FCC Group Password Security Standard

January 2026

Document Version Control				
Version	**Date**	**Author**	**Detail**	**Approved by**
1.0	April 2009	IS	Document Creation	Chief Information Security Officer (CISO)
2.1	February 2012	IS	General update and integration with the password security procedure	Chief Information Security Officer (CISO)
	October 2019	IS	Document Review	Chief Information Security Officer (CISO)
2.2	June 2020	IS	Update of the Password Standard and General Review	Chief Information Security Officer (CISO)
2.3	April 2021	IS	Password Management System Update and General Review	Chief Information Security Officer (CISO)
3.0	July 202	IS	Document Review Unification of the format with the rest of the Regulations	Chief Information Security Officer (CISO)
3.1	May 2025	IS	Review of the document and adaptation to regulations ISO27001:2022 and ENS	Chief Information Security Officer (CISO)
3.2	January 2026	IS	Document Review	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 objective of this Standard is to establish, manage, and promote best practices in the creation and use of passwords in the FCC Group’s systems, in order to ensure an appropriate authentication process and prevent failures during the process.

1.2 Scope

This standard applies to all internal staff and collaborators of the FCC Group who use passwords as an authentication mechanism to access:

- FCC Group information systems.
- Data storage systems.
- Corporate technological devices and media.
- Information processing facilities.

2. Development

2.1 Principles

- Information systems that use passwords as an authentication method must incorporate a password management system to ensure their security and quality.
- All passwords are personal and non-transferable. All personnel with access to FCC Group technological resources must manage their passwords in a strictly confidential manner and comply with the guidelines for the proper selection and use of passwords described in this standard.
- The provision of passwords shall be carried out in a way that ensures availability, confidentiality, integrity, authenticity, and traceability.

2.2 Password Management System

The password management system must comply with the following set of rules to ensure good quality and correct management.

2.2.1 General rules

- All user accounts must be protected by a password that can be freely modified by the user and must have a procedure to resolve errors in character entry.
- The user must be forced to change the password after the first login.
- Prevent the reuse of previous passwords.
- Do not display the password on screen during its entry.
- The user must never access another user's password, nor modify other users' passwords, without the express authorization and prior knowledge of the information owner.
- The user must not share accounts or passwords with other users, even if they are superiors or collaborators, nor discuss them in public.
- The user must not write down passwords on visible or easily accessible physical or digital media, nor store them on technological media without protection.
- The minimum password length must be 12 characters.
- Passwords must combine different typographic characters: uppercase, lowercase, numbers, and special characters.
- Easily predictable character sequences and/or those containing personal information about the user are prohibited.

- Password expiration must be as follows:
    - Personal user passwords (FCC network accounts, email accounts, web services, etc.) must expire every six months.
    - Personal administrator passwords (operating systems, databases, applications, communications, etc.) must be changed at least once every six months or when they leave the organization or change their role.
    - System and/or service account passwords not associated with a person may have no expiration date but must be changed at least once a year.
- The last 10 passwords must not be allowed to be reused.
- First access to the system must require a change of the initial password.
- The password must be changed if there is any indication that it may be compromised.
- Repeatedly changing passwords to retain the initial password is not allowed.
- Whenever possible and appropriate, use the two-factor authentication provided by the FCC Group to access information systems or technological resources.
- Use secure, official, and previously authorized password managers approved by the IS Department.

2.2.2 Login

- The display of passwords at the moment of their entry is strictly prohibited.
- Login must be blocked after five failed access attempts for at least 15 minutes. After that period, access may be attempted again.
- The “Remember password” option offered by some applications, such as web browsers or email, must not be used.

2.2.3 Session Lock

- Workstations will automatically lock the session after fifteen (15) minutes of inactivity. In addition, the user must manually lock the session when leaving the computer unattended.
- In the case of business applications and depending on the risks, a password lock due to inactivity may be added, with a period sufficient for it to take effect but not cause continuous interruptions for users.

2.2.4 Storage and Transmission

Authentication systems must store and transmit passwords in an encrypted manner and aligned with the guidelines of the Cryptography Standard.

2.3 Password Provisioning

- The delivery of any password after creating a user account must be carried out through a secure and private environment (examples: email, sealed envelope, personal telephone) to the requester.
- In the event of password restoration, delivery will be made directly to the user. In these cases, it is essential to securely identify and authenticate the requester to prevent identity impersonation.
- In all cases, the default password will be temporary and must be changed after the first access.
- The supplied password will be temporary and must be modified during or immediately after its reception by the user. It will be valid for 21 calendar days from its creation.
- Default passwords for any system supplied by manufacturers must be changed during or immediately after the installation of the products.

2.4 Selection and Use of Appropriate Passwords

Regardless of the measures implemented in the management of system passwords, all users must comply with the guidelines for the selection and proper use of passwords detailed in the Policy for the Use of Technological Resources.

2.5 Passwords on Mobile Devices

Passwords used on mobile devices, due to their nature, must have different security characteristics. The following conditions must be met:

- Passwords must have a minimum length of 6 characters.
- It is recommended to include at least one letter of the alphabet and one number.
- The user must not associate them with personal or easily guessable information, such as: “0000”, “9999”, date of birth, current date, vehicle registration number, etc.
- The device must lock after 10 failed attempts. After the lock, password retry will be prohibited for a determined period of time.
- The device may require re-entry of the password after five minutes of inactivity.
- The password must be changed every 6 months.
- Unlock patterns must not be used as passwords.

Any case where it is not possible to comply with the above conditions due to technical limitations of the technological device or when using a mechanism different from password-based authentication must be evaluated and approved by the IS Department.

3. Responsibilities

The IS Department must:

- Coordinate the security tasks related to the creation, safeguarding, and control of passwords.
- Monitor failed access attempts associated with incorrect passwords of authorized users.
- Inform users of the requirements established in this Standard.
- Develop the operational guidelines for implementing the Password Security Procedure.

The Information Systems and Technology Division (ISTD) must ensure that all administrators can:

- Generate and manage all system and application passwords under their control, in accordance with this Standard.
- Inform the IS Department of any suspicion regarding the disclosure of a password.

FCC personnel must:

- Safeguard their passwords from any possible loss, theft, or disclosure.
- Understand the consequences of violating this Standard and assume the responsibilities that may arise from such violation.
- Report immediately to the IS Department any suspicion regarding the security of passwords.

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
5.10	Acceptable use of information and other associated assets	[org.2] Security Regulations; [org.3] Security Procedures; [mp.si.3] Custody
5.17	Authentication information	[op.acc.6] Authentication mechanisms (organization users)
5.18	Access rights	[op.acc.4] Access rights management process
8.2	Privileged access rights	[op.acc.2] Access requirements
8.3	Restriction of access to information	[op.acc.3] Segregation of functions and tasks
8.5	Secure authentication	[op.acc.6] Authentication mechanisms (organization users)