FCC Group Portable Devices Standard

January 2026

Document Version Control				
Version	**Date**	**Author**	**Detail**	**Approved by**
1.0	April 2009	IS	Document creation	FCC Executive Committee
2.0	February 2013	IS	Document Review	Policy Committee
2.1	July 2014	IS	Document Review	Chief Information Security Officer (CISO)
	September 2019	IS	Document Review	Chief Information Security Officer (CISO)
3.0	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 security criteria and measures necessary to ensure the confidentiality, integrity, authenticity, traceability, availability, and auditability of the FCC Group’s information accessed and/or processed through mobile devices used by employees and collaborators.

1.2 Scope

This Standard applies to:

- Corporate mobile devices provided by the FCC Group to its employees or collaborators.
- Personal mobile devices that are authorized to access FCC Group information resources.

The supported manufacturers and models shall be those determined by the Information Systems and Technology Division (hereinafter ISTD) and the Information Security department. Laptop computers are not included within the scope.

2. Development

2.1 Definitions

Mobile device: A small-sized device with processing capability, data network connectivity, and memory. Currently, the most used and well-known mobile devices are smartphones and tablets. Another type of device, mainly used for field work, is the so-called rugged devices, which are specifically designed to operate reliably in harsh environments and conditions, such as strong vibrations, extreme temperatures, and humidity or dust exposure.

Types of mobile devices depending on ownership:

- Corporate device: Provided by the FCC Group to employees or collaborators who access the FCC Group's information systems.
- Personal device: Owned by employees or collaborators and used under authorization to access the FCC Group's information systems.
- External company device: Provided by an external company to its collaborator and used under authorization to access the FCC Group's information systems.

2.2 Mobility Principles

The use of mobile devices to access corporate information is based on the following principles:

- The use of mobile devices to access the FCC Group's information systems shall be permitted only when the following conditions are met:
    - It must be previously authorized by the user's hierarchical superior (from Department Director or Delegate onwards), for business reasons.
    - Users shall only have access to those resources necessary for the performance of their duties.
- All mobile devices connected to the FCC Group's information systems shall have implemented the security profiles and/or controls established by the FCC Group.
- The selection of such profiles and security controls shall be determined by the classification level of the information accessed, the user's role, and the associated risks.
- All devices accessing the FCC Group's information systems shall be registered and monitored.
- The FCC Group should monitor only the corporate-use information of the device.
- In accordance with the Access Control Standard, any change in functions or termination of activity by users shall entail the revocation or removal of all access to the FCC Group's information systems.

2.3 Conditions for the Use of Mobile Devices

Authorized users accessing the FCC Group's information systems through mobile devices must accept the following conditions prior to such access:

- The FCC Group reserves the right to implement or require the minimum and necessary security measures on mobile devices that access corporate resources.
- Users must not disable any security measure that the FCC Group has implemented or required, and must configure the device according to the security specifications issued by the Information Security department:
    - In general, the device must be kept up to date (Operating System version and other software), users may not bypass manufacturer-imposed restrictions (jailbreaking) and must follow the FCC Group's guidelines regarding the installation of applications and obtain them through official repositories.
- The FCC Group may deny access when the device does not comply with the required security measures and configuration.
- The FCC Group will monitor the proper use of mobile devices when corporate information is managed.
- Users must immediately hand over the mobile device, without tampering, if required for judicial investigations or internal audits.
- In case of loss or theft of the device, the user must inform the user support service (Global ServiceDesk) as soon as possible. The FCC Group may remotely delete the data and configuration stored on the device.
- In the specific case of using devices not provided by the FCC Group, the following additional conditions shall apply:
    - With a personal device, users may only access corporate information through applications approved by the Information Security department, and only if the corporate MDM tool is installed on the device.
    - Users will receive technical support only for applications related to their professional activity.
    - The FCC Group is not responsible for the loss of personal data on mobile devices. Users are responsible for backing up their personal data if they consider it necessary.
- FCC Group users and collaborators must delete all corporate information stored on the device when it is no longer in use due to malfunction, replacement, or due to the user's termination of activity or change of duties (and the device is no longer required for their new functions).
- Users are responsible for the use and safekeeping of mobile devices to prevent loss, theft, damage, or deterioration.
- In addition to the conditions specified in this section, users must be aware of and comply with the rules described in the Technology Media Use Policy.

2.4 Security Measures

This section describes the set of measures to protect FCC Group information that is transmitted, accessed, and/or stored through mobile devices.

The mandatory nature and level of implementation of each security measure will depend on the classification level of the information accessed, the user profile, the technology, and the associated risks, and will be determined by the Information Security department.

Access Control

- Devices must have authentication mechanisms in place prior to accessing the FCC Group's information systems.
- When the authentication mechanism is based on passwords, these must follow the guidelines of the FCC Group Password Standard, specifically the section applicable to mobile devices.
- If another type of authentication mechanism is used, the Information Security department must evaluate it.

