FCC Group Database Standard

January 2026

Document Version Control				
Version	**Date**	**Author**	**Detail**	**Approved by**
1.0	April 2009	IS	Document creation	FCC Executive Committee
1.1	July 2014	IS	Document Review	FCC Executive Committee
	August 2019	IS	Document Review	FCC Executive Committee
2.0	January 2026	IS	Document Review ISO/IEC 27001:2022 ENS	Chief Information Security Officer (CISO)

INDEX

1. Introduction

This document is part of the FCC Group's Information Security Regulatory Framework, which establishes the Group's mandatory requirements on Information Security.

The Security Regulatory Framework is periodically reviewed and updated by the Information Security Department (hereinafter, the IS Department), in accordance with the provisions of the Regulatory Framework Management and Maintenance Document. This document contains information on the version history, revisions, and approvals of this Standard, as well as its relationship and dependence on the rest of the regulatory documents.

This Standard will be reviewed at least once a year unless circumstances recommend or require an earlier revision.

1.1 Purpose

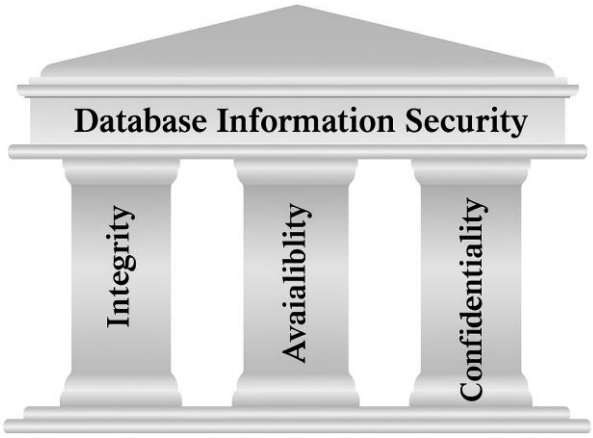
The purpose of this Standard is to ensure the protection of the data stored in Group’s Databases against unauthorized access, alteration, or destruction.

1.2 Scope

This Standard applies to all personnel and collaborators of the FCC Group, hereinafter referred to as FCC, who have access to the information contained in the Databases hosted in the Group’s Information Systems, as well as to the information systems that are interconnected with such Databases.

2. Development

2.1 Principles



- Access to FCC information stored in the databases must be authorized by the person responsible for that information.
- When a database access account is not expected to be used for a period longer than three months, it must remain blocked.
- The person responsible for the information shall conduct regular checks of database access activity. When access accounts are identified with periods of inactivity exceeding three months, the corresponding responsible party should be informed so that appropriate measures may be taken regarding the revocation of access.
- Any user who, while being authorized to access the databases, improperly modifies, destroys, copies, or causes loss of information shall be sanctioned in accordance with the applicable disciplinary regime.

Database administrators or FCC personnel who perform Database maintenance shall:

- Maintain, always, the integrity and stability of the Databases.
- Be aware of the risks and vulnerabilities associated with the use of databases supplied by providers.
- Access control to the tables that are part of the Database shall be conducted through roles/profiles and access permissions. These privileges shall be strictly necessary for the performance of the functions conducted by FCC personnel who will manage the information contained in the Databases; additionally, privileges shall be granted on a temporary basis until the user makes the changes or completes the relevant task.
- Default passwords supplied by the manufacturer must be changed in accordance with the FCC Group Password Security Standard.
- The use of links within the Databases to information contained in other Databases is prohibited and may only be conducted in cases where their necessity is formally justified.

Modifications to FCC Databases shall comply with the following requirements:

