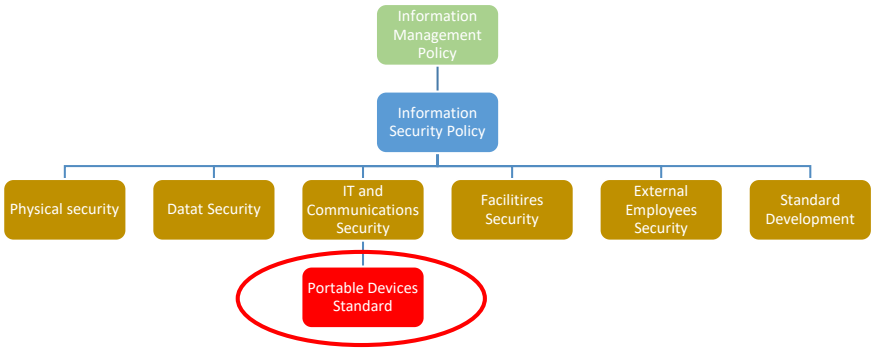
DATA SECURITY STANDARDS

~~NRM-06~~
PORTABLE DEVICES

ID Code:	**NRM-06-EN**
Version:	v2.1 ~~July2014~~September 2019
Classification:	FCC_INTERNAL_USE
Intended for:	• **Information Systems and Technology Department.** • **Unit Responsible for Data.** • **Portable devices users.**

INDEX

INTRODUCTION



Mobility is becoming the main feature of data processing technologies. Portable devices allow users flexibility to remotely access corporate systems and Internet from everywhere, increasing productivity and assisting communication and Information sharing.

In addition, and as a consequence of fast dissemination of portable personal devices, regulation of access to corporate information is required.

Portable devices, widen security perimeters and adds new logical and physical menaces. Indeed, these devices should be controlled and supervised by to secure FCC Group Security.

PURPOSE

The purpose of this Standard is to establish the measures required to ensure the confidentiality, integrity and availability of FCC data processed on portable devices used by staff or external collaborators.

SCOPE

This Standard applies to all corporate portable devices provided by FCC Group to employees, as well as to personal portable devices authorized to access information owned by FCC Group.

Manufacturers and admitted models will be those approved by Information Systems and Technology Department (ISTD/DSTI) and Information Security and IT Risks Department (ISITRD/DSIGRT). Laptops are out of scope of this standard, but tablets, PDAs, rugged devices, etc. are included.

DEFINITIONS

Portable device: It is a small device with processing abilities, limited storage capabilities and network connection. Nowadays, most used and popular portable devices are smart phones and tablets. Other devices, used primarily in field work, are called rugged devices, which are specifically designed to function reliably in difficult environments and conditions, such as strong vibrations, extreme temperatures and wet or dusty conditions.

Types of handset depending on the property:

• Corporate Device: Those provided by FCC Group to employees for professional use.

• Personal Device: Those owned by the employees to access corporate resources, if previously authorized.

MOBILITY PRINCIPLES

The use of portable devices, regardless if they are corporate or personal devices, to access corporate information is based on the following principles:

• The use of portable devices to access corporate resources will be allowed if these requirements are accomplished:

- It must be previously authorized by the supervisor of the user (starting at Department Director or Delegates Level) for business requirements.
- Only necessary Information to carry out its functions may be accessed.

• All portable devices connected to corporate resources will have implemented profiles and/or security controls required by the FCC Group.

• The selection of these profiles and security controls will be based on classification level of the information accessed, user profile and associated risks.

• All devices accessing corporate resources will be registered and monitored.

• FCC will not register private information on portable devices.

• According to the Access Control Standard, any change of duties or separation from service by users will involve the removal of all access to corporate resources that the user had through his/her portable device.

TERMS OF USE OF PORTABLE DEVICES

All employees authorized to access corporate resources through portable devices, regardless if they are corporate or personal devices, must accept the following conditions previously to any access:

• FCC reserves the right to implement or require minimum security requirements to access corporate resources.

• The user must not disable any security measures that FCC has implemented or required, and must configure portable device according to FCC security requirements.

- As a general rule, employee must have his/her device updated (Operating System and other software versions), must not bypass the restrictions imposed by the manufacturer (jailbreaking / rooting) and must follow FCC instructions about installing applications and download them through the official repositories.

• FCC may ban access when portable device does not reach security and configuration required.

• FCC will monitor the appropriate use of portable devices when accessing corporate resources. FCC will never register personal use of the portable device.

• Employees or external collaborators should grant access to portable devices to allow judicial investigations or internal audits when required.

• In case of loss or theft of the device, the user must inform the service user as soon as possible. FCC can remotely delete data and device configuration.

• In the case of personal devices, following conditions will also be applied:

- Users will only have technical support for uses related to corporate applications.
- FCC is not responsible for the loss of sensitive data on portable devices. Users are responsible for backing up his/her private data when necessary.

• Users will delete all corporate information when replacing their portable device as well as when separation from FCC service occurs, following *Return and Disposal of Technological Media Standard (NRM-18)*.

• Users are responsible for the use and safe-keeping of portable devices, to prevent loss, theft, damage or degradation.

• In addition to the conditions requirements included in this section, users must know and follow the rules outlined in the *Code of Using of Technological Media*, particularly those detailed in the Annex 14 and related to the use of portable devices.

SECURITY MEASURES

This section describes all measures intended to protect FCC information transmitted, accessed and /or stored in Portable devices.

Mandatory and Implementation levels of each security measure depend on the level of classification of the information accessed, user profile, technology and associated risks, and will be determined by the ISITRD/DSIGRT.

