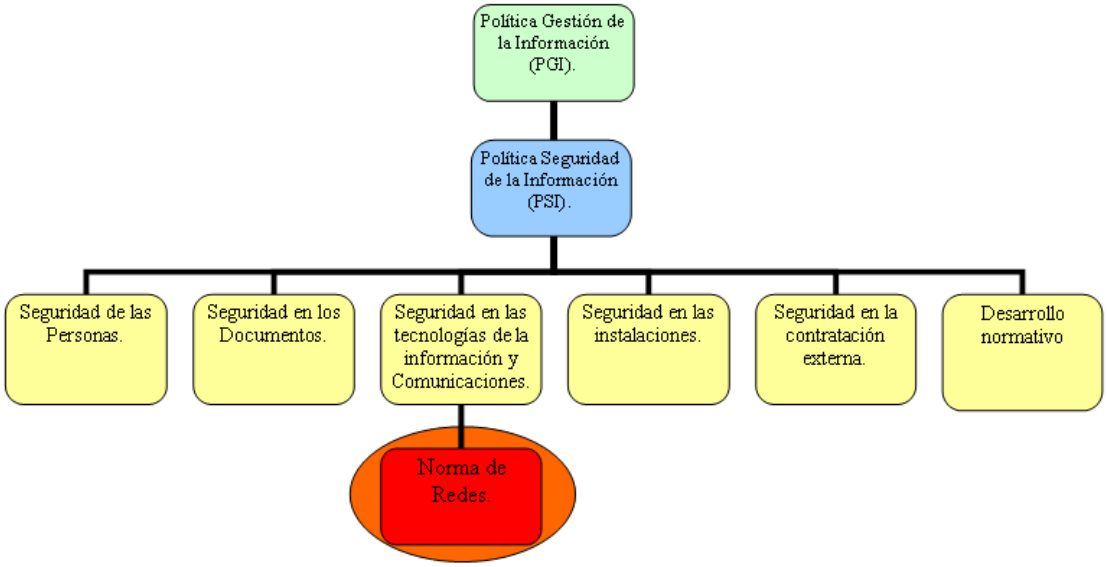
NETWORK SECURITY STANDARD

ID Code:	**NRM-10-EN**
Version:	**1.4**
Classification:	**FCC_INTERNAL_USE**
Approved by:	
Date:	

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

INDEX



With the evolution of IT, communications networks have become the backbone of communications between companies and individuals, transforming into an infrastructure that is key to the correct functioning of the information processed by the various areas of businesses everywhere.

In addition to these functionalities, networks allow businesses to connect to supplier networks over the Internet, which improves productivity and speeds up decision making.

Since networks are essential infrastructure, high security standards must be implemented for internal and external company networks.

PURPOSE

The purpose of this Standard is to establish the security requirements for managing FCC's information networks, in order to ensure the availability, integrity and confidentiality of information transmitted over them.

For the purposes of this Standard, an FCC network is understood as any network that is controlled and monitored by the Information Systems and Technology Department.

SCOPE

This Standard applies to all staff that manages or uses FCC's communications networks.

DESIGN AND DEVELOPMENT OF NETWORK ARCHITECTURE

The design and development of the architecture of the FCC networks are basic elements for the security of internal and external information communications. A correct design will help to achieve security objectives and will favor future network growth.

The principles that should be taken into account in the design and development of communication networks to ensure the assigned security levels are the following:

- Access to the networks must be based on criteria of authentication and authorization of prior access to the connection, complying with the principles of "need to know" and "minimum privilege" established in the Access Control Standard.
- Design considering the confidentiality, integrity and availability of the information that circulates through them.
- Principle of traffic control: blocking all connections unless specifically authorized.
- Networks must be operational and available on an uninterrupted basis.
- Use dominant technologies in the market, sufficiently tested in the industry and based on standards.
- Segmentation of the network in domains according to criteria of sensitivity (classification of information), type of business, functionality (eg, application servers, databases, ...) and others deemed necessary.
- Protection of all service areas or domains, both internally and at the perimeter level, by means of firewall technologies, which must have established the corresponding security policies and be all monitored activity.
- High availability of all components of the perimeter network architecture
- Services accessible from external networks and / or the Internet must be carried out through the deployment of an exchange zone, commonly called the Demilitarized Zone (DMZ).
- The security of FCC communications networks should be multilevel, covering the different types of devices that make up the networks, in order to reduce the

impact of the possible threats that they may suffer.

NETWORK INSTALLATION AND CONFIGURATION

The configuration of the networks during the installation and maintenance stages is essential when it comes to achieving the security levels that FCC has proposed in each of its communication networks.

The installation of FCC communication networks will take into account the following principles:

- All network devices will be located in a secure area with limited access in accordance with the FCC Facilities Physical Security Policy.
- The connection points between the FCC communications networks and those of the telecommunications operators and Access Providers must be located in secure environments with controlled access.

