Password Security Standard

of the FCC Group

May 2025

Version History			
Version	**Date**	**Author**	**Detail**
1.0	April 2009	IS	Document Creation
2.1	February 2012	IS	General update and integration with the password security procedure
	October 2019	IS	Document Review
2.2	June 2020	IS	Update of the Password Standard and General Review
2.3	April 2021	IS	Password Management System Update and General Review
3.0	July 2021	IS	Document Review Unification of the format with the rest of the Regulations.
3.1	May 2025	IS	Review of the document and adaptation to regulations ISO27001:2022

INDEX

1. Introduction

This document is part of the FCC Group's Information Security Regulatory Framework, which develops the Group's mandatory precepts on Information Security.

The Security Regulatory Framework is reviewed and updated periodically by the Information Security Department (hereinafter 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.

1.1 Object

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 means.
- 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 the security and quality of passwords.
- All passwords are personal and non-transferable. All personnel with access to the FCC Group's technological resources must manage their passwords in strict confidentiality and comply with the guidelines for the selection and proper use of the password described in this standard.
- The provision of passwords will be developed in such a way as to guarantee confidentiality and integrity.

2.2 Password Management System

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

2.2.1 General rules

- All user data accounts must be protected by a password that can be freely modified by the user and have a procedure for resolving errors in character entry.
- The user must be forced to make a password change after the first login.
- Prevent the reuse of previous passwords.
- Do not display the password on the screen during its entry.
- The user must never access the password of another user, or modify the passwords of other users, without the express authorization and prior knowledge of the person responsible for the information.
- The user must not share accounts and passwords with other users, even if they are superiors or collaborators, or talk about them in public.
- The user must not write down passwords on visible or easily accessible physical or digital media, nor store them on an unprotected technological medium.
- The minimum password length must be 12 characters.
- Passwords must combine different typographic characters: uppercase, lowercase, numbers, and special characters.

- Sequences of characters that are easily predictable and/or contain personal information of the user are prohibited.
- The password expiration must be as follows:
    - Personal user or user passwords (FCC network accounts, email accounts, and web services, etc.) must expire in six months.
    - Personal administrators' passwords (operating systems, databases, applications, communications, etc.) should be changed at least once every six months or, in case they are disengaged or change activity.
    - Passwords for system and/or service accounts that are not associated with a person may not have an expiration date but must be changed at least once a year.
- The last 10 passwords should not be repeatable.
- First access to the system must require an initial password change.
- The password should be changed in case there is any indication of being compromised.
- It is not allowed to change passwords repeatedly to keep the initial password.
- Use, whenever possible and convenient, the double authentication factor that the FCC group makes available to the user to access information systems or technological means.
- Use secure, official password managers previously authorized by the IS department.

2.2.2 Login

- It is strictly forbidden to display passwords at the time of their entry.
- The login must be blocked after five failed login attempts for at least 15 minutes. After that period, access can be retried.
- You should not use the "Remember Password" option offered by some applications, such as web browsers or email.

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.

- For enterprise applications, depending on the risks, an inactivity password lock may be added, with sufficient time to take effect but not cause ongoing disruption to 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 Provision

- The delivery of any password after creating a user account must be done through a secure and private environment (examples: email, stamping, personal phone) to the requestor.
- In the event of password restoration, the password will be delivered directly to the user. In these cases, it is essential to securely identify and authenticate the requester, to prevent identity theft.
- In all cases, the default password will be temporary and shall be changed after the first access.
- The password provided will be temporary and must be modified during or immediately after receipt of the password by the user. This will be valid for 21 calendar days from its creation.
- The default passwords for any system supplied by the manufacturers must be changed during or immediately after the installation of the products.

2.4 Selecting and Using Proper 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 the password detailed in the Policy for the use of technological means.

2.5 Passwords on Mobile Devices

Passwords used on mobile devices, by their nature, must have different security features. The following conditions must be met:

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

Any case in which it is not possible to comply with the above conditions due to the technical limitations of the technological device or when a mechanism other than password authentication is used, must be evaluated and approved by the IS department.

3. Responsibilities

The IS department must:

- Coordinate security tasks related to the creation, safeguarding, and control of passwords.
- Monitor failed login attempts associated with password failures for authorized users.
- Inform users of the requirements established in this Standard.
- Prepare the operational guidelines to develop the Password Security Procedure.

The Information Systems and Technology Division should ensure that all admins are able to:

- Generate and manage all passwords for systems and applications under their control, in accordance with this Standard.
- Report any suspicion about the disclosure of a password to the IS department.

FCC staff must:

- Safeguard their passwords from any potential loss, theft, or disclosure.
- Understand the consequences of a violation of this Standard and assume any responsibilities that may arise from such a violation.
- Immediately inform the IS department of any suspicions about the security of the passwords.

4. Normative reference

This document has been reviewed by the IS department and its wording takes as a reference the international standard ISO27001:2022.

4.1 Regulatory Controls ISO27001:2022

Control Type	Control ID	Control
ORGANIZATIONAL CONTROLS	**5**	5.10 Acceptable Use of Information and Other Associated Assets 5.17 Authentication Information 5.18 Access Rights
TECHNOLOGICAL CONTROLS	**8**	8.2 Privileged Access Rights 8.3 Restricting Access to Information 8.5 Secure Authentication