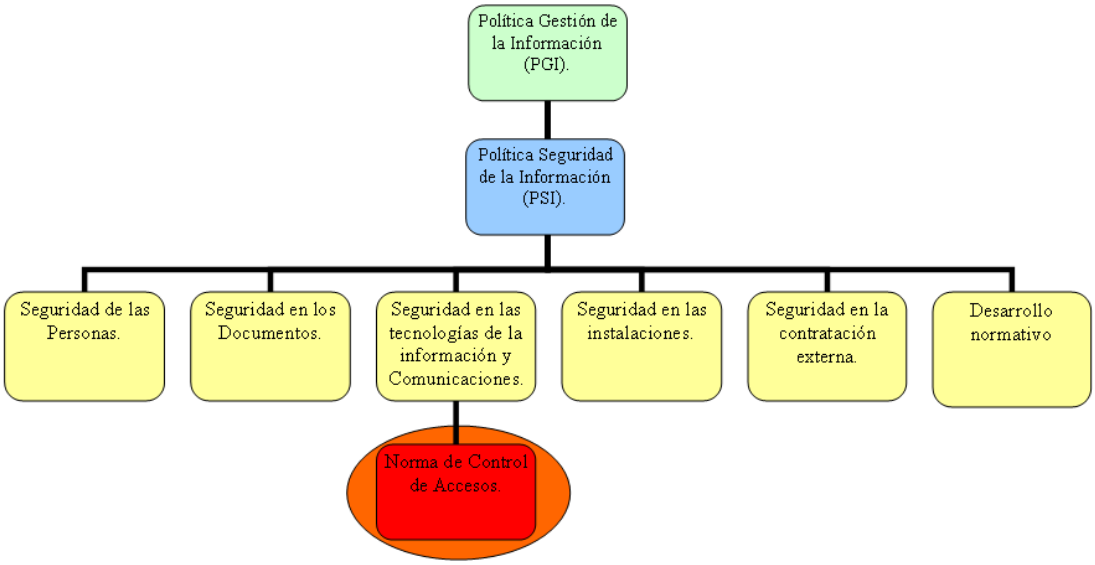
DATA SECURITY STANDARDS

ACCESS CONTROL

ID Code:	**NRM-04-EN**
Version:	1.0
Classification:	FCC_INTERNAL_USE
Approved by:	
Date:	

Intended for:	All FCC Staff and Users

INDEX



Within the context of Data Security, Access Control is the set of security mechanisms implemented to ensure that each individual or entity can only access the data they are authorised to. The goal of Access Control is to ensure the protection of the two main attributes of data security: Confidentiality and Integrity.

Access to FCC's Data Systems and other content or electronic services is regulated by FCC's Data Security Policy, which establishes that users to be pre-registered to access these services, i.e., they must be authorised to access any of the systems.

PURPOSE

The purpose of this Standard is to control access to the data processed by FCC data systems, by means of mechanisms implemented to ensure that the data can only be accessed by duly authorised users.

SCOPE

This Standard applies to all users who access data stored on FCC data systems, as well as the resources associated to that data as a result of its management and/or use, irrespective of:

- The mode of access (logical or physical).
- The location the user accesses the data from (local or remote).

PRINCIPLES

- The rationale behind Access Control is to guarantee a scenario where users can only access the data or resources they are authorised to in order to be able to carry out their functions.
- Access Control mechanisms must manage access to FCC data and resources, regardless of the data/resource format or the location of the user.
- Access Control must fulfil the minimum security requirements established by the classification of the data it controls, in accordance with the provisions of the Data Management Policy.

.

- Whenever a data system indiscriminately processes data classified according to the various levels defined in the Data Classification Model established for FCC, the minimum security requirements to be implemented must correspond to the data classified at the highest level.
- Physical access to FCC's premises and facilities where the data systems are located must be managed in accordance with the provisions of the Security Policy for Facilities.
- Whenever FCC data is processed by external companies, both the physical access to the premises and facilities where the data systems are located and the physical or logical access to these systems must be managed in accordance with the provisions of the Data Security Policy for External Companies.
- Data access controls must comply with all applicable regulations in force.

ACCESS CONTROL

- To develop this Standard correctly, all FCC data systems, premises and facilities that process Group data must have Access Control mechanisms in place.

- Access will be based on Access Profiles, which facilitate unique and personalised user identification. Profiles are grouped with specific access rights that represent the permissions that one or more work roles must have over data resources or systems.

- Access Control Lists (ACLs) must be established for system resources and functions. These ACLs must contain the various Access Profiles defined.

- Access rights are based on read, write and execute permissions.

- The Units Responsible for their own Data must specify which staff members are assigned which profiles, in order to process the data they are responsible for.

- FCC has categorised three access account types:

    - User Account: a system access account assigned to individuals for specific business reasons.
    - Service Account: a user account used by an application or system to access another system automatically.
    - Generic Account: an account shared by a group of individuals, which uses a shared password to access the system.

- The people responsible for these accounts will be:

    - For User Accounts: anyone who is assigned the User Account.
    - For Service Accounts: the person in charge of the system accessed.
    - For Generic Accounts: the person responsible for the data.

- The following accounts are prohibited:
    - Service Accounts with system administrator privileges.
    - Generic Accounts.

- Whenever business procedures require two account types for effective development, those responsible for these accounts must assess the associated risks.

- The activities carried out using privileged service or generic accounts must be monitored, and access must be logged in the system audit.

- The access rights assigned to users must be generally reviewed at least once a year. A different term can be established if there is a clear business need for it; in this case, the term must be specified in the procedures developed by this Standard.