The configuration of communications networks will take into account the following principles:

- Compliance with the security requirements that are determined based on the risks and the level of classification of the information they process or access.
- All network devices will be protected with passwords, in accordance with the Password Security Standard. Accounts for network devices must be created with the minimum level of privileges that allow them to perform their functions.
- All FCC networks must follow the FCC Addressing Plan.
- The local interfaces of the routers that connect to external networks should be configured so that only incoming packets that are destined for network addresses that are within the address space of the internal network are accepted.
- The addresses of the Access Provider networks will not be redistributed or announced within the FCC communications network.
- DHCP servers will be configured so that they register the names of computers or MAC addresses of the clients, as well as that these records are available for a minimum period of 30 days.
- The disabling of all functions, ports and services except those strictly necessary for the operational operation of the network.
- All firewalls will have the "deny by default" parameter set.
- All incoming / outgoing traffic to / from the FCC network must pass through firewalls and be monitored through intrusion detection and prevention systems (IDS / IPS).
- All outgoing traffic, regardless of its destination, must be filtered so that it is verified that the source address of the packet belongs to the local internal network.
- All outgoing traffic to external networks must be analyzed through information leakage prevention mechanisms, in order to detect shipments of restricted information to the outside in an unauthorized manner.
- Traffic must be encrypted whenever business (non-public) information is transmitted on public or external networks, and restricted information on internal networks.
- Network traffic monitoring, both internally and externally, through:
    - Access and activity audit records.
    - Analysis and inspection in real time.
- The end users' equipment connected to the internal network must maintain a private IP address throughout the session, in order to maintain the traceability of the IP address with the user.

Where technically possible, communications networks should:

- Use an authentication server that grants the necessary credentials for administrative access to all network devices.
- Be configured so that all network devices end the session through the console port in case of prolonged inactivity.

NETWORK MANAGEMENT

The security related to managing communications networks must consider the following principles:

- All communications networks must be operated and administered using documented procedures, so that they can be used efficiently and the information flowing over them is effectively protected.
- Configuration, update and change control management must be carried using the procedures established, in accordance with the Configuration Management Standard.
- FCC networks must be managed by duly qualified system administrators, who are responsible for checking system performance and security on a daily basis.
- Connecting and using software or hardware components to FCC's communications networks is strictly forbidden when the components have not been expressly approved by FCC's Information Systems and Technology Department.
- Firewalls must be running at all times and must be administered centrally.
- All systems must be synchronised with the same system source.
- Network services provided to companies external to FCC and/or accessible from the Internet must be deployed in a Demilitarised Zone (DMZ).
- Connections to IAPs must comply with the External Companies' Security Policy.

NETWORK INTERCONNECTION

All network connections to the FCC network that take place after this Standard comes into force must be approved by the Certification Committee.

Network interconnections must establish the mechanisms to ensure the confidentiality, integrity and availability of the information flowing over all network nodes. To this end:

- Connections to non-FCC networks must take place in accordance with the External Companies' Security Policy.
- Remote access to network resources will only be allowed to authorised users authenticated on the system. In addition, user privileges will be restricted and information will be encrypted in accordance with the classification requirements of the information accessed.
- FCC connections to any external networks can take place via gateways, which must use the following devices and systems as a minimum:
    - Intrusion Detection System on the external network
    - Router ACLs
    - Firewalls
    - The use of a DMZ, whenever access to public services is required
    - Interconnected networks must not share DNS servers

WIRELESS NETWORK SECURITY

The specific principles that have to be considered for wireless networks are described in this section, as well as those described in previous sections that apply equally to wireless networks.

Installation and configuration of wireless networks must fulfill the following principles:

- Access points must be protected to prevent physical tampering attempts. Moreover, these devices must stay away from external sources that may cause electromagnetic interference.
- The signal strength should be the lowest possible to cover the physical area of the location under service, in order to prevent the signal arrives too powerful outside the facilities.
- Information should be transmitted encrypted prior to transmission to protect the confidentiality and integrity. Encryption must comply with the principles defined in the FCC Encryption Standard. (See Appendix I security protocols for wireless networks).
- Implementation of intrusion detection/prevention system (IDS / IPS) for wireless networks.
- Change the default SSID by a name that does not allows identifying the organization.
- In case of wireless networks used for public or guests access, there must be a firewall to separate the internal network from the wired network.

In addition from the principles of access control, the **access control to the wireless networks** must rule the following specific principles:

- The authentication protocol for wireless networks should be recognized by industry as secure (See Appendix I security protocols for wireless networks).
- Authentication should be always delegated to an authentication server and never in the access point. The authentication should be mutual, both client and access point.
- In case of networks where users store and transmit sensitive information, access must be made with certificates or other strong authentication mechanism.
- Automatic disconnection of devices after 15 minutes idle.
- Client devices before connecting to the wireless network must meet a list of requirements (authorized devices, antivirus updates, patches, firewall enabled, etc.).
- The administrator's access to access points must be with robust authentication mechanisms. Moreover, management tasks must be "out of band" through a wired network (encrypted) or in local mode (console).

