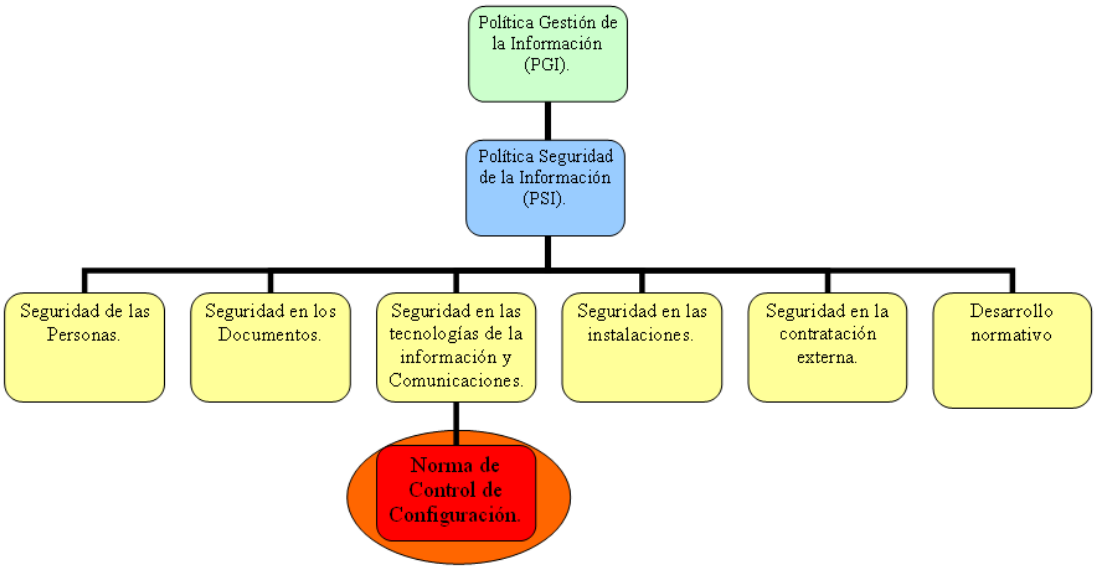
DATA SECURITY STANDARDS

DATA SYSTEM CONFIGURATION AND CHANGE CONTROL

ID Code:	NRM-05-EN
Version:	1.0
Classification:	FCC_INTERNAL_USE
Approved by:	
Date:	

Intended for:	Information Systems and Technology Department

INDEX



Bearing in mind the complexity of data systems, change control measures must be implemented for applications and programmes during the development, operation and maintenance of the components that make up an organisation's systems.

As a process, Change Control ensures that the methods and procedures used for quickly and efficiently assessing and approving changes carried out to system components are standardised. This serves to protect data systems from unauthorised changes, which denotes greater system availability.

Configuration and Change Control comes into play at the initial stages of any data system project, and remains in place for the entire life cycle.

Whenever an organisation is at the Requirements Stage of a data system deployment or upgrade project, having the right procedures and documentation to configure the system's hardware, software and firmware correctly is considered an essential part of establishing the desired functional security requirements.

PURPOSE

The purpose of this Standard is to establish the Configuration and Change Control management requirements for the components that make up FCC's data systems.

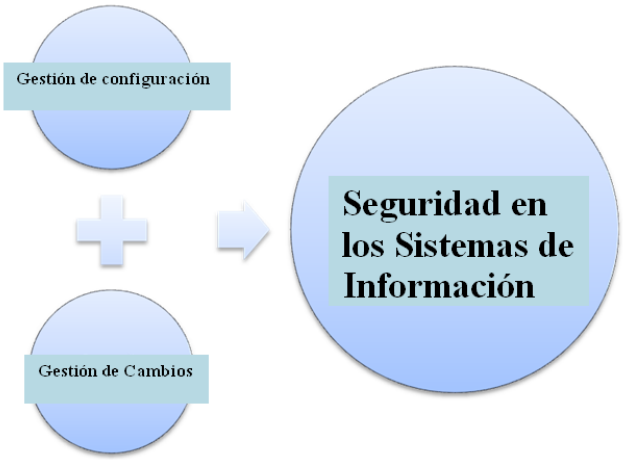
SCOPE

This Standard applies to the processes of identifying, monitoring, inventorying and checking the status of all FCC data system components during development and operation.

This Standard applies to all staff of the FCC Group (hereinafter referred to as FCC) who are responsible for the management, control and use of such processes.

Configuration and Change Control management must be established, documented, maintained and applied to all FCC data systems.

PRINCIPLES



- All equipment used by FCC, regardless of its ownership, must have the required staff and material resources available to properly maintain it.
- The acquisition and installation of software or hardware components without the prior approval of the Information Systems and Technology Department is prohibited.
- All components installed on FCC data systems must be carried out in accordance with the manufacturer's recommended security specifications.

