks, in order to reduce the impact of potential threats.
- Audit logs must be enabled on network devices to allow analysis and investigation of generated network traffic.
- Network diagrams and device configuration files must be kept up to date as general practice.

2.2 Network Installation and Configuration

The configuration of networks during installation and maintenance stages is essential for achieving the security levels established by the FCC Group for each of its communication networks.

The installation of FCC Group communication networks shall follow these principles:

- All network devices must be located in a secure area with limited and controlled access, in accordance with the FCC Group Physical Security Standard.
- Connection points between FCC Group communication networks and those of telecommunications operators or access providers must be located in secure environments with controlled access.

The configuration of communication networks shall follow these principles**:**

- Communication networks must comply with the security requirements determined by the defined risks and the classification level of the information they process or access.
- All network devices must be protected with passwords in accordance with the Password Security Standard. Accounts for network devices must be created with the minimum level of privileges required to perform their functions.
- All FCC Group networks must follow the FCC Group Addressing Plan.
- Local interfaces of routers connecting to external networks must be configured to accept only incoming packets destined for network addresses within the internal network address space or other trusted networks.
- Access provider network addresses must not be distributed or advertised within the FCC Group communication network.
- DHCP servers must be configured to log client hostnames or MAC addresses, and these records must remain available for a minimum of 7 days on the server itself and for the period defined by the security monitoring directive in an event management system.
- All functions, ports, and services must be disabled except those strictly necessary for the operational functioning of the network.
- All firewalls must be configured with a “deny by default” policy.
- All inbound and outbound traffic to/from the FCC Group network must pass through firewalls and be monitored by Intrusion Detection and Prevention Systems (IDS/IPS).
- All outbound traffic, regardless of destination, must be filtered to verify that the packet’s source address belongs to the local internal network.
- All outbound traffic to external networks must be analyzed using data loss prevention mechanisms to detect unauthorized transmission of restricted information.
- Traffic must be encrypted whenever restricted information is transmitted, whether over the internal network or public networks.
- Network traffic, both internal and external, must be monitored through:
    - Access and activity audit logs
    - Real-time analysis and inspection

- End-user devices connected to the internal network must maintain a private IP address throughout the session to ensure traceability between the IP address and the user.

Where technically feasible, communication networks must:

- Use an authentication server that provides the necessary credentials for administrative access to all network devices.
- Be configured so that all network devices terminate the session through the console port after prolonged inactivity.

2.3 Network Management

The security associated with the management of communication networks must adhere to the following principles:

- All communication networks must operate and be administered using documented procedures that ensure efficient use and effective protection of the information transmitted through them.
- Configuration, update, and change management must be carried out following the established procedures, in accordance with the Configuration and Change Management Standard.
- FCC Group networks must be managed by properly qualified system administrators, who will be responsible for supervising daily operational and security tasks. In addition, system administrator activities must be auditable.
- There must be a dedicated management or administration network, separate from the data network to which all main communication components will be connected and which only network and system administrators may access.
- The connection and use of communication network components—software or hardware—not expressly approved by the FCC Group's Information Systems and Technology Division (ISTD) is strictly prohibited.
- Firewalls must be running at all times and must be centrally administered.
- All systems must be synchronized to the same time.
- The connection between an access provider and the FCC Group must comply with the Group's External Companies Security Standard.

2.4 Network Interconnection

Connections with external networks to FCC, as well as with FCC Group sites that are not integrated into the corporate network and do not share the same security levels, must establish mechanisms that ensure the availability, integrity, confidentiality, authenticity, traceability, and auditability of the information circulating through each of their nodes. For this purpose:

