DATA SECURITY STANDARDS

DEVELOPMENT SECURITY

ID Code:	**NRM-13-EN**
Version:	**1.0**
Classification:	FCC_INTERNAL_USE
Approved by:	
Date:	
Intended for:	**Information Systems and Technology Department**

INDEX

INDEX .....¡Error! Marcador no definido.

PURPOSE.....¡Error! Marcador no definido.

SCOPE.....¡Error! Marcador no definido.

PRINCIPLES OF SECURE DEVELOPMENT.....¡Error! Marcador no definido.

DATA SECURITY IN DEVELOPMENT TASKS .....¡Error! Marcador no definido.

DEVELOPMENT OF DATA SECURITY FUNCTIONALITIES ... ¡Error! Marcador no definido.

DEVELOPMENT OF APPLICATIONS CONTAINING PERSONAL DATA ¡Error! Marcador no definido.

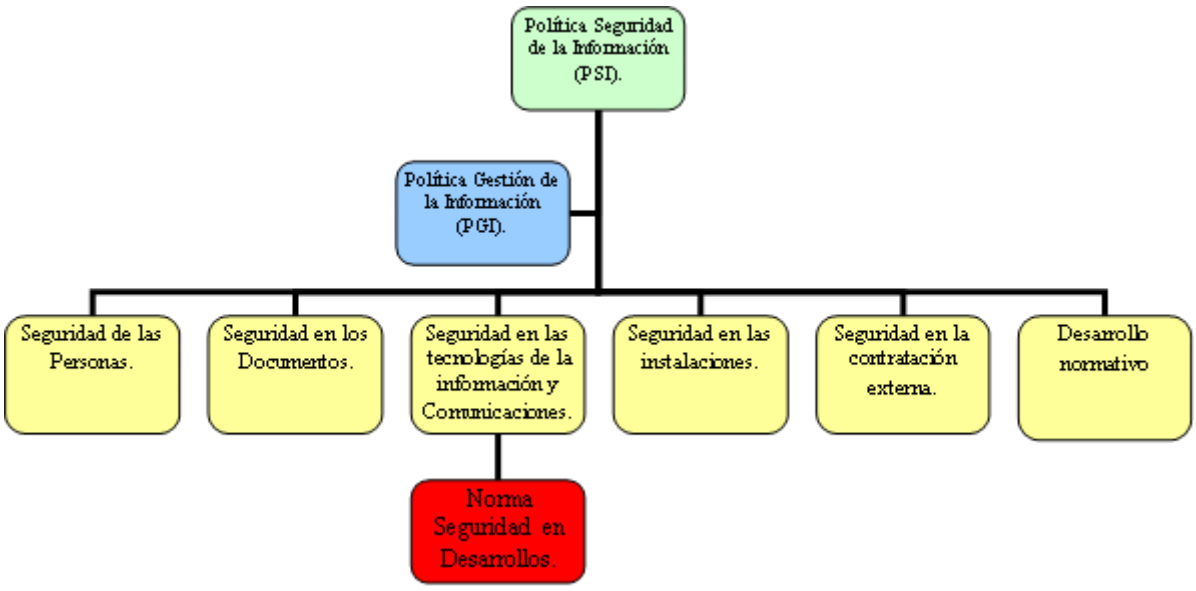
RESPONSIBILITIES .....¡Error! Marcador no definido.

REVIEW OF THIS STANDARD .....¡Error! Marcador no definido.

VIOLATIONS .....¡Error! Marcador no definido.

REFERENCES.....¡Error! Marcador no definido.

DOCUMENT CONTROL CHANGE .....¡Error! Marcador no definido.



Application development and data system integration projects are growing increasingly complex due to the human and technical resources involved, as well as the bearing they

have on the correct functioning of an organisation's business units and their stakeholders.

Whenever business or customised applications are migrated, upgraded or integrated - and the data involved in these processes, also demonstrates the complexity of these projects. This complexity must be carefully thought-out, since the interconnection of secure applications does not necessarily result in a new system with a similar level of security.

The diversity of applications used by FCC, and the nature of the data processed by them, requires the implementation of controls over the entire life cycle of data system development projects. The objective is to implement the security functionalities required for software, and establish a working environment that preserves the integrity of the end product.

The principles included in this Standard apply to both the development of FCC data systems in controlled environments, and the integration of more desirable data security attributes in development projects.

PURPOSE

The purpose of this Standard is to ensure that confidentiality, integrity and availability are considered for the entire life cycle of FCC data processing application and software development and maintenance projects.

SCOPE

This Standard applies to all data processing application and software development and maintenance projects of the FCC Group (hereinafter FCC), regardless of where they take place or the staff involved.

The term "*data system development project(s)*" included throughout this Standard refers to both the development of new FCC data systems and the maintenance of existing FCC data systems.