- Each unit must conduct a periodic review of the rights assigned to the data they are responsible for, based on the following criteria:

  - Do the rights assigned need to be maintained?
  - Are the rights assigned appropriate?

- For access rights associated to generic user accounts, the review must be conducted at least quarterly.

- The administrators in charge of creating, cancelling or modifying system/resource access profiles must keep copies of the requests for these changes, as well as the reviews conducted, for at least one year after they have been initially requested.

- The mechanism used to assign access permissions must be capable of tracking any changes to the privileges assigned and their corresponding authorisations. A privilege is considered the right to bypass security controls to access functions.

- The procedures used to develop the applicable requirements and circumstances must consider every single stage of the user's access lifecycle, i.e., from the initial request to the cancellation or revocation of an account.

- Any changes to a user's responsibilities or functions will involve modification of the rights granted or removal of the access permissions granted.

- Applications and systems must be capable of maintaining an up-to-date list or log of users and their access profiles.

- Data systems that use passwords for authentication must be compliant with the provisions of the Password Security Standard.

- The documentation for using and administering data systems must include sections on Access Control measures and profile access types (administrator, user, process, etc).

- Data systems that process Restricted Data must be monitored at all times to detect any unauthorised access attempts or the use of unauthorised access rights.

- As a minimum, this monitoring must log all failed login attempts, the username, date and time the event takes place, and the resource used to access the system.

RESPONSIBILITIES

The Data Security and Risk Management Department must:

- Establish access control needs of the data systems.
- Approve and supervise the Access Control management plan established for the data systems.
- Check the access audit logs to verify that they are up-to-date and match real user privileges.
- Ensure that the provisions established in this Standard are implemented correctly and compliantly.

The Information Systems and Technology Department must:

- Manage:
  - The measures established for access profiles and the access accounts assigned to each profile.
  - The procedures for implementing and managing access control mechanisms.
- Monitor the performance of the FCC Data Systems they are responsible for.
- Notify the Data Security and Risk Management Department of any reported security incidents.

The Units Responsible for their own Data must:

- Establish the access profile rights they require.
- Formally approve access to the Data Systems they are responsible for.
- Ensure the fulfilment of this Standard, and inform the Data Security and Risk Management Department of any discrepancies that may arise.
- Notify the relevant section of the Data Security and Risk Management Department of any long-term absences of users under their control, regardless of whether these absences have been scheduled in advance or not.

Users must:

- Safeguard their FCC data system access passwords.
- Understand the consequences that could arise from violating this Standard.
- Immediately notify the Data Security and Risk Management Department of any suspect violations of this policy.
- Immediately report any lost, stolen or broken Access Control devices to the Data Security and Risk Management Department.

VIOLATIONS OF THIS STANDARD

Any violations of this Standard will be disciplined in accordance with the current FCC disciplinary system, without prejudice to the provisions of the legal regulations in force.

REVIEW OF THIS STANDARD

This Standard may be reviewed in the following circumstances:

- Whenever there are significant changes in the FCC Group.
- Whenever improvements are suggested as a result of audits carried out.
- Whenever there are major technology changes.
- Whenever there are changes to the current legislation regarding the provisions established in this Standard.

The information used for the review of this Standard must be notified to the Data Security Department, who must then notify the Data Security Department Committee of this information.

REFERENCES

- **Related Regulations**

  - FCC Data Security Policy
  - FCC Data Management Policy
  - FCC Security Policy for Physical Facilities
  - FCC Information Encryption Standard
  - Data Security Policy for External Companies
  - FCC Network Security Standard
  - FCC Password Security Standard

- **References to the ISO/IEC 27002:2007 Standard**

  - 9.1 Secure Areas
    - 9.1.2 Physical Entry Controls
    - 9.1.3 Office and Resource Security
    - 9.1.6 Public Access, Loading and Unloading Areas
  - 9.2 Equipment Security
    - 9.2.1 Installation and Protection of Equipment
    - 9.2.5 Security of Equipment Outside the Organisation's Facilities
  - 10.10 Monitoring
    - 10.10.2 Monitoring System Use
  - 11.1 Business Requirements for Access Control
    - 11.1.1 Access Control Policy
  - 11.2 User Access Management
    - 11.2.1 User Registration
    - 11.2.2 Privilege Management
    - 11.2.3 User Password Management

- 11.2.4 User Access Rights Reviews

- 11.3 User Responsibilities
  - 11.3.1 Use of Passwords
  - 11.3.2 Unattended User Equipment
  - 11.3.3 Unattended Workstations and Screen-locking Policy

- 11.4 Network Access Control
  - 11.4.2 User Authentication for External Connections

- 11.5 Operating System Access Control
  - 11.5.1 Secure Connection Procedures
  - 11.5.2 User Identification and Authentication
  - 11.5.6 Connection Time Limits

- 11.6 Data and Application Access Control
  - 11.6.1 Data Access Restrictions
  - 11.6.2 Sensitive System Isolation

DOCUMENT CHANGE CONTROL

Document Information

FILE NAME:				
VERSION	DATE	CHANGE	AUTHOR	REVIEWED BY
1.0	2009 April	Document creation	Information Security and IT Risks Department	FCC Executive Committee
1.0	September 2019	Revision of the document	Information Security and IT Risks Department	FCC Executive Committee

Please Note: Hard-copies are not controlled

Distribution List

FROM:		DATE	EMAIL
TO:	ACTION	DATE EXPECTED	EMAIL

Action Types: Approve, Review, Report, Archive, Make Decision, Other (please specify)

Version History

VERSION #	DATE	CARRIED OUT BY	DESCRIPTION

END OF DOCUMENT