- Contracting Internet connection services must ensure compliance with the provisions of the Law on Information Society Services and Electronic Commerce (LSSICE).
- Connections between external networks and the FCC Group must be carried out in accordance with the External Companies Security Standard.
- Remote access to network resources will be permitted exclusively to users expressly authorized for this purpose, authenticated to the system, with restricted privileges, and with encrypted data whenever the information classification level requires it.
- Connections to any external network outside the FCC Group, as well as to FCC Group sites not integrated into the corporate network, must include the following security measures and systems:
    - Secure connection gateway via VPN, with robust authentication and encryption mechanisms whenever the connection is over a public network.
    - External network Intrusion Detection System.
    - Router with Access Control Lists (ACLs).
    - Firewall.
    - Demilitarized Zone (DMZ) if access to public services is required.
    - DNS (Domain Name Service) servers must not be shared in external network connections.
    - Interconnection between the corporate network and other group sites must be carried out in such a way that the corporate network is the central point of protection and management, avoiding the deployment of firewalls at each site, except when the site has connections to non-corporate networks (Internet, third parties, etc.).
- As a general rule, contracting public network connection services other than those offered by ISTD will not be permitted. In cases where justified business needs require contracting non-corporate services, such connections will be allowed only if the compensatory measures defined by the Information Security department are implemented.

2.5 Wireless Network Security

The following security requirements describe the specific principles that must be implemented for wireless networks, in addition to those already outlined in the previous sections.

The **installation and configuration of FCC Group wireless networks** must comply with the following principles:

- Physical access points must be protected to prevent attempts by tampering. In addition, these devices must be kept away from external sources that may cause electromagnetic interference.
- Signal strength must be set to the minimum level necessary to cover the physical area intended to receive service, in order to prevent the signal from extending too strongly beyond the facilities. Whenever possible, access points should be placed in the center of the room and away from exterior walls and windows.
- Information must be encrypted prior to transmission to protect its confidentiality, integrity, authenticity, and traceability. Encryption must comply with the principles defined in the Cryptography Standard (detailed in the Encryption Procedure).
- Wireless Intrusion Detection/Prevention Systems (IDS/IPS) must be implemented.
- The default SSID must be changed to a name that does not identify the organization.
- In the case of public or guest wireless networks, a firewall must be in place to separate the internal wired network from the wireless network.

Access control for FCC wireless networks must comply with the Access Control Standard, as well as the following specific principles:

- The authentication protocol for wireless networks must be recognized by the industry as secure (see Encryption Procedure).
- Authentication must be delegated to a third party, never to the wireless access point itself. Authentication must be mutual between the client and the access point.
- For networks where users store and transmit confidential information, access must be performed using certificates or another robust authentication mechanism.
- Automatic disconnection of clients after more than 60 minutes of inactivity.
- Client devices must meet a series of requirements before connecting to the wireless network (authorized device, updated antivirus, installed patches, firewall enabled, among others).
- Administrator access to access points must be performed using robust authentication mechanisms. In addition, administrative tasks must be performed “out of band,” through a wired (encrypted) network or locally.

The following wireless network usage scenarios are **not permitted:**

- Ad-hoc networks (direct connections between two or more devices without an access point) in which at least one device has access to the internal network or contains confidential information, unless justified for business reasons and properly controlled.
- Access points not approved by the Information Security department.

2.5.1 Security Protocols for Wireless Networks

The recommendations regarding authentication and encryption protocols for wireless networks, as defined by the industry (Wi-Fi Alliance), are included in the Encryption Procedure.

2.5.2 Wireless Network for Internal Personnel

2.5.2.1 Scope

The wireless network for internal personnel is a network intended exclusively for the connection of corporate laptops. These laptops are configured by ISTD with the FCC Group's default setup, which includes the corresponding certificates for the user's credentials.

2.5.2.2 Guidelines

- Access to this network must be performed exclusively through a certificate installed on the device, and this certificate must be associated with the internal employee's credentials.
- The network must not be accessible to external collaborators and may only be accessed using corporate laptops.

2.5.3 Guest Wireless Network

2.5.3.1 Scope

A guest wireless network is a network provided for individuals external to the FCC Group (suppliers, clients, etc.) who are present at FCC Group facilities and require Internet access. This network does not have access to the internal network.

2.5.3.2 Guidelines

The following guidelines apply to the guest wireless network scenario:

- To grant external user access to the guest network, an FCC Group employee must create the access request by registering it in the Sponsor Wi-Fi Portal. Access may be requested for an individual or for a group, specifying the maximum number of connections. In the latter case, individual identification is not required.
- Responsibility for the guest user's use of the network will always fall on the employee who created access.

