DATA SECURITY STANDARDS

~~NRM-02~~ DATABASES

ID Code:	**NRM-02-EN**
Version and Date:	**v1.1 July2014**
Classification:	FCC_INTERNAL_USE
Intended for:	**Information Systems and Technology Department**

INDEX

INTRODUCTION

Data is one of the main assets used by the FCC Group in their business activities. The use of data is essential for competing in the various environments and geographical areas FCC operates in.

Most data is stored in Databases (DBs) offering various features and technologies. To ensure the correct management of FCC data, DBs must guarantee the confidentiality, integrity and availability of the data they store.

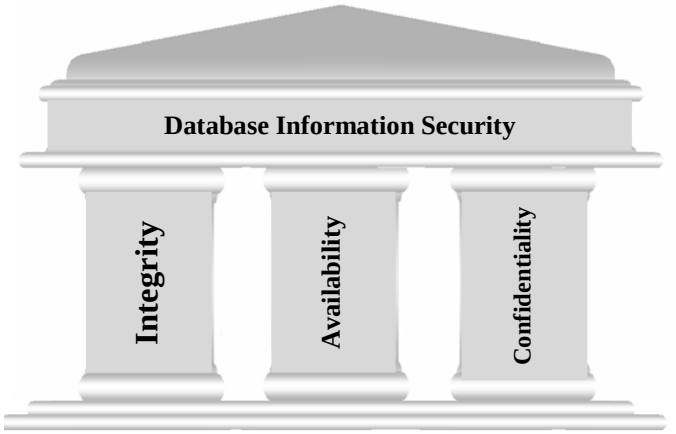
PURPOSE

The purpose of this Standard is to protect FCC Group DB data from unauthorised access, modification or destruction.

SCOPE

This Standard applies to all staff of the FCC Group either internal or external, (hereinafter referred to as FCC), with access to the DB data residing in the Group's IT Systems.

DATABASE SECURITY STANDARD



- Access to FCC DB data must be authorised by the functional unit responsible for that data.
- When a DB access account has not been used for more than three months, it must be blocked.
- The Information Systems and Technology Department will conduct monthly inspections of DB access activities; any accounts that have not been active for more than three months will be reported to the functional unit responsible for data, so that they can take the necessary measures to revoke access.
- Any authorised DB users who unduly modifies, destroys, copies or causes data loss will be disciplined in accordance with the current disciplinary system.

All FCC DB administrators (DBA) and staff responsible for DB maintenance must:

- Maintain the integrity and stability of DBs at all times.
- Ensure that DB table access control is carried out by means of roles/profiles and access permissions. In case a user of a Database stop providing his/her services to FCC, all his/her privileges to access database will be removed immediately by Database manager.
- These access privileges are strict requirements for FCC DB data processing staff to be able to carry out their functions.
- Ensure that default manufacturers' passwords are changed in accordance with the FCC Password Security Standard.
- Ensure that links within DBs to other DB data are not used, unless there are formally justified grounds to use them.

Any modifications to FCC DBs must be carried out as follows:

- Modifications to the DB structure must be authorised by the unit responsible for the data, as well as the DBA. The reason for the modification and the technical procedures must be duly documented.
- The DB must be fully backed up before any changes are initiated following Backup Standard.
- The business functionalities and processing capacities of all FCC DBs must be tested before they are transferred to live environments.
- Emergency data modifications can only be carried out under critical circumstances, in accordance with the emergency procedures established in the Incident Management and Business Continuity Standards. It is always assumed that an incident has taken place in these cases, so that incident must be registered accordingly.
- The consistency and integrity of indexes must be verified at least once monthly. Any loss of integrity must be resolved immediately.
- An index update and optimisation strategy must also be defined, which will depend on the size and established response times required. This strategy must be prepared in accordance with the guidelines established in this Standard.
- Whenever a business unit establishes that the availability of their data is highly critical, a DB redundancy strategy must be implemented by them.
- All DB access attempts and session logins must be recorded in an audit log.
- Whenever the classification assigned to FCC DB data requires the content to be encrypted, the encryption must be carried out in accordance with the provisions established in the Encryption Security Standard. Encryption must be carried out with no user intervention.
- Whenever data collection tasks are carried out, the temporary files and locations they are loaded to must never be left unprotected. In addition, measures must be in place to ensure that these temporary files and locations are deleted and destroyed once they have been used. These measures shall be established and carried out by the Information Systems and Technology Department on a weekly basis.
- DB management must comply with the provisions established in both the Configuration Control Standard and the Backup Management Standard.
- To prevent unauthorised access, all tools used for data cleansing, debugging and loading processes must be installed with their security measures correctly configured.

RESPONSIBILITIES

The Data Security and Risk Management Department must:

- Ensure that the management and control measures established for FCC DBs have been implemented and are operational, in accordance with the provisions established in this Standard.

The Information Systems and Technology Department must:

- Manage the correct implementation of the security measures and technological controls for DBs established in this Standard.
- Notify the Data Security and Risk Management Department of any incidents that take place, in accordance with the FCC Incident Management Standard.

The Units Responsible for the Data must:

- Notify the Data Security and Risk Management Department of any DB security requirements.
- Immediately notify the Data Security and Risk Management Department whenever they suspect their data access has been accessed without authorisation.
- Authorize or unauthorize access to FCC DB data.

REVIEW OF THIS STANDARD

This Standard may be reviewed in the following circumstances:

- Whenever there are changes to the responsibilities undertaken by Committees and/or Security Authorities and/or FCC departments.
- Whenever improvements are suggested as a result of audits carried out.
- 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

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**

- FCC Data Security Policy
- FCC Information Encryption Standard
- FCC Personal Data Policy
- FCC Password Security Standard
- Configuration Control Standard

- **References to the ISO/IEC 27002:2007 Standard**
  - 6.1 INTERNAL ORGANISATION
    - 6.1.4 Resource authorisation process for data processing
  - 7.2.1 CLASSIFICATION GUIDELINES
  - 10.3 SYSTEM PLANNING AND ACCEPTANCE
    - 10.3.2 System Acceptance
  - 10.5 BACKUPS
    - 10.5.1 Data Backups
  - 10.7 USE OF DATA MEDIUMS
    - 10.7.3 Data Processing Procedures
    - 10.7.4 System Documentation Security
  - 11.1 BUSINESS REQUIREMENTS FOR ACCESS CONTROL
    - 11.1.1 Access Control
  - 12.2 CORRECT APPLICATION PROCESSING
  - 12.5 DEVELOPMENT AND SUPPORT PROCESS SECURITY
    - 12.5.1 Change Control 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
1.1	2014 July	General Revision	Information Security and IT Risks Department	FCC Executive Committee
1.1	August 2019	General Revision	Information Security and IT Risks Department	FCC Executive Committee

Please Note: Hard-copies are not controlled

END OF DOCUMENT