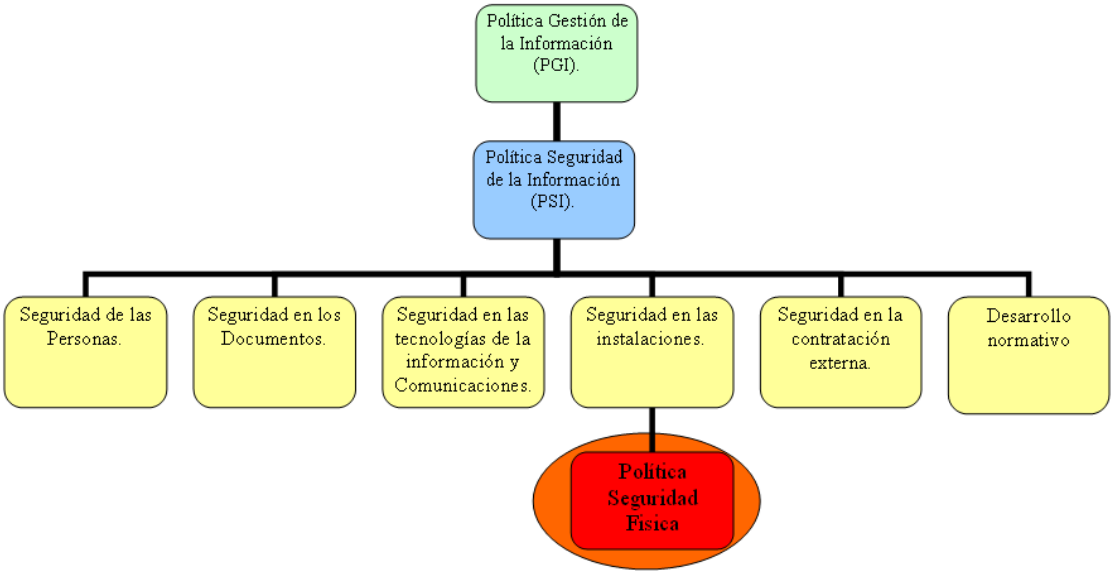
DATA SECURITY POLICY

PHYSICAL SECURITY OF INSTALLATIONS

ID Code:	**NRM-16-EN**
Version:	**1.0**
Classification:	**FCC_INTERNAL_USE**
Approved by:	
Date:	

Intended for:	**Information Systems and Technology Department**

INDEX



Physical security is essential for protecting FCC's IT facilities and Data from unauthorized access and damage arising from natural causes, voluntary actions, errors or accidents.

Physical security requirements vary considerably depending on the activity, type of facilities and Data systems requiring protection. Regardless of the circumstances, security can be achieved through a combination of environmental safeguards and control of physical access to systems and data.

FCC believes that both FCC's Management and staff are jointly responsible for effectively securing data assets in the workplace.

PURPOSE

The purpose of this Policy is to implement the technical and organisational measures required to detect, reduce, prevent and/or delay the risks arising from accidents, environmental hazards or malicious acts that could affect FCC's data assets and the facilities where data is processed.

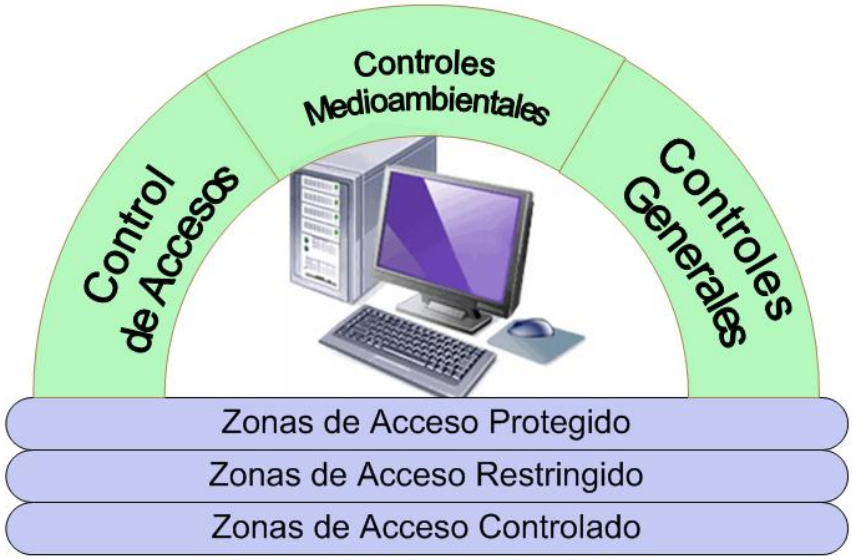
SCOPE

This Policy applies to all FCC facilities where data is processed, regardless of their location, the type of data processed and the equipment used.