Data Protection. Information Leakage

- Corporate information, during access, transmission, and processing, must be isolated or separated from personal information stored on the mobile device.
- Corporate information must reside in the FCC Group's information systems; otherwise, any corporate information stored locally on the device must be encrypted in accordance with the Cryptography Standard.
- All applications that manage corporate information, such as email, must include measures to prevent information leakage.

Theft and Loss

- Remote wipe mechanisms must exist in case of loss or theft of the device.

Device Compliance

- The device must be updated with the latest versions and patches provided by the manufacturer.
- Devices in which manufacturer-imposed protections and restrictions have been removed (commonly known as "jailbreak") will not be accepted.
- Mechanisms must exist to verify that, prior to connecting to corporate resources, the device has the appropriate security level (e.g., updated with the latest versions and patches, PIN enabled, etc.).

Communication Security

- When corporate information is transmitted over public networks, it must be done through encrypted channels between the mobile device and corporate services.

- Within FCC Group facilities, mobile devices may connect only to guest Wi-Fi networks.

Auditability

- The FCC Group's information systems will collect logs of the connections made by mobile devices to FCC resources.

Mobile Device Applications

- The FCC Group may block access to corporate information from applications considered unsafe.
- Any development or acquisition of corporate mobile applications must be reviewed in advance by the Information Security department to include security requirements, and subsequently for security testing prior to production deployment.

Device Inventory

- There must be an inventory or registry of all devices capable of connecting to FCC Group information resources, along with the person associated with each device.

End of Device Use by Employees

- When a device is no longer in use due to malfunction, replacement, or due to the user's termination of activity or change of duties (and the device is no longer required for their new functions), all corporate information stored on the device must be deleted.

Antimalware

- The presence of antimalware protection on all mobile devices is recommended.

3. Responsibilities

The hierarchical superior (from Department Director or Delegate onwards) shall:

- Authorize cases in which a user (under their hierarchical responsibility) needs to use a mobile device—whether provided by the FCC Group or personal—to access Group information, always with a justified business reason.

The Information Security department (IS) shall:

- Define the requirements and necessary measures to maintain security in the access of mobile devices to corporate information and resources.
- Define the appropriate rules and procedures to ensure acceptable use of FCC Group information through corporate mobile devices.
- Supervise that security measures are correctly implemented on the devices.
- Be aware of the information security risks associated with the use of mobile devices and vendor products.
- Monitor the access of mobile devices to the FCC Group's information systems.
- Conduct user audits, when necessary and without prior notice, to ensure the confidentiality, integrity, authenticity, traceability, and availability of FCC Group information.
- Analyze and authorize exceptions to this Standard.

The Information Systems and Technology Division shall:

- Implement the technical measures required to comply with this Standard, according to the specifications of the Information Security department.
- Enable access to corporate resources through mobile devices, provided the request is authorized, and implement the necessary security controls.
- Maintain an up-to-date inventory of mobile devices distributed and authorized by the FCC Group.
- Manage incidents related to mobile devices.
- Maintain a list of the mobile device technologies and manufacturers supported within the FCC Group.

Users shall:

- Accept and comply with the conditions for the use of mobile devices specified in this Standard and in the Technology Media Use Policy.
- Be responsible for the use and safekeeping of mobile devices that have access to FCC Group resources.
- Report without delay to the user support service (Global ServiceDesk), or otherwise to the Information Security department, any security incidents.

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
5.9	Information inventory and other associated assets	[op.exp.1] Asset Inventory; [op.pl.2] Security Architecture
5.10	Acceptable use of information and other associated assets	[org.2] Security Regulations; [org.3] Security Procedures; [mp.si.3] Custody
5.11	Return of assets	[org.2] Security Regulations
5.12	Information classification	[mp.info.2] Information Classification
5.13	Information labelling	[mp.si.1] Media Labelling
5.15	Access control	[op.acc.2] Access Requirements
5.17	Authentication information	[op.acc.6] Authentication Mechanisms
5.19	Information security in supplier relationships	[op.ext.1] Contracting and Service Level Agreements
5.20	Addressing information security in supplier agreements	[op.ext.1] Contracting and Service Level Agreements
5.21	Information security in the ICT supply chain	[op.ext.3] Supply Chain Protection
6.7	Remote working	[org.2] Security Regulations; [mp.per.2] Duties and Obligations
7.7	Clear desk and clear screen	[mp.eq.1] Clear Workspace; [mp.eq.2] Workstation Locking
7.8	Equipment location and protection	[mp.eq.3] Portable Device Protection
7.9	Security of assets off-premises	[mp.eq.3] Portable Device Protection
7.10	Storage systems	[mp.si.1] Media Labelling; [mp.si.2] Cryptography; [mp.si.3] Custody; [mp.si.4] Transport; [mp.si.5] Erasure and Destruction
7.11	Utility services	[mp.if.4] Electrical Power
7.12	Cabling security	[mp.if.3] Facilities Conditioning

7.13	Equipment maintenance	[op.exp.4] Maintenance and Security Updates
7.14	Secure disposal or reuse of equipment	[mp.si.5] Erasure and Destruction
8.1	User endpoint devices	[mp.eq.3] Portable Device Protection; [mp.eq.4] Other Network-Connected Devices