FCC Group Privacy Standard

January 2026

Document Version Control				
Version	**Date**	**Author**	**Detail**	**Approved by**
1.0	April 2009	IS	Document creation	FCC Executive Committee
	October 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 4

1.1 Purpose 4

1.2 Scope 4

1.2.1 Geographical 4

1.2.1 Material 4

2. Data Privacy Security 5

2.1 Definitions 5

2.2 Values in Data Protection 6

2.3 General Principles in the Management of Personal Data 7

2.3.1 Principle of Consent 7

2.3.2 Principle of Information to the Data Subject 7

2.3.3 Principle of Proportionality 7

2.3.4 Principle of Quality 7

2.3.5 Principle of Security 7

2.3.6 Principle of Legality 7

2.4 Processing Guidelines 8

2.4.1 Organization and Responsibilities in Privacy Matters 8

2.4.1.1 Organizational Structure 8

2.4.1.2 Roles and responsibilities 8

2.4.2 Processing of Sensitive Data 9

2.4.3 Service Provision Contracts 9

2.4.4 International Data Transfers 9

2.4.5 Rights of Access, Rectification, Erasure, and Objection 10

2.4.6 Audits 10

2.4.7 Immediate Reporting of Data Protection Incidents 10

2.4.8 Compliance with Applicable Data Protection Legislation in Each State 10

3. Responsibilities 10

4. Normative reference 11

4.1 Regulatory controls ISO27001:2022 and ENS 11

1. Introduction

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

The Security Regulatory Framework is periodically reviewed and updated periodically 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 other 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 specify the fundamental principles and essential requirements that must be observed and fulfilled in the processing of Personal Data by the Entities of the FCC Group.

1.2 Scope

1.2.1 Geographical

This Standard applies to the Entities belonging to the FCC Group located in any State/Country/Region worldwide (hereinafter, FCC Entity/Entities), which include the following:

- Entities in which the FCC Group holds a majority ownership stake.
- Entities in which, despite the FCC Group not holding a majority ownership stake, it nevertheless exercises management control.

1.2.1 Material

This Standard applies to all information containing Personal Data (in paper and/or electronic format) that is collected, accessed, managed, transferred, or otherwise processed by personnel of FCC Entities or their Partners and/or Providers.

2. Data Privacy Security

2.1 Definitions

- “Personal Data”: All information relating to an identified or identifiable natural person (the “data subject”). A person shall be considered identifiable when their identity can be determined, directly or indirectly, in particular by reference to an identification number or to one or more specific elements characteristic of their physical, physiological, mental, economic, cultural, or social identity.
- “Processing of Personal Data” (“processing”): Any operation or set of operations, whether or not carried out by automated means, applied to personal data, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or any other form of enabling access, comparison or interconnection, as well as blocking, erasure, or destruction.
- **“**Data Controller”: The natural or legal person, public authority, service, or any other body which, alone or jointly with others, determines the purposes and means of the processing of personal data, and which shall be governed by its national law. in this regard, each FCC Group Entity shall function as the Data Controller in relation to the personal data it manages (e.g., Employees, Customers, and Suppliers).
- “Data Processor”: The natural or legal person, public authority, service, or any other body which, alone or jointly with others, processes personal data on behalf of the Data Controller.
- “Data Subject’s Consent”: Any freely given, specific, and informed expression of will by which the data subject agrees to the processing of personal data concerning them.
- “Sensitive Data”: Data relating to health, trade union membership, racial or ethnic origin, political opinions, religious or philosophical beliefs, as well as data relating to sexuality.
- “Data Protection Coordinator”: A person belonging to an FCC Group Entity, appointed to coordinate data protection actions within a specific area of the FCC Group.
- “Data Protection Security Officer”: A person belonging to an FCC Group Entity, appointed to manage data protection–related actions for one or more FCC Group Entities.
- “Data Cancellation”: A procedure by which the Data Controller ceases to use the data. Cancellation entails the deletion or physical removal of the data, except when it is necessary to retain them for the statute of limitations of potential liabilities arising from the processing. In such cases, the data shall be retained after being blocked, meaning they are identified and reserved in order to prevent their processing except for making them available to public administrations, courts, or tribunals. Once this period has elapsed, the data must be deleted.

2.2 Values in Data Protection

The FCC Group is a constantly evolving organization committed to the use of the latest information systems and technological advancements. As a result, information can, in practice, be stored and processed in large volumes and within short periods of time.