PRINCIPLES

- Data assets must be located in secure areas, which prevent unauthorised individuals from accessing, manipulating, stealing or destroying data and data-processing equipment at all times.
- Security controls at data processing facilities must be coordinated with the physical security measures implemented in the buildings where they are located.
- The physical security controls at the facilities must be based on the economic value of an impact caused by a data processing incident.
- Access to the facilities and areas where FCC Data is processed must be restricted to authorized staff who require access to the data, or staff who hold a personal authorisation to do so, where appropriate.
- Visits to the facilities must fulfil the security requirements established in this Policy for that purpose. No other type of access is permitted.
- Data processing facilities must have minimal signage to prevent identification of their activities.
- Staff authorised to take portable devices out of FCC's facilities will be responsible for the protection and control of that equipment, in accordance with the Portable Devices Standard.
- In accordance with the Asset Inventory Standard, the identification and location of physical assets must be controlled; an annual physical inventory of desktop equipment must be carried out, and the assets' serial numbers and locations must be controlled.
- Physical security systems must comply with the rules and regulations for buildings and access control.

- No paper or media containing FCC data must be left on office desks outside office hours.



SECURE ACCESS AREAS

For the purposes of implementing physical security measures, FCC facilities are divided into three areas:

Controlled Access Areas

These areas are open to FCC staff, where there are no specific environmental controls in this Policy to protect data systems.

Example:
FCC offices where computers and peripherals are used.

Restricted Access Areas

Access to these areas is restricted to the FCC staff who work in them, or staff whose access has been expressly authorised; these areas have specific environmental controls for data-processing systems in place.

Examples:
Departmental server rooms; electronic network cabinets located outside computer rooms; Data Processing Centres; departmental archives.

Protected Access Areas

Access to these areas is restricted and controlled via identification mechanisms, as the data-processing systems process data that is sensitive to FCC's business activities or Restricted Data.

Examples:
Data Processing Centres; general archives; Senior Management offices.

PROTECTED ACCESS AREAS

The location of these areas must minimise environmental hazards and unauthorized access.

ENVIRONMENTAL CONTROLS

- The windows and doors of these areas must be locked and controlled at all times. The windows must be externally protected with security grilles or similar physical barrier.

- Protected access areas must not be located in the following areas, unless expressly agreed by the Data Security Committee upon receipt of a risk assessment report:

  - Cellars or basements
  - Top floors of buildings
  - Near downpipes or areas where water is used

- Data Processing Centres (DPCs) must have the following technical measures implemented:

  - Suitable floors and ceilings for the equipment and risks associated to the works carried out in the room, with insulating and antistatic specifications
  - Watertight walls, floors and ceilings, that allow water to drain in the event of flooding
  - Water and fireproof walls, doors and windows
  - Redundant air conditioning systems that are independent of the building's general systems
  - Water leak detection and evacuation systems
  - Temperature, humidity and suspended particle concentration meters
  - Uninterruptable Power Supply (UPS) systems or dual-provider supply
  - Cable protection and channelling systems
  - Mechanisms to prevent electromagnetic interferences
  - Fire detection and extinguishing systems
  - Fire, water, humidity and temperature alarm systems
  - Loading and unloading areas annexed to the DPC.

ACCESS CONTROL

- DPC access must be controlled using identification mechanisms. All individuals must be identified upon entry using one of the following methods:
    - A mechanism for physical access control
    - A list of individuals authorised to access
    - A log of the person's identity in the access control documents
- Access logs must contain the name, date and time of access
- All access outside normal working hours must be authorised and logged
- Visitors must access these areas accompanied by a person from the list of individuals authorised to access Visits must be monitored at all times, either by a person or a surveillance system such as video surveillance
- Doors must have electronic locks and self-locking mechanisms
- The video surveillance system must be capable of recording images on physical media, and must be stored outside the secure area
- Cleaning works must be supervised by a person in charge of the room who can notify and prevent accidents or deliberate damage to equipment

GENERAL CONTROLS

- Environmental and access control systems, and alarm systems, must be maintained and tested according to the manufacturer's instructions or the rules and regulations in force. These systems must have scheduled maintenance and testing works carried at least once a year
- The following must be logged accordingly:
    - The maintenance and testing results regarding the control systems and their alarms
    - Any incidents related to the environmental and access control systems
    - The issuance, delivery and revocation of keys, access cards and security codes
- Hazardous materials and/or fuel must be stored at a safe distance from the location of the secure area, and must not be stored in locations adjacent to the perimeter of this area
- Cabinets must be fireproof and lockable

- Emergency procedures must be maintained and tested at least once a year for each facility and significant risk

- Controls must include documentation for logging technical data, contact data and control procedures concerning the building where this area is located

- The environment in the security area must be clean and tidy; drinking and eating in the rooms in this area is forbidden

RESTRICTED ACCESS AREAS

Access to these areas is restricted to the FCC staff who work in them, or staff whose access has been expressly authorised.