- When developing the Configuration and Change Control management plan for FCC data systems, the segregation of tasks and functions for all planned activities must be properly considered. To this end, the roles for configuring and administering components must be clearly segregated.

- Configurations and changes must be duly checked and verified by qualified FCC staff.

- When developing the Configuration and Change Control management plan, the availability of all FCC data system components must be considered.

CONFIGURATION MANAGEMENT

- To safeguard the integrity of data system software, technical access control measures, a policy based on minimum use privileges and strict change control procedures must be applied.

- Configuration management procedures must include documentation of the security requirements and justification for any exceptions that may arise.

- Data system security parameters must be configured as restrictively as possible, in accordance with the functional requirements established for each system.

- The security modifications (patches) to resolve errors (bugs) must be only applied after their need has been approved; these modifications must be made by reliable sources, and must be tested before deployment on the production systems.

CHANGE CONTROL MANAGEMENT

- The versions of the individual components that make up an FCC data system must be documented; these components and their versions define the system.

- The use real FCC data in test environments is not permitted. The Data Security and Risk Management Department may approve the use of real FCC data, on condition that the security controls implemented ensure the level of protection required for the classification of the data processed.

- If the required level of security cannot be guaranteed, testing must be approved by the unit responsible for that data, and the reasons why the security level cannot be guaranteed must be expressly stated in the approval log.

- Whenever a test environment has been established and it becomes apparent that the required security level cannot be guaranteed, the FCC data must be properly sanitised to re-establish the previous security attributes.

- The test procedures for FCC data systems must include a period of parallel test deployment before being deployed to the production environment.

- The replacement or removal of software and data files must have the formal consent of the unit responsible for the data, and must be subsequently approved by the Information Systems and Technology Department.

- Any software and data files that have been replaced or removed must be carried out according to the media removal procedures.

- Any modifications to FCC data systems must follow the following sequence:

    - A formal request must first be submitted for each change. This request can be submitted by the unit responsible for the data, the Information Systems and Technology Department or the Data Security and Risk Management Department.
    - Before the changes are approved, any possible impacts on other systems must be assessed. This assessment can be carried out by analysing all dependant systems.
    - Changes must be authorised by the unit or owner of the FCC Data System that will be affected, as well as the FCC Information Systems and Technology Department.

- The changes and the scope of their application must be notified in advance to any staff affected, to ensure that they are aware of the works that must carried out.

- In emergency situations, changes must be carried out according to the operating procedures established for that purpose, and the change and configuration requests must be submitted immediately after the actions have been carried out.

- The documentation that must be produced for changes or installing system software and hardware must state the following:

    - The change or installation process management procedure followed.
    - The changes carried out.

      The documentation for these last points must state the following as a minimum:

        - The origin of the change.
        - The type and scope of the change.
        - The techniques used and the sequence of activities.
        - The testing carried out and the results.

- The following actions must be carried out before any changes or modifications to data systems are deployed in the production environment:

    - The business functionalities and their processing capabilities must be properly tested.

- The FCC data systems that will be affected by the change must be fully backed up.

- Data system components can only be replaced by authorised staff, who must ensure the sanitisation and removal of technical risks.

- *Preventive maintenance for all system components must be scheduled periodically, and includes:*

  - Monthly maintenance including log purging.
  - Six-monthly maintenance including configuration reviews.
  - Yearly maintenance including equipment cleanups.
  - Maintenance procedures must include the following as a minimum:

    - Scope
    - Results
    - Time
    - Staff assigned to task
    - Procedures for notifying users of maintenance works

The Configuration and Change Control Management procedures must:

- Establish:
  - The staff responsible for the configuration and maintenance works.
  - The following procedures:
    - The emergency procedures for carrying out configuration and maintenance works.
    - The sanitisation procedures for resources that must leave FCC facilities for configuration and maintenance works.
    - The procedures for ensuring that data system failures are reported and logged on time and correctly.
    - The procedures for verifying that the data system security features that were in place before a change takes place will remain in place and work correctly after the change has been applied.
    - The procedures for ensuring that data systems configuration changes are properly audited.
    - The procedures for ensuring that all FCC staff receive the training required to carry out their duties regarding the functionalities and operations of new components.

  - The controls for ensuring that configuration and maintenance works carried out by external companies are in compliance with FCC's Data Security Policy and above all the External Company Policy.

- Identify:
  - The professional and material resources needed for the maintenance of internal and external FCC facilities.

