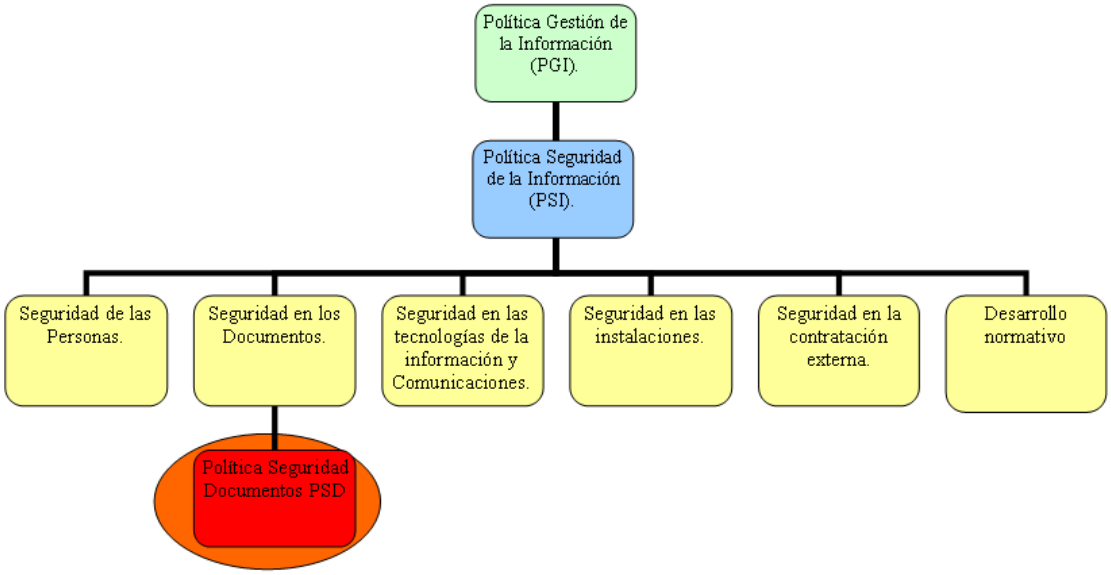
INFORMATION SECURITY POLICY

Citizen Services

DOCUMENT SECURITY

ID Code:	NRM-15-EN
Version:	1.0
Classification:	FCC_INTERNAL_USE
Approved by:	
Date:	
Intended for:	

INDEX



The data processed by FCC is recorded in documents with different characteristics and formats that require specific protection throughout their entire life cycle. From initial creation, through to storage and final destruction.

If these documents are to be used as the basis for making business decisions and recording business activities with the interest groups related to FCC, they must ensure the confidentiality, integrity and availability of the data contained in them, regardless of their timeline and the physical or logical media used to store them.

PURPOSE

The purpose of this Policy is to establish protective measures for all documents containing FCC Group (hereinafter FCC) Data, in order to ensure the confidentiality, integrity and availability of that data throughout its entire life cycle.

SCOPE

This Policy applies to all documents containing FCC data, regardless of their location, the media used to store them or their format.

The term “document” herein refers to documents containing Data owned by FCC.

PRINCIPLES

- Documents must be comprehensively protected throughout all stages of their life cycle, and regardless of their format and the media used.
- The protective, organisational and technical measures that must be implemented for documents must be proportionate to the risk and classification levels of the data contained in them.
- Documents must only be accessed by people who require access to the data contained in them. A Personal Security Authorisation is required to access Restricted data.
- Documents can be processed by external staff, who must fulfil the Data Security Policy for External Companies.
- For documents containing different data security classifications, the security measures corresponding to the most restrictive classification must be applied, whenever the specific measures for each level cannot be applied.

MANAGING DOCUMENTATION

Storage

- Only documents containing data required to fulfil FCC’s business purposes may be stored.

- Documents that contravene current legislation, public order, moral or good practices must not be stored.

- Documents must be stored on media or devices that ensure they can be processed within FCC's technological environment at all times, so that no outdated media technology can affect the availability of the data stored.

- Whenever data storage management is outsourced, the agreements executed must state the security measures and responsibilities applicable to the outsourcer, as well as the requirements indicated in FCC's Data Security Policy for External Companies.

