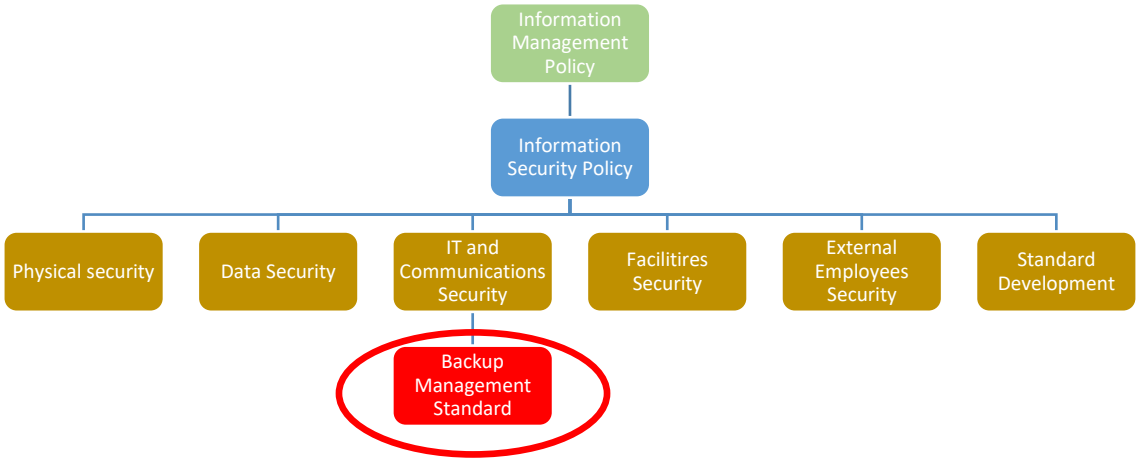
DATA SECURITY STANDARDS

BACKUP MANAGEMENT

ID Code:	**NRM-07-EN**
Version:	**V1.1 September2019**
Classification:	**FCC_INTERNAL_USE**
Intended for:	**Information Systems and Technology Department**

INDEX

INTRODUCTION



One of the biggest concerns regarding the correct performance of data systems is maintaining the availability levels agreed with users for data technology services, which are based on how critical the data processed in their systems is.

In today's highly interconnected world, organisations believe the availability of data backups is an essential part of systems supporting business activities efficiently and affordably.

Scheduled backups are not only crucial for the continuity of day-to-day operations, they are also a key element of disaster recovery planning and safeguarding data for legal or financial purposes.

Advances in technology and communications are changing the way we view backing up data, with the traditional concept of hardware filing replaced by high-availability and remote data mirroring systems. Whatever the system used to backup, the underlying concept is the need for high data availability for data technology services, against a backdrop of threats of varying size and origin.

PURPOSE

The purpose of this Standard is to establish the measures required to ensure the integrity, confidentiality and availability of FCC Group Data for the entire backup life cycle.

SCOPE

This Standard applies to the storage devices used for the data systems managed by the FCC Group. Namely:

- Fixed discs or other non-volatile storage devices, which work in stand-alone or network-connected mode
- Other removable electronic media

Backup management is understood as:

- Creating backups
- Data recovery testing
- Maintenance and storage of devices
- Backup data deletion

Correctly executing these actions will ensure effective data backup and recovery.

PRINCIPLES

The backups carried out by FCC's data systems must:

- be documented and scheduled according to:
  - how critical the data processes are,
  - the recovery and restore times,
  - the time backup logs must be retained, as stipulated in current legislation;

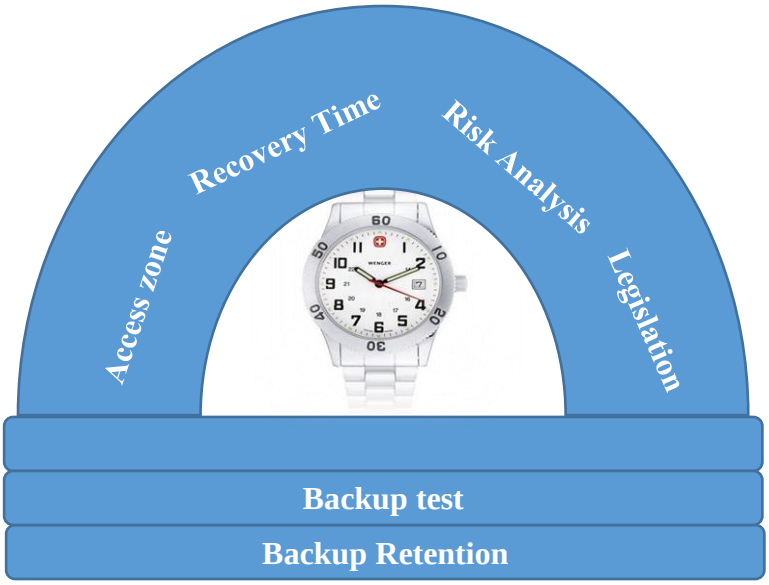
- be scheduled considering:
  - the specific measures for ensuring that data can be recovered whenever unforeseen incidents occur,
  - the fulfilment of the requirements established in this Standard and other related Standards;