The following situations are **not allowed** using wireless connections:

- Ad-hoc connections (direct connections between two or more teams) between devices, when at least one of them has access to the internal network or store confidential information, unless the connection is justified and approved for business and properly controlled. It is also not allowed the use of other wireless technologies (Example: Bluetooth).
- Access points not approved by the Systems and Technology Division

Periodic audits should be performed to verify compliance with the principles contained in this statement.

UNAUTHORISED NETWORK USAGE

Unauthorised usage of FCC networks is described in Code of use of technological media.

RESPONSIBILITIES

The Information Security and Risk Management Department must:

- Establish the security needs for FCC's communications networks.
- Recommend and coordinate the network audits, intrusion testing and vulnerability scanning required to maintain security on the communications networks.
- Verify the implementation and effectiveness of the controls and monitoring for network security.
- Report on the vulnerability testing carried out, as well as the actions undertaken, conclusions and recommendations after investigating any security incident or potential security incident.
- Monitor network traffic in real-time to detect unauthorised usage, intrusion attempts and any network device being compromised.

The Information Systems and Technology Department must:

- Establish and keep updated:
    - The network connection and interconnection architecture, and the Network IP Addressing Plan.
    - FCC's network topology - especially in relation to internal and external links, subnetworks and network equipment.
- Produce the procedures for securing network components
- Maintain an inventory of network elements, among which would be the access points to wireless networks authorized.
- Review all connection requirements at least six-monthly, in order to ensure that they are compliant and to evaluate the status of undocumented networks discovered during inspections.
- Review network access audit logs to determine whether there has been any unauthorised access or use of privileges on FCC's networks.
- Establish the technical mechanisms required to keep the time on all network components synchronized.
- Inform the Information security and Risk Management Department of any security incidents or potential security incidents affecting FCC's information networks.

The Certification Committee must:

- Approve FCC's network interconnections, ensuring the correct implementation of the security requirements.

The Units Responsible for their own Information must:

- Establish the security needs for their respective business areas

regardingFCC’s communications networks.

The Users must:

- Immediately notify the Information Systems and Technology Department of any system failures detected.
- Not install any hardware or software components without the approval of those in charge of administering the networks.
- Use network resources exclusively for the purposes of their functions within FCC, and comply with the information assets and services use policies.

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 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 Information security Department, who must then notify the Information 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

- External Companies’ Security Policy
- Information Management Policy
- FCC Security Policy for Physical Installations
- FCC Information Encryption
- Standard FCC Password
- Security Standard Access
- Control Standard

References to the ISO/IEC 27002:2007 Standard

10.1 OPERATING PROCEDURES AND RESPONSIBILITIES
- 10.1.1 Operating Procedures Documentation

10.4 PROTECTION AGAINST MALICIOUS SOFTWARE AND MOBILE CODE
- 10.4.1 Anti-Malware Control Measures

10.6 NETWORK SECURITY MANAGEMENT

10.10 NETWORK SECURITY MONITORING
- 10.10.1 Audit Logs
- 10.10.2 Monitoring System Use
- 10.10.6 Time Synchronisation

11.1 BUSINESS REQUIREMENTS FOR ACCESS CONTROL

11.4 NETWORK ACCESS CONTROL
- 11.4.1 Network Services Usage Policy
- 11.4.2 User Authentication for External Connections

APPENDIX I WIRELESS NETWORK SECURITY PROTOCOLS

The recommendations regarding the authentication and encryption protocols for wireless networks are the following:

- Wireless LAN connections based on IEEE 802.11i / WPA2 Enterprise. WPA2 is recommended due to be considered more advanced than WPA.
  - WPA2 uses AES encryption that is internationally considered as secure.
- Implement 802.1X/EAP IEEE authentication.
  - EAP types supported by IEEE 802.1X include: EAP-TLS, EAP-TTLS, PEAP V.0, PEAP v.1
  - The EAP type selection will depend on the type of service authentication in the organization (AD, LDAP, etc), and the requirement of authentication (password, certificate, etc).
  - The use of PSK authentication (Pre-shared keys) should be implemented only when there is not an authentication server and it is justified. In such cases, the password must be strong enough (at least 13 characters) and be changed periodically (30 days)
- Acquire WPA2 certified products
- Disable access points the ability to use WEP and TKIP authentication.

Source: Wi-Fi Alliance

DOCUMENT CHANGE CONTROL

Document Information

FILE NAME:				
VERSION	DATE	CHANGE	AUTHOR	REVIEWED BY
1.03	December 2011	New chapter "wireless networds" and small changes in some chapters.	Security Department	Sarto, Magda
1.4	August 2019	Revision of the document, translation update, equivalence with original document	Information Security and IT Risks	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