Access Control:

• All devices must have authentication mechanisms previously to accessing corporate resources.

• When the authentication mechanism is based on the use of passwords, this, should follow the Passwords Standard, in particular the specific section for portable devices.

• In case of implementation of any other authentication mechanism, it should be previously evaluated by ISITRD/DSIGRT.

Data Protection. Information leak:

• Corporate information during the access, transmission and treatment, should be isolated or separated from personal information in portable devices.

• When available, corporate information should be stored on corporate servers. If this is not possible, corporate information stored locally on the device must be encrypted following *Encryption Standard*.

• All applications that may access corporate information, such as email, must have measures to prevent information leaks.

Theft and loss:

• There will be mechanisms to remotely wipe all data in case of loss or theft of the device.

"Compliance" device:

• The device must be updated with the latest vendor patches and versions.

• Removing protections and limitations imposed by the manufacturer ("jailbreak" or Rooting) will not be allowed.

• There will be mechanisms to ensure that previously accessing to corporate resources, the portable device has the appropriate security level (eg: updated with latest versions and patches, PIN enabled, etc).

Secure Communications

• When corporate information is transmitted over public networks must be established an encrypted between the portable device and the corporate services channels.

Traceability:

• FCC information systems will collect all connections records made by portable devices on the resources of FCC.

Applications for portable devices:

• FCC may block the installation of applications considered unsafe.

• All development or acquisition of corporate portable applications must previously be reviewed and approved by ISITRD/DSIGRT in order to include security requirements, and then to perform the tests before putting into production safety.

Device Inventory:

• There will be an inventory or register of all devices with access to FCC information, and the person associated with that device.

Termination of use of device:

• Corporate information should be removed of any device when device is no longer usable by breakdown, update, separation from FCC service, or change of user Role (and device is not needed in his/her new role), following *Return and Disposal of Technological Media Standard*.

Antimalware

• Antimalware protection is always recommended on devices with open-source technology manufacturers.

RESPONSIBILITIES

The Units Responsible for their own Data must:

- Grant or revoke the permissions for processing their FCC Data via portable devices either through a corporate device or through a personal device. In any case, there should be a justified business reason.

The Data Security and Risk Management Department must:

- Establish the requirements for maintaining data security on portable devices accessing data or corporate resources.
- Oversee that safety measures are correctly implemented in the devices.
- Gather and analyse connections logs registered from portable devices.
- Monitor the use of the portable devices.
- Conduct User audits, without notice if necessary, to detect misuse and unauthorized access

- Authorize exceptions to this policy.

The Information Systems and Technology Department must:

- Implement technical measures to comply with this standard, as specified by the Information Security and Technology Risk Department (ISTRD)
- Enable access to corporate resources through portable devices owned by users, previously requested by the Chief, Director of Department or his/her hierarchical superior manager and the necessary security controls were implemented.
- Maintain an inventory of portable devices accessing the FCC resources.
- Manage incidents concerning portable devices.
- Keep a list of technologies and manufacturers of portable devices supported by FCC.

The Users must:

- Accept and fulfill the conditions of use of portable devices, as specified in this standard, and the Code of Use of Technology Media.
- Assume responsibility for the use and care of portable devices that have access to resources FCC.
- To communicate immediately to Servicedesk, or alternatively, to Information Security Department (ISITRD/DSIGRT), any security incident.

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 Data Security Department, who must then notify the Data Security Department Committee of this information.

EXCEPTIONS TO THIS STANDARD

Any exception to this Standard should be justified in writing and authorized by DSIGRT.

The only way to communicate the exceptions will be the official mailbox INFOSECURITY@fcc.es and/or any other channel managed by "Service Desk FCC" to receive request.

Código de campo cambiado

The person responsible for the exception will be a hierarchical superior (beginning in Director of Department or Delegate).

The protocol to communicate this exception will use this form:

EXCEPTIONS TO THIS STANDARD	
Applicant	
Responsible	
Policy/Code of use/Standard	
Non-compliant Section	
Description of the Exception and justification	

DISCIPLINARY SYSTEM

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
  - Data Assets Inventory Standard
  - Incident Management Standard
  - Password Standard
  - Access Control Standard
  - Backup Management Standard
  - Encryption Standard

- **References to the ISO/IEC 27002:2007 Standard**
  - 6.2 THIRD PARTY ACCESS SECURITY
    - 6.2.1 Identification of third party access risks
  - 7.1. RESPONSIBILITY OVER ASSETS

- 7.1.1 Asset inventory
- 7.1.2 Asset ownership
- 7.1.3 Proper use of assets

- 7.2. CLASSIFICATION OF DATA
  - 7.2.1. Classification guidelines
  - 7.2.2 Data labelling and handling

- 9.2 EQUIPMENT SECURITY
  - 9.2.1 Installation and Protection of Equipment
  - 9.2.5 Security of Equipment Outside the Organisation's Facilities
  - 9.2.7 Transferring FCC Assets to External Organisations

- 10.4 PROTECTION AGAINST MALICIOUS SOFTWARE AND PORTABLE CODE
  - 10.4.1 Malicious software control measures

- 10.7 DATA MEDIA USE
  - 10.7.1 Removable media management
  - 10.7.2 Withdrawal of media
  - 10.7.3 Data Processing Procedures

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
2.0	February 2013	General Revision	ISITRD/DSIGRT	Policy Committee
2.1	July 2014	General Revision	ISITRD/DSIGRT	
2.1	September 2019	General Revision	ISITRD/DSIGRT	

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

CLASIFICACIÓN: FCC_INTERNAL_USE

END OF DOCUMENT