- Units responsible for their own document(s) that contain Restricted Data must keep an updated list of people authorised to access that data.

Distribution

- Documents containing Non-Restricted Data can be distributed to anyone who requires access to them, without the prior authorisation of the unit responsible for them.

- In accordance with FCC's Data Security Policy for External Companies, whenever document management has been outsourced, the agreement governing such services must include a confidentiality and nondisclosure agreement applicable to all staff of the external company involved in the provision of the service.

- The agreements governing the distribution of documents to third parties must include the obligation for the receiver to implement the security measures established by FCC, which are based on the classification of the data contained in such documents.

- The distribution of documents must be carried out via media that can ensure:

    - Unequivocal reception by the addressee or the staff authorised by him/her
    - The confidentiality and integrity of the data

- Documents must not be left unattended on printer trays

- Restricted Data contained in duly labelled documents must be distributed via media that do not contain explicit reference to the classification of the data contained in them.

Labelling

- Regardless of their format or the media they are stored on, documents containing FCC Data must clearly and visibly state the classification of the data contained in them using one of the following labels:

- FCC_SECRET
- FCC_CONFIDENTIAL
- FCC_INTERNAL_USE
- FCC_PUBLIC_USE

- Documents labelled “FCC_SECRET” must include a heading clearly stating the classification level and the authorised distribution list, in order to prevent individuals from accessing the content without opening them.

- With the exception of documents filed before this Policy enters into force, documents not labelled with the classification level of the Data contained in them will be considered for *Internal Use* only. These documents must be classified when they are next opened.

Destruction

- Documents must be destroyed using means that renders the data unrecognisable and unrecoverable, and the confidentiality of the data contained in them must be maintained throughout all actions of the destruction.

- In the event that the Company chooses to outsource the destruction of documentation, the agreements executed must include a confidentiality and nondisclosure agreement applicable to all staff of the external company directly or indirectly involved in the provision of the service, regardless of the additional requirements established in the current legislation regarding the nature of the data contained in them.

- Whenever data destruction has been outsourced, the agreement executed between the companies must state the requirement for the service provider to present a document destruction certificate stating that the data contained within has been completely destroyed.

- Specific procedures must be established for the security requirements regarding the destruction of the different classification levels of data.

- The transportation of documents to the location where they are to be destroyed must guarantee that no theft, loss or leakage of data takes place during transportation.

- The distribution of electronic documents containing personal data can only take place once the data has been encrypted or a mechanism that guarantees that the data cannot be read or handled during transportation has been implemented.

- Documents must never be disposed of or destroyed when they maintain a probative value regarding the rights and obligations of individuals or legal entities, or when the retention timeframes established by current legislation have not yet expired.

RESPONSIBILITIES

The Data Security and Risk Management Department must:

- Establish the security criteria for labelling documents
- Approve and establish the document distribution and destruction methods
- Verify document security procedures

The Information Systems and Technology Department must:

- Ensure that the data contained in electronic documents is available for use on data processing media at all times

The Units Responsible for their own Data must:

- Verify the access identification and authentication procedures
- Be aware of the document security controls implemented

The Users must:

- Report any incident detected regarding data documents, in as much detail as possible

REVIEW OF THIS POLICY

This Policy may be reviewed in the following circumstances:

- Whenever there are significant changes to FCC's working processes
- Whenever there are improvements suggested as a result of audits carried out
- Whenever there are changes to the current legislation regarding the provisions established in this Policy
- Whenever there are major technology changes

The information used for the review of this Policy 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 Policy 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**

  - Data Security Policy
  - Data Management Policy
  - Data Security Policy for External Companies
  - Backup Management Standard

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

7.2. Classification of Data
- 7.2.2 Data Labelling and Handling

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 Asset Responsibility .
- 7.1.2 Asset Ownership
- 7.1.3 Proper Use of Assets

9.2 Equipment Security
- 9.2.1 Location and Protection of Equipment

10.5 Backups
- 10.5.1 Data Backups

10.7 Backup Media Handling
- 10.7.1 Removable Media Management
- 10.7.3 Data Handling Procedures
- 10.7.4 System Data Security

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