For this reason, the FCC Group is continuously concerned with the confidentiality, security, and proper use of the information it manages in its daily processes and, in particular, with the Personal Data of its Employees, Customers, and Suppliers, to which it pays special attention.

Accordingly, in the processing of Personal Data, the FCC Group bases such processing on the following values:

- Transparency and trust regarding the secure processing of Personal Data at all times.
- Responsibility and commitment in the use of Personal Data, primarily based on their confidentiality.
- Efficiency in the secure management of the Personal Data processed within the FCC Group.
- Availability of Personal Data when needed and only by those individuals who require access due to their functions.
- Integrity of the information to prevent unauthorized alterations.

2.3 General Principles in the Management of Personal Data

Each FCC Entity shall manage Personal Data in accordance with the following principles:

2.3.1 Principle of Consent

Personal Data may only be processed by the FCC Entity or disclosed to another body if the data subject has previously given their consent. Notwithstanding the above, the processing or disclosure of Personal Data without the data subject's consent shall be permitted when authorized by national law or when necessary for the management and maintenance of a contract.

2.3.2 Principle of Information to the Data Subject

Prior to any collection of Personal Data, the FCC Entity must duly inform the data subject, at a minimum, of its identifying details, the purposes of the collection and processing, the recipients of the data if they are to be disclosed to persons other than the data subject, and the possibility of exercising the rights of access, rectification, erasure, and objection regarding their Personal Data.

2.3.3 Principle of Proportionality

Personal Data managed by the FCC Entity may only be collected and processed for specific and explicit purposes and must be adequate, relevant, and not excessive in relation to the purpose for which they were collected.

2.3.4 Principle of Quality

Personal Data managed by the FCC Entity must reflect reality and remain up to date at all times. Personal Data shall be cancelled once the purpose for which they were collected has been fulfilled.

2.3.5 Principle of Security

The FCC Entity must ensure the confidentiality of Personal Data, guarantee that access is restricted to authorized personnel only and ensure their security by implementing the necessary technical and organizational measures according to the type of Personal Data processed, preventing unauthorized access, destruction, and/or loss.

2.3.6 Principle of Legality

In all cases, and in addition to the above, Personal Data managed by the FCC Entity must be used lawfully and in accordance with the purpose for which they were collected, in compliance with the legislation of each State/Country/Region and respecting the rights and freedoms of the Data Subjects.

2.4 Processing Guidelines

2.4.1 Organization and Responsibilities in Privacy Matters

In matters of Privacy, the FCC Group has established an organizational structure with defined roles and responsibilities:

2.4.1.1 Organizational Structure

- The Information Security (SI) Department: The highest authority in the management and coordination of Privacy across the entire FCC Group.
- Data Protection Coordinator: The highest authority in the management and coordination of Privacy within their Area of responsibility.
- For the purposes of this document, the following are considered Areas: FCC Corporación, FCC Construcción, FCC Versia, FCC Environmental Services, FCC Industrial Waste Services, FCC Water Services, FCC Energy, and Cementos Portland Valderrivas Group.
- Entity Security Officer: The highest authority in management and coordination of Privacy within the specific FCC Entity.

If deemed appropriate, the SI Department may create and/or modify the roles described above in matters of Privacy.

2.4.1.2 Roles and responsibilities

The roles and responsibilities for each position are, at a minimum, the following:

- IS Department:
    - Define the general guidelines that must be observed and comply with regarding Privacy within FCC.
    - Manage, implement measures, and coordinate Privacy across the FCC Group.
    - Support the other roles in implementing the necessary actions and measures related to Privacy.

- Data Protection Coordinator:
    - Manage, implement necessary measures, and coordinate Privacy within the Area they oversee.
    - Support the SI Department and the Security Officers of the Entities within their Area in fulfilling the required Privacy-related actions.
    - Periodically report to the SI Department on the actions and measures implemented in their Area and in the FCC Entities within it.
    - Immediately report to the SI Department any Privacy-related incident, as well as any communication or request for information received from the Data Protection Authority.

- Security Officer:
  - Manage, implement necessary measures, and coordinate Privacy within the FCC Entity for which they are responsible.
  - Support the SI Department, the Data Protection Coordinator of their Area, and the Security Officers of other Entities within the same Area in fulfilling the required Privacy-related actions.
  - Periodically report to the Data Protection Coordinator of their Area on the actions and measures implemented in their Entity.
  - Immediately report to the SI Department any Privacy-related incident, as well as any communication or request for information received from the Data Protection Authority.