Configuration and Change Control Management documentation must contain the following as a minimum:

- A Version Control system that links system components to the correct version.
- An analysis of the impact that proposed changes will have on existing security controls.
- The procedures for:
    - Evaluating and/or approving data system components before they are deployed in production environments.
    - Ensuring the review of the functions, controls and services that may be potentially removed by the changes carried out.
    - Ensuring that the contingency plans and associated documentation are updated with the changes carried out.
    - Managing and resolving potential emergencies or returning to the last known good configuration when configuration or version change processes have to be cancelled.
- The requirements for all hardware, software and firmware installations and modifications to ensure that they are carried out in accordance with current regulations on intellectual and industrial property.
- The estimated useful life of components, so their renewal can be scheduled in advance.

Error logs for management operations must contain the following as a minimum:

- The name and version of the systems involved.
- The date and time of the error.
- A description of the error and the system components involved.
- The name of the person responsible for resolving the error.
- The resolution actions carried out.
- The date and time the error is resolved.

RESPONSIBILITIES

The Data Security and Risk Management Department must:

- Establish the requirements for controlling data system configurations correctly.

- Checking the error logs, unauthorised use logs and activity logs for FCC's data systems.
- Verifying that the hardware, software and firmware change control documentation is secure.

The Information Systems and Technology Department must:

- Approve components, and how they are installed, maintained and withdrawn.
- Conduct an impact analysis for data system component changes.
- Produce the procedures regarding installations and change control, and emergency and last known good configuration.
- Manage:
    - The technical requirements, controls and testing plans.
    - Change requests
    - The coordination of approved change implementation.
- Monitor FCC data systems to ensure compliance with this Standard.
- Ensure that both technical staff and system users receive adequate training.
- Investigate security incidents or potential incidents in FCC data systems, analysing the impact and causes, in cooperation with the Data Security and Risk Management Department.

The Units Responsible for their own Data must approve:

- Any changes to data system configurations.
- Testing, in the event that the required security level cannot be guaranteed.

REVIEW OF THIS STANDARD

This Standard may be reviewed in the following circumstances:

- Whenever improvements are suggested as a result of audits carried out.
- Whenever there are major technology changes.
- Whenever there are improvements to the data systems management processes.
- 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.

VIOLATIONS

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.

REFERENCES

- **Related Regulations**

  - FCC Data Security Policy
  - External Company Standard.
  - Systems Laboratories' Standard.
  - Backup Management Standard.
  - Disaster Recovery Standard.
  - Incident Management Standard.

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

- 6.1 INTERNAL ORGANISATION
  - 6.1.3 Assignation of responsibilities to ensure data security
  - 6.1.4 Process of resource authorisation for data processing
- 6.2 THIRD PARTY ACCESS SECURITY
  - 6.2.1 Identification of third party access risks
  - 6.2.3 Security considerations for third party contracts
- 7.1 RESPONSIBILITY OVER ASSETS
  - 7.1.1 Asset inventory
  - 7.1.2 Asset ownership
  - 7.1.3 Proper use of assets
- 8.2 SECURITY WHILE EXECUTING DUTIES
  - 8.2.2 Data security awareness and training
- 9.2 EQUIPMENT SECURITY
  - 9.2.1 Installation and Protection of Equipment
  - 9.2.2 Supplies
  - 9.2.4 Equipment Maintenance
  - 9.2.5 Security of Equipment Outside the Organisation's Facilities
  - 9.2.6 Security Regarding the Reuse or Removal of Equipment
  - 9.2.7 Transferring FCC Assets to External Organisations
- 10.1 OPERATING PROCEDURES AND RESPONSIBILITIES
  - 10.1.1 Operating Procedures Documentation
  - 10.1.2 Change Control Management
  - 10.1.3 Segregation of Tasks
  - 10.1.4 Distribution of Resources in the Development, Test and Production Environments
- 10.3 SYSTEM PLANNING AND ACCEPTANCE
  - Capacity Planning
  - System Acceptance
- 10.7 DATA MEDIA USE
  - 10.7.2 Withdrawal of Media
  - 10.7.4 System Documentation Security
- 10.10 MONITORING
  - 10.10.1 Audit Logs
  - 10.10.2 Monitoring System Use
  - 10.10.4 Administrators' and Operators' Log

- 10.10.5 Error Log
- 12.1 DATA SYSTEM SECURITY REQUIREMENTS
  - 12.1.1 Analysis and Specification of Security Requirements
- 12.4 SYSTEM FILE SECURITY
  - 12.4.1 Software Control in the Production Environment
  - 12.4.2 Protecting System Test Data
- 12.5 DEVELOPMENT AND SUPPORT PROCESS SECURITY
  - 12.5.1 Change Control Procedures
  - 12.5.2 Technical Review of Applications due to Operating System Changes
  - 12.5.5 External Software Development
- 15.1 CONFORMITY WITH LEGAL REQUIREMENTS
  - 15.1.2 Intellectual Property Rights
- 15.3 CONSIDERATIONS FOR DATA SYSTEM AUDITS
  - 15.3.1 System Audit Controls

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