ENVIRONMENTAL CONTROLS

- The windows and doors of these areas must be locked and controlled at all times The windows must be externally protected with security grilles or other physical barriers

- These areas must have the following technical measures implemented:

  - Suitable floors and ceilings for the equipment and risks associated to the works carried out in the room
  - Water and fireproof walls, doors and windows
  - Air conditioning systems
  - UPS systems
  - Cable protection and channelling systems
  - Fire detection and extinguishing systems

ACCESS CONTROL

- Access must be controlled by personal identification mechanisms or doors with security locks

- Visitors must access these areas accompanied by a person from the list of individuals authorised to access Visitors must be monitored for their entire stay

GENERAL CONTROLS

- Environmental and access control systems, and alarm systems, must be maintained according to the manufacturer's instructions or the rules and regulations in force Scheduled maintenance and testing works must be carried at least once a year

- The following must be logged accordingly:
    - The maintenance and testing results regarding the control systems and their alarms
    - Any incidents related to the environmental and access control systems
    - The issuance, delivery and revocation of keys, access cards and security codes
    - All people who access the area outside normal working hours. This access must be duly authorised
- Hazardous materials and/or fuel must be stored at a safe distance from the location of the secure area, and must not be stored in locations adjacent to the perimeter of the area.
- The environment in the security area must be clean and tidy; drinking, eating and storing unnecessary fuels in or close to the rooms in this area is forbidden

CONTROLLED ACCESS AREAS

Controlled Access Areas are open to FCC staff.

ENVIRONMENTAL CONTROLS

- The environmental controls implemented must be those established for the building where these areas are located
- At least one of the extinguishers located in these rooms must be suitable for electrical fires This equipment must be maintained and reviewed in accordance with the time limits established in the fire prevention regulations
- Computer equipment must be:
    - Raised at least ten centimetres from the floor in order to protect it from potential flooding
    - Not be close to windows, to protect them from theft and heat
    - Located in areas where the confidentiality of the data they process can be protected
- Critical data-processing systems must be connected to a UPS system to ensure their availability immediately after a power outage
- Equipment located in public areas must:
    - Be secured to office desks, especially laptops
    - Be unequivocally identified as the property of FCC

GENERAL CONTROLS

- Storage media must not be left on desks
- All offices fitted with computers and IT equipment must be kept locked whenever they are not occupied
- Cabinets must be fireproof and lockable whenever Restricted Data is stored in them

RESPONSIBILITIES

The Data Security and Risk Management Department must:

- Ensure that the security measures for the facilities are appropriate

The Information Systems and Technology Department must:

- Design the physical security measures required to ensure data processing in each of the secure areas
- Ensure that the physical security measures have been implemented according to the established plans
- Inform the Data Security and Risk Management Department of any physical security incidents that occur
- Designate a person to ensure the physical security controls required for each DPC are implemented

REVIEW OF THIS POLICY

This Physical Security Policy must be reviewed periodically for the following reasons:

- Whenever there are significant changes to FCC's working processes
- Whenever there are changes to the responsibilities of FCC's Committees and/or departments
- 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
  - Document Security Policy
  - Portable Devices' Standard
  - Asset Inventory Standard
  - IT Assets Usage Standard

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

  9. PHYSICAL AND ENVIRONMENTAL SECURITY

  - 9.1. Secure Areas
    - 9.1.1 Physical Security Perimeter
    - 9.1.2 Physical Entry Controls
    - 9.1.3 Office, Desk and Facilities' Security
    - 9.1.4 Protection Against External Threats and Environmental Conditions
    - 9.1.5 Working in Secure Areas
    - 9.1.6 Public Access, Loading and Unloading Areas

  - 9.2. Equipment Security
    - 9.2.1 Location and Protection of Equipment
    - 9.2.2 Supply Facilities
    - 9.2.3 Cable Security
    - 9.2.4 Equipment Maintenance

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