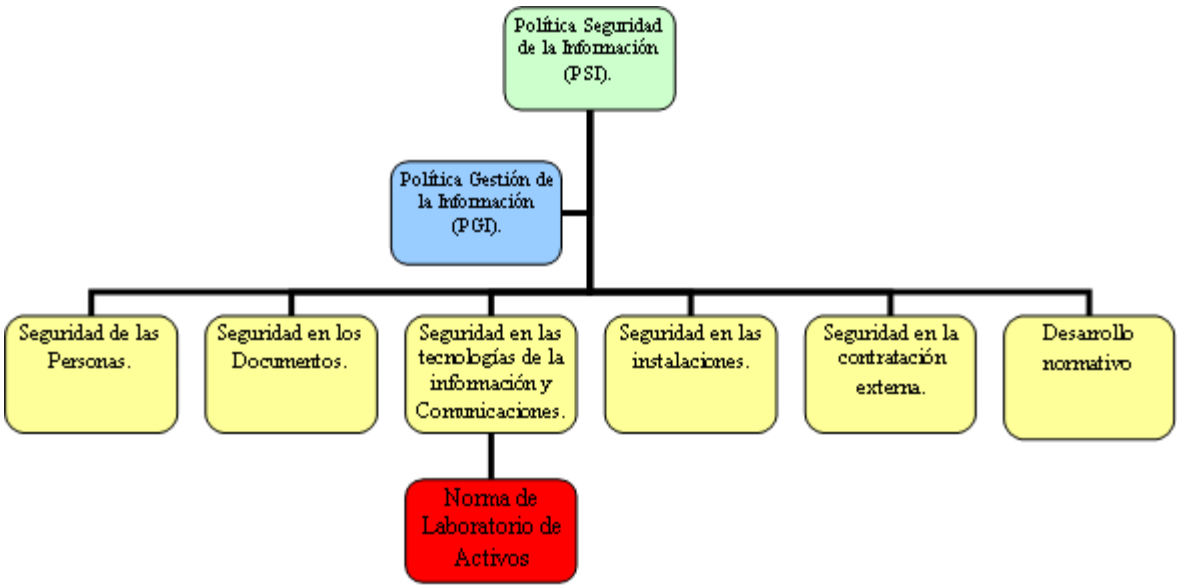
DATA SECURITY STANDARDS

SYSTEMS LABORATORIES

ID Code:	NRM-09-EN
Version:	1.0
Classification:	FCC_INTERNAL_USE
Approved by:	
Date:	

Intended for:	Information Systems and Technology Department

INDEX



Systems laboratories are places where configuration, testing, maintenance, repairs and the destruction of the IT equipment takes place. Their purpose is to ensure the fulfilment of internal physical and logical technological control procedures, as well as work procedures.

IT assets processed in the laboratories may be compromised in the course of the different activities carried out.

PURPOSE

The purpose of this Standard is to ensure the integrity and confidentiality of FCC data during configuration, testing, maintenance, repairs and destruction of data systems or assets.

SCOPE

This Standard applies to any data systems or assets that are configured, tested, maintained, repaired or destroyed, regardless of the data processed or the laboratory where these works are carried out.

PRINCIPLES

Data security at FCC's systems laboratories is based on the following principles:

- Systems laboratories will service FCC IT assets only, with the exception of when the Information Systems and Technology Department expressly authorises the provision of these services to other parties' assets.
- All asset or system works carried out at a laboratory will require prior approval from the unit responsible for the data involved.
- Whenever one or more of the tasks stated in this Standard is carried out by a company outside the FCC Group, the security measures established in the External Companies' Policy must be fulfilled.
- The security measures implemented when IT assets are configured, tested, maintained, repaired or destroyed must be in accordance with the classification of the data involved.

SYSTEMS LABORATORIES

A controlled working environment must be implemented at the Systems laboratories, in accordance with the protection levels established for the IT resources used. Regardless of their location, systems laboratories must:

- Fulfil the principles of the Physical Security Policy, as well as the principles of both the Access Control and Configuration Control Standards, in order to

prevent any alterations, loss or unauthorised processing or access to the FCC data processed by the IT assets they use on a daily basis.

- Log all incoming and outgoing IT assets handled at the systems laboratory, as well as those that need to be disposed of.

- Fully log any incident that could affect data security while the data asset is at the laboratory, and notify the unit responsible for the data.

  The laboratory's incoming and outgoing IT asset logs must contain the following as a minimum:

  - The asset type
  - The date and time
  - The sender/receiver
  - The department/area/company that owns the data
  - The number of assets
  - The delivery method
  - The name of the duly authorised person responsible for the reception/delivery

- Whenever IT assets are configured, tested, maintained, repaired or destroyed by FCC staff outside their normal facilities, the security measures implemented must ensure data protection, in accordance with both the External Companies' Policy and the Portable Devices Standard.

- Laboratory staff must implement the measures required to prevent any unauthorised data recovery from IT assets that need to leave the installations as a result of maintenance or destruction works.

RESPONSIBILITIES

The Data Security and Risk Management Department must:

- Approve and monitor the logical and physical controls established for managing FCC's IT systems laboratory.

- Analyse any violations of this Standard that could constitute a security incident.

The Information Systems and Technology Department must:

- Implement the operating procedures to ensure that both the laboratories and the activities carried out in them comply with the corresponding security levels established.

- Log all incoming and outgoing IT assets handled by the systems laboratory, as well as any that need to be destroyed.

- Report any suspected, attempted or executed actions that violate this Standard, or any abnormal behaviour regarding access control of applications and systems to the Data Security and Risk Management Department.

The unit responsible for the data must:

- Authorise any configuration, testing, maintenance, repair or destruction of IT assets used for processing FCC data which they are responsible for.

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.

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**

  - Data Management Policy
  - Physical Security Policy
  - Data Security Policy for External Companies
  - Security Policy for Individuals
  - Document Security Policy
  - Incident Management Standard
  - Portable Devices Management Standard

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

- 12.1 DATA SYSTEM SECURITY REQUIREMENTS
  - 12.1.1 Analysis and Specification of Security Requirements

- 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 Restrictions on Software Package Changes
  - 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