- Modifications to the structure of the Databases must be authorized by the information owner and by the Database Administrator. The reason for the modification and the technical procedure must be duly documented.
- A full backup must be performed before initiating any change.
- Before being moved to live production environments, all FCC Databases must be previously evaluated regarding their business functionalities and processing capacities.
- Emergency data modifications may only be conducted under critical circumstances, in accordance with the emergency procedures developed in the Incident Management and Business Continuity Standards. In this case, it shall always be considered that an incident has occurred and, as such, must be duly recorded.
- The consistency and integrity of indexes shall be verified with a maximum periodicity of one month. Any loss of integrity must be resolved immediately.
- An index update and optimization strategy must be established, based on size, and established response time requirements, and always in accordance with the guidelines set out in this Standard.
- If the business establishes an elevated level of criticality with respect to information availability, a database redundancy strategy must be implemented.
- All access to the Databases and login sessions shall be recorded in an audit log.
- When, based on the classification level assigned to the information stored in FCC Databases, encryption of their contents is mandatory, it shall be conducted in accordance with the provisions of the Cryptography Standard. Encryption shall be performed without the need for user intervention.
- Temporary files and loading areas used for data acquisition tasks shall not be left unprotected. Likewise, their secure deletion and destruction must be ensured once they are no longer in use. The Information Owner shall establish periodic deletion processes for such data on a weekly basis.
- Database management shall comply with the principles established in the Configuration and Change Control Standard and in the Backup Management Standard.
- Tools used in data cleansing, debugging and data loading processes must be installed with their security measures fully configured and approved by the FCC Group to prevent unauthorized access and ensure secure data handling.

3. Responsibilities

The IS Department shall:

- Ensure that the management measures and controls established for FCC Databases have been implemented and are operational, as set out in this Standard.
- Stay up to date and produce intelligence on new threats and vulnerabilities related to databases.

The Information Systems and Technology Division shall:

- Manage the correct implementation of the security measures and technological control of the Databases established in this Standard.
- Notify any incident to the IS Department, in compliance with the FCC Group Incident Management Standard.

The Information Owners shall:

- Notify the IS Department of their needs regarding Database security measures.
- Immediately notify the IS Department of any suspicion of unauthorized access to information.
- Notify any incident in which personal data may be or have been compromised to the DPO/Data Protection Coordinator of the corresponding area.
- Authorize access to FCC Information stored in the Databases.

4. Normative reference

This document has been reviewed by the IS Department, and its drafting takes as a reference the international standard ISO 27001:2022 and the ENS.

4.1 Regulatory controls ISO27001:2022 and ENS

ID Control ISO	ISO/IEC 27001:2022 control	ENS Correspondence
5.2	Roles and responsibilities in information security	[org.4] Authorization Process
5.3	Segregation of duties	[op.acc.3] Segregation of functions and tasks
5.5	Contact with authorities	[op.exp.7] Incident Management
5.6	Contact with special interest groups	[org.1] Security Policy
5.7	Threat intelligence	[op.mon.3] Monitoring
5.8	Information security in project management	[op.pl.3] Acquisition of new components
5.12	Information classification	[mp.info.2] Information qualification
5.13	Information labelling	[mp.si.1] Media marking
5.15	Access control	[op.acc.2] Access requirements
5.19	Information security in supplier relationships	[op.ext.1] Contracting and service level agreements
5.37	Documented operating procedures	[org.3] Security procedures
8.2	Privileged access rights	[op.acc.1] Identification
8.6	Capacity management	[op.pl.4] Capacity management; [mp.s.4] Protection against denial of service
8.7	Protection against malware	[op.exp.6] Protection against malicious code
8.8	Technical vulnerability management	[op.mon.3] Monitoring; [op.exp.4] Maintenance and updates
8.9	Configuration management	[op.exp.2] Security configuration; [op.exp.3] Configuration management
8.10	Information disposal	[mp.si.5] Deletion and destruction
8.13	Information backups	[mp.info.6] Backups
8.19	Software installation on operating systems	[op.exp.2] Security configuration; [op.acc.3] Segregation of functions and

		tasks; [mp.sw.2] Acceptance and commissioning
8.25	Secure developments lifecycle	[mp.sw.1] Application development
8.27	Secure system architecture and engineering principles	[op.pl.2] Security architecture; [mp.sw.1] Application development
8.28	Secure coding	[mp.sw.1] Application development
8.29	Security testing in development and acceptance	[mp.sw.2] Acceptance and commissioning
8.30	Outsourced development	[op.ext.1] Contracting and service level agreements; [mp.sw.1] Application development; [mp.sw.2] Acceptance and commissioning; [op.ext.3] Supply chain protection
8.31	Separation of development, testing, and production environments	[mp.sw.2] Acceptance and commissioning
8.32	Change management	[op.exp.5] Change management
8.33	Test data	[mp.sw.1] Application development; [mp.sw.2] Acceptance and commissioning