- be protected by organisational measures and techniques for their entire life cycle, based on:
  - the risk level of the backed-up data
  - the classification of the data. To this end, backup storage devices must be labelled and protected according to the highest classification level of the backed-up data;

- be stored on devices that:
  - ensure the availability of data while it is being backed-up,
  - fulfil the data migration security operating procedures whenever data needs to be migrated from one storage device to another, as well as ensuring that the new device is as secure as the device where the data was initially stored;

- be protected, encrypted, labelled and transported according to the requirements of both the Data Management Policy and current legislation

Whenever FCC outsources backup management to an external company, this company must be contracted in accordance with the provisions of FCC's External Companies' Policy.



BACKUPS

Data systems must be backed up in such a way that they ensure full system recovery for any eventuality, and safeguard the confidentiality and integrity of the data processed at all stages of their life cycle.

Backups must be carried out by authorised staff, specially trained for this purpose.

Backup schedules can be defined in Service Level Agreements (SLAs), operating procedures or user guides for the data systems managed by FCC. Regardless of where they are defined, backups must be carried out at least once a week.

Wherever technically possible, systems must be backed-up automatically, in order to facilitate the smooth running of operational tasks and prevent human error.

Accurate and complete audit logs must be generated as part of the backup process; these audits must log the name of the person who carried out the backup, the date and time, the reason for backing-up, the file contents, and any subsequent actions required. Backups must be referenced with a code or sequence number.

BACKUP TESTING

Disaster recovery procedures must be tested at least once a year, and must ensure:

- that data can be recovered correctly whenever required
- that data can be recovered within the target recovery time

DATA RESTORES

Any data restored from backup must:

- be authorised by the person responsible for the data, or the person(s) delegated to this task
- be carried out by qualified staff who are authorised to carry out such tasks, by means of a formal procedure
- be documented in a log which identifies the operation, the tape and the data recovered, as well as the outcome of the operation and any related events that may have occurred

BACKUP RETENTION

Backup storage media must be stored in a suitable environment; this environment must be far enough away from the main data systems location, that the media is protected from any damage arising from unforeseen incidents that could occur there.

All incoming and outgoing, formally documented backup media must be logged.

Backups containing **Non-Restricted** Data must be stored for a minimum of one year, with the security controls for preventing theft or deterioration of the media maintained throughout this period.

Backups containing **Restricted** Data must be stored for a minimum of two years, and must only be accessed by duly authorised staff. Media containing this type of data must be safeguarded from physical and environmental hazards in a lockable fireproof safe or similar enclosure, with physical or logical access controls in place to ensure the confidentiality and integrity of the data.

Backups must be retained for the periods stipulated by current legislation, or based on the needs of the unit responsible for the data.

DATA DELETIONS

Backup data deletions must:

- be carried out using the correct corporate mechanisms for the classification of the data and the disclosure risks involved

- be carried out in such a way that the action is irreversible and the data cannot be recovered

Please Note: Backup storage media must be destroyed if it hinders the deletion of the data.

RESPONSIBILITIES

The Data Security and Risk Management Department must:

- Oversee the correct implementation of this Standard
- Ensure that the encryption method to be used is compliant with the FCC Data Encryption Policy, where appropriate

The Information Systems and Technology Department must:

- Manage the security requirements for the entire backup life cycle.
- Provide the resources required to backup the systems managed by them.
- Ensure that all FCC backup data for the systems managed by them can be recovered in the event of an unforeseen incident.
- Implement the required technical means for protecting the security of data stored on backup media.
- Configure the audit logs to record all actions carried out over the entire backup life cycle.

The Units Responsible for their own Data must:

- Classify the data stored on backup media
- Authorise the recovery of the backed-up data
- Ensure that the controls established in this Standard regarding backups of their data are properly implemented

System users must backup the data stored on their local computers.

REVIEW OF THIS STANDARD

This Standard may be reviewed in the following circumstances:

- Whenever there are significant changes to FCC's working processes
- 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 Standard
- Whenever there are major technology changes

The information used for the review of this Standard must be notified to the Data Security Department by the departments or services affected by it, 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.

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

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
- Asset Inventory Standard
- Data Encryption Standard

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

  - 10.5 Backups
    - 10.5.1 Data Backups

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	July 2014	General Review	Information Security and IT Risks Department	
1.1	September 2019	General Review	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

CLASSIFICATION: FCC_INTERNAL_USE

END OF DOCUMENT