FCC Group Domain Registration and Management Standard

January 2026

Document Version Control				
Version	**Date**	**Author**	**Detail**	**Approved by**
1.0	January 2026	IS	Document creation ISO/IEC 27001:2022 ENS	Chief Information Security Officer (CISO)

INDEX

1. Introduction

The present document is part of the FCC Group Information Security Regulatory Framework, which establishes the mandatory requirements within the Group regarding Information Security.

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

This standard shall be reviewed at least annually, unless circumstances arise that recommend or require a review before that date.

1.1 Purpose

The purpose of this standard is to establish the **criteria and guidelines for the registration, management, and ownership of internet domains related to the FCC Group.** Its aim is to ensure the proper protection of the FCC brand, safeguard the integrity and consistency of the corporate digital presence, and centralize the administration of domains within the FCC Group Information Systems and Technologies Division, as the unit responsible for their technical and operational management.

1.2 Scope

This standard applies to all internet domains (and associated subdomains) that meet any of the following conditions:

- **Refer to the business, activities, services, or products of the FCC Group**, regardless of the business unit, whether for internal purposes or for the end customer.
- Use, directly or indirectly, **the brand, corporate identity, or reputation of the FCC Group.**
- Point to or **are associated with IT services managed, maintained, or hosted by the FCC Group Information Systems and Technologies Division**.

1.3 Definitions

- **Internet domain**: A unique name that identifies a resource or service on the network (e.g., fcc.es).
- **Domain ownership**: Legal and administrative responsibility over the registration of a domain.
- **Domain management**: Set of activities related to the acquisition, renewal, technical configuration, and administration of a domain.
- **FCC Group IT services**: Platforms, applications, systems, or technological infrastructures managed by the Information Systems and Technologies Division.
- **FCC brand**: Any designation, logo, corporate identity, or registered element owned by the FCC Group.

2. Development

2.1 Principles

The management and registration of internet domains of the FCC Group shall be governed by the following fundamental principles:

- All domains related to the FCC Group must be registered and administered in a centralized manner through the FCC Group Information Systems and Technologies Division, ensuring control, traceability, and consistency in their use.
- The registration and use of domains must safeguard the integrity, reputation, and image of the FCC brand. The use of domains that may cause confusion, harm the brand, or generate reputational risks shall not be permitted.
- Domains must be managed in accordance with the FCC Group information security standards and policies, minimizing risks associated with attacks, impersonation, unauthorized access, or loss of ownership control.
- The process for requesting, approving, and managing domains must be documented and auditable. Every domain must have a clearly identified business owner and a defined purpose.
- The use and registration of domains must comply with applicable legislation (including intellectual property, data protection, and communications regulations), as well as the internal policies and standards of the FCC Group.
- An orderly, efficient, and sustainable use of the domain portfolio shall be promoted, avoiding duplications, unnecessary registrations, or domains without a clear purpose.
- When domains are required for temporary initiatives (campaigns, events, or specific projects), the assessment of their necessity, their impact on the brand, and their life cycle shall be the responsibility of the Internal and/or External Communications Department of the requesting business unit, which must ensure that the existence of the domain is proportional to the objective pursued. In the case of initiatives affecting the entire FCC Group, this assessment shall be carried out by the FCC Group Internal and/or External Communications Departments.
- Although ownership and technical management are centralized, each requesting area shall be responsible for the proper use of the domain, compliance with the applicable regulations, and the quality of the associated content.

2.2 Contacts Associated with Domain Registration

Every domain registered on behalf of the FCC Group must include in its registration record the mandatory contacts defined by the domain name management authorities (owner, administrative, technical, and billing contacts). These contacts must be configured in a standardized manner and comply with the requirements established by this standard.

2.2.1 Domain Owner Contact (Registrant)

The registrant contact is the legal entity that holds ownership of the domain and is therefore the ultimate legal responsible party for it.

Definition and function:

- Represents **the legal ownership of the domain** before the registrar and regulatory entities.
- Has the authority to authorize critical changes, such as transfers, DNS modifications, or updates to contacts.

Limitations and requirements:

- As a general rule, the registrant contact for the domains shall be the legal entity "**Fomento de Construcciones y Contratas, S.A.**", using the email address internet.domain@fcc.es as the contact address.
- Exceptionally, and only in cases where a specific local regulation or legislation of the country requires it, the registrant contact may be a natural person, who must be an employee of the FCC Group. In such cases, the preferred email address to be used shall be internet.domain@fcc.es. If this is not possible, the email address must in any case be a corporate FCC Group email address.
- Any other circumstance not covered in the preceding sections must be expressly approved by the Information Systems and Technologies Division, the Information Security Department, and the Legal area of the affected business unit or area.
- It may not be modified without prior approval from the Information Systems and Technologies Division, the Information Security Department, and the Legal area of the affected business unit or area.

2.2.2 Administrative Contact (Admin Contact)

The administrative contact acts as the functional owner of the domain and facilitates communications related to its use or contractual management.

Definition and function:

- Manages requests related to administrative or validation operations.
- Serves as the point of contact in case of disputes or external requirements.

Limitations and requirements:

- Must be **a natural person** belonging to the FCC Group.
- Must be identified with a **corporate FCC Group email address**.
- Exceptionally, and solely to facilitate administrative tasks, the use of the registrar agent's