- The maximum duration of user authentication is one working day. After this period, access is automatically revoked. Access will also be automatically revoked at 24:00 on the day the request was created.
- Access may be created for up to 7 days. This period may be extended if there is a justified business need.
- Guests may connect to this network using a maximum of 3 devices.
- In all cases, the guest wireless network must remain segregated from the corporate internal network. Additionally, users connected to this network must not have visibility of other users connected to it.

2.5.4 Wireless Network for Access by Corporate Mobile Devices

2.5.4.1 Scope

The wireless network for access by corporate mobile devices is a network provided for FCC Group personnel who require Internet access on their mobile devices. This network is segregated from the corporate network and does not have access to the internal network.

2.5.4.2 Guidelines

The following guidelines apply to accessing wireless networks without a certificate through corporate mobile devices:

- Access is permitted for all internal FCC Group personnel.
- To access this network, users must request access through a form or have a corporate MDM installed on their device.
- Access requests must be processed through the Global Service Desk, which will carry out the necessary steps to grant access.
- The maximum duration of access to this wireless network is 1 year.
- The user may only connect from the device identified during the registration process.
- During the first connection, the user will be shown the access terms, which must be accepted in order to proceed.
- In all cases, the wireless network for mobile device access will remain segregated from the corporate internal network.

3. Responsibilities

The Information Security (IS) Department must:

- Define the security requirements for the FCC Group's communication networks.
- Propose and coordinate network audits, intrusion tests, and vulnerability scans deemed necessary to maintain the security level of communication networks.
- Report on the vulnerability tests performed, as well as the actions taken, conclusions, and recommendations following the investigation of any security incident or potential incident.
- Verify the implementation and effectiveness of network security controls and monitoring.
- Monitor network traffic in real time to detect unauthorized use, intrusion attempts, and the compromise of any network device.
- Define web-filtering guidelines to reduce exposure to malicious content.

The Information Systems and Technology Division (ISTD) must:

- Define and keep updated:
  - The architecture for network connection and interconnection, as well as the Network Addressing Plan.
  - The FCC Group's network topology, especially regarding all external and internal links, subnets, and network equipment.
- Develop procedures for securing network components.
- Maintain an inventory of network elements, including authorized wireless access points.
- Review all connection requirements at least every six months to ensure they remain valid and assess the status of undocumented networks discovered during inspections.
- Establish the technical mechanisms necessary to keep all network components synchronized in time.
- Inform the SI department of any security incident or potential incident affecting FCC communication networks.
- Define the needs of the respective business areas regarding communication network security.

Users must:

- Immediately notify ISTD of any failure detected in network systems and/or resources.
- Use network resources exclusively for purposes related to their duties within FCC, and in general according to the Technology Use Policy regarding the use of systems over the network.

4. Regulatory References

This document has been reviewed by the Information Security (IS) Department, and its content is based on the international standard ISO 27001:2022 and the National Security Scheme (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
5.37	Documented Operating Procedures	[org.3] Security Procedures
8.7	Protection Against Malware	[op.exp.6] Protection Against Malicious Code
8.10	Information Disposal	[mp.si.5] Deletion and Destruction
8.20	Network Security	[mp.com.1] Secure Perimeter
8.21	Security of Network Services	[mp.com.2] Confidentiality Protection, [mp.com.3] Integrity and Authenticity Protection
8.22	Network Segregation	[mp.com.4] Separation of Information Flows
8.23	Web Filtering	[mp.s.3] Web Browsing Protection
8.24	Use of Cryptography	[op.exp.10] Cryptographic Key Protection [mp.si.2] Cryptography [mp.info.3] Electronic Signature
8.27	Secure System Architecture and Engineering Principles	[op.pl.2] Security Architecture; [mp.sw.1] Application Development
8.31	Separation of Development, Test, and Production Environments	[mp.sw.2] Acceptance and Commissioning
8.32	Change Management	[op.exp.5] Change Management