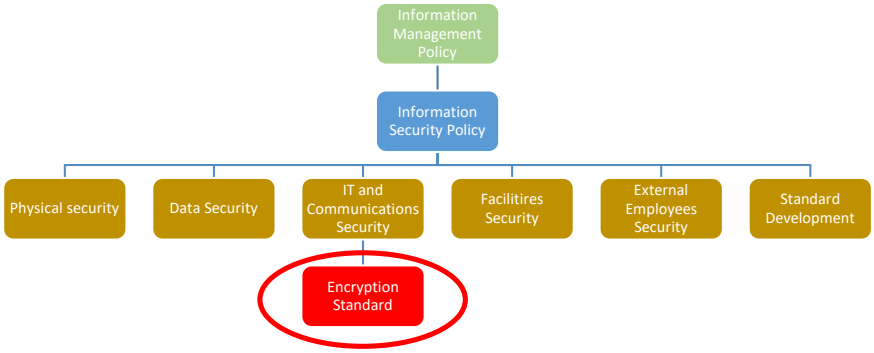
DATA SECURITY STANDARDS

~~NRM-03~~ ENCRYPTION

ID Code:	**NRM-03-EN**
Version and Date:	**v1.1 ~~July2014~~August 2019**
Classification:	FCC_INTERNAL_USE
Intended for:	**Information Systems and Technology Department**

INDEX

INTRODUCTION



Encryption is one of the most important means of ensuring the confidentiality and integrity of data, both in storage and while transmitting it.

Cryptologic systems render electronic data illegible to individuals not authorised to access it.

Encryption mechanisms are increasingly becoming a requirement imposed by national and international regulations to guarantee secure data exchanges.

The use of encryption technologies requires the user to hold a specific encryption key to render the data legible. Therefore, the implementation of an encryption service must be accompanied by suitable measures and controls to ensure the availability of the encrypted data when necessary.

PURPOSE

This Standard establishes the measures required to ensure the integrity and confidentiality of data by means of:

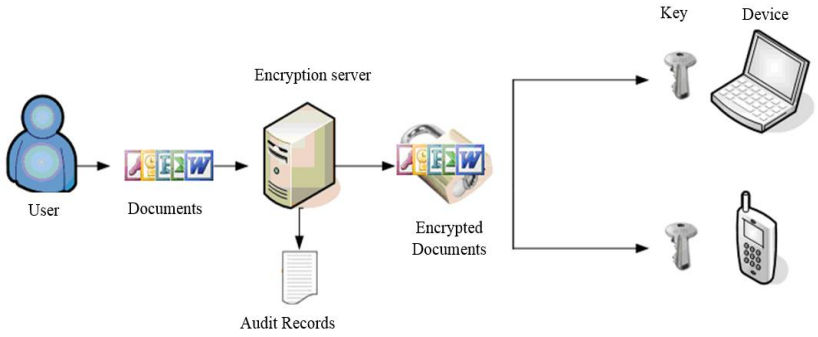
- A data encryption strategy for both information stored and transmitted.
- Data systems encryption key management

SCOPE

This Standard applies to all automated FCC Group data, whose confidentiality requires encryption mechanisms to protect it.

PRINCIPLES

- Data is encrypted based on the potential impact of a given incident, rather than the likelihood of the incident actually taking place.
- The data encryption measures to be implemented must be proportionate to the data risk level, which is based on the classification of the data.
- The products and algorithms chosen for data encryption must:
  - Be certified industrially
  - Only be handled by authorised staff
  - Be approved by the Data Security Department
- The implementation strategy must consider the effect the encryption mechanisms may have on the performance of the data systems used, and implementation must not diminish the availability of such systems.



ENCRYPTION STANDARD

The data encryption strategy shall be based on the following technical and organisational measures:

- Encryption can be deployed via hardware and/or software solutions
- The files and devices to be encrypted are the following:

- Passwords stored or transmitted via any data system
- Highly classified personal data
- The following must be encrypted for Restricted Data:
    - Backups
    - Emails
    - Transmissions sent outside FCC's data systems
    - Access from remote systems or devices
    - Data stored on any server, workstation or device, when its protection cannot be guaranteed via physical or logical controls, and there is a risk of data disclosure or theft

- All systems containing encrypted data must have the procedures in place to ensure access to the encryption keys when necessary, to allow decryption of Information in reasonable time period.
- All legal implications on the use of cryptographic techniques must be considered before any encrypted data is transmitted.
- The procedures for managing cryptologic material must ensure the segregation of functions and rotation of tasks within a dual control scenario.
- The length of encryption keys will be established based on the associated algorithm and the classification of the data to be protected.
- Encryption keys must be securely stored in a location other than the place where the encrypted data is stored.
- Whenever possible, encryption keys should be managed through directory-services-based technologies, such as Active Directory.
- Encryption, decryption and encryption key management must be transparent to the user.

RESPONSIBILITIES

The Data Security and Risk Management Department must:

- Establish the encryption needs
- Control the correct implementation of this Standard
- Evaluate any security incidents related to data encryption

The Information Systems and Technology Department must:

- Manage:
  - The cryptographic solutions implemented in the FCC Group
  - The procedures for implementing and managing encryption solutions, as well as the procedures for safeguarding and recovering encryption keys
- Notify the Data Security and Risk Management Department of any reported security incidents related to encryption

The Units Responsible for their Data must notify the Data Security and Risk Management Department of their encryption needs, as well as any incident related to data or transmission encryption.

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	

VIOLATIONS OF THIS STANDARD

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 Security Policy.
  - Data Management Policy.
  - Document Security Policy.
  - Incident Management Standard.

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

  12. ACQUISITION, DEVELOPMENT AND MAINTENANCE OF DATA SYSTEMS

  - 12.3 Cryptographic Controls.
  - 12.3.2 Encryption Key Management

  15. COMPLIANCE

  - 15.1.3 Protecting organisational logs
  - 15.1.6 Regulation of encryption controls

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
1.1	2014 July	General Revision	Information Security and IT Risks Department	
1.1	2019~~4~~ August~~July~~	General Revision	Information Security and IT Risks Department	

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