2.4.2 Processing of Sensitive Data

FCC Entities are prohibited from processing Personal Data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, or data relating to sexuality.

In any case, for the processing of health data or trade union membership data, the FCC Entity must obtain the data subject's explicit, prior, and written consent, except in cases where the legislation of the State in which the FCC Group Entity is located establishes that the prohibition in the first paragraph cannot be lifted even with the data subject's consent.

2.4.3 Service Provision Contracts

If it becomes necessary to contract certain Services from an external Entity or another FCC Group Entity (hereinafter, Data Processor) that may or must access Personal Data, the FCC Entity must:

- Select a Data Processor that has implemented the necessary security measures appropriate to the type of data to be processed.
- Sign, prior to any access/processing of data, a Service Provision Contract expressly stating that the Data Processor shall act only under the instructions of the FCC Entity, shall not apply or use the data for purposes other than those established in the contract, and shall not disclose them—even for storage—to third parties.
- For drafting the Service Provision Contract, the Legal Department of each FCC Entity must use as a basis the model contract provided by the Data Protection Coordinator of the Area to which the Entity belongs and must adapt it to the obligations and requirements of national legislation. Any Service Provision Contract signed with a Data Processor must be immediately communicated to the Data Protection Coordinator of the corresponding Area.

2.4.4 International Data Transfers

If an FCC Entity must transfer Personal Data to another FCC Entity and/or a Public/Private Organization located in a different country, the exporting FCC Entity must review and comply with the specific requirements of its national legislation, which may require obtaining prior approval and authorization from the Data Protection Authorities and regulators of the country in which the exporting Entity is located.

In this regard, any FCC Entity intending to transfer Personal Data to another country must notify the Data Protection Coordinator of its Area.

2.4.5 Rights of Access, Rectification, Erasure, and Objection

The FCC Entity must manage requests to exercise the Rights of Access, Rectification, Erasure, and Objection in compliance with the deadlines and procedures required by its applicable national legislation.

Unless national legislation specifies otherwise, responses must be provided in writing:

Within one month for Access requests.

Within 10 business days from receipt of the request for the remaining Rights.

2.4.6 Audits

FCC Entities must conduct periodic audits (internal or external) to verify compliance with this Standard and with the implemented security measures.

The SI Department will provide the necessary instructions prior to the audit, and the FCC Entity must report the results back to the SI Department.

2.4.7 Immediate Reporting of Data Protection Incidents

Any security incident related to Personal Data must be immediately reported by the FCC Entity to the FCC SI Department.

2.4.8 Compliance with Applicable Data Protection Legislation in Each State

This Standard applies directly to all Entities. If any Area or FCC Entity approves or has approved its own internal regulations on Personal Data protection, such regulations must not contradict this Standard, which shall prevail in all cases.

Furthermore, each FCC Entity must always comply with the requirements established by its national Data Protection legislation.

3. Responsibilities

The roles and responsibilities of the personnel referred to in this Standard are specified in section 2.4.1, Organization and Responsibilities in Privacy Matters, of this document.

4. Normative reference

This document has been reviewed by the IS Department, and its wording is based on the international standard ISO27001:2022 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
5.5	Contact with authorities	[op.exp.7] Incident Management
5.6	Contact with special interest groups	[org.1] Security Policy
5.19	Information security in supplier relationships	[op.ext.1] Contracting and Service Level Agreements
5.20	Addressing information security in supplier agreements	[op.ext.1] Contracting and Service Level Agreements
5.31	Identification of legal, regulatory and contractual requirements	[op.leg.1] Identification of Legal Requirements
5.34	Privacy and protection of personal data	[op.pdp.1] Personal Data Protection
5.35	Independent review of information security	Art. 31 / Annex III Security Audit
5.36	Compliance with information security policies, rules and standards	[org.4] Authorization Process; [op.exp.3] Configuration Management; [op.exp.4] Security Maintenance and Updates
6.8	Reporting information security events	[op.exp.7] Incident Management
8.34	Protection of information systems during audit testing	[op.exp.2] Security Configuration; [op.exp.3] Configuration Management; [op.exp.4] Security Maintenance and Updates; [mp.s.2] Protection of Web Services and Applications