PRINCIPLES OF SECURE DEVELOPMENT

- The security measures that apply to FCC data processed in data system development projects must based on the classification requirements for that data

- A software development methodology must be used for all projects, regardless of whether they are carried out by FCC staff or External Companies, so that applications and software have the required security

- Those responsible for developing a data system must correctly manage the controls established by both the FCC Security Policy and the business needs defined

- Data system development projects must only be carried out in development, preproduction or test environments

  Whenever production data is used for testing and development, the security measures implemented in those environments must fulfil the requirements established by the Password Standard, Access Control Standard and Encryption Standard, as well as the current legal regulations

- Production environments must be properly isolated from testing and development environments using logical media, to ensure the confidentiality of FCC data's in operating environments

- Applications must be upgraded in accordance with:

  - The technological conditions stated by the manufacturer
  - The changes to data security functionalities
  - The applicable legal requirements

- Readily available data systems that must be acquired from official, secure websites

- All changes carried out to data systems must:

  - Be duly authorised by the unit responsible for the data
  - Have the internal functionality and application interfaces, as well as the locations of their source code and activity logs duly documented

- The units responsible for their own data must only provide FCC staff with the data that is strictly required to carry out their work within the development project

- Temporary and test files generated in these projects must comply with the security measures established for the classification level required by the FCC data contained in them

DATA SECURITY IN DEVELOPMENT TASKS

Generally speaking, data system development projects carried out by FCC must:

- Use verified analysis, design, implementation, documentation and development testing methodologies, which allow the development of secure data systems, in accordance with FCC's Data Security Policies

- Ensure proper FCC data security for the project's entire life cycle

- Provide sufficient training to technical and functional staff on how to use the new applications

- Fulfil the security regulations regarding data system migrations from a development environment to an integrated or operating environment

- Ensure that all data system development designs are controlled, in order to guarantee that the security of the system or operating environment is not compromised

- Adopt proper change management and software version controls, in accordance with the Configuration Control Policy

- Migrating data system developments into a production environment must be carried out ensuring that the availability of the data is not affected by the process

- All modifications to FCC business applications must consider the technical and post-sale maintenance implications; to this end, they must be duly documented to facilitate the installation of subsequent application versions

DEVELOPMENT OF DATA SECURITY FUNCTIONALITIES

Data system development projects carried out by FCC must consider the need to:

- Assign the security requirements at the functional analysis stage of developing the application
- Develop applications with security requirements such as mechanisms for identification, authentication, access controls and audit or activity logs, in order to safeguard the security of the data processed by them
- Include mechanisms that maintain control over FCC data processing procedures, reporting any errors produced, in order to preserve the integrity and availability of that data
- Ensure the integrity of both stored and transmitted data
- Produce the functional and security documentation for the development analysis and design stages

DEVELOPMENT OF APPLICATIONS CONTAINING PERSONAL DATA

Testing of implemented or modified data systems that process personal data files must not be carried out using real data, unless the security levels required for that data can be ensured

RESPONSIBILITIES

The Data Security and Risk Management Department must:

- Establish the security functionalities to be implemented in applications and software

- Ensure that the functionalities of both the applications and the development environments fulfil the requirements established by FCC's Security Standards

The Information Systems and Technology Department must:

- Implement the technical and organisational measures required to protect the security of data processed in development projects .
- Integrate the security requirements into application and software functionalities
- Validate the technical testing carried out on applications and software, verifying that the required security functionalities have been met
- Comprehensively manage the inventory, upgrading the applications, environments and software versions periodically

The Units Responsible for their own Data must:

- Propose measures to improve the security functionalities of FCC's data system developments
- Validate the testing carried out on applications and software to verify whether the security functions defined in the security requirements analysis have been implemented correctly

REVIEW OF THIS STANDARD

This Standard may be reviewed in the following circumstances:

- Whenever new secure development methodologies are introduced, or the existing methodologies change (applies to development projects)
- Whenever improvements are suggested as a result of audits carried out
- Whenever there are technology or programming language 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.

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 Encryption Standard
  - FCC Password Security Standard
  - Configuration Control Standard

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

- 10.1 OPERATING PROCEDURES AND RESPONSIBILITIES
  - 10.1.3 Segregation of Tasks

- 12.2 CORRECT APPLICATION PROCESSING
  - 12.2.1 Incoming Data Validation
  - 12.2.2 Internal Processing Control
  - 12.2.3 Message Integrity
  - 12.2.4 Outgoing Data Validation

- 12.4 SYSTEM FILE SECURITY
  - 12.4.1 Software Control in the Production Environment
  - 12.4.2 Protecting System Test Data
  - 12.4.3 Software Source Code Access Control

- 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
  - 12.5.3 Software Package Change Restrictions
  - 12.5.4 Data Leaks
  - 12.5.5 External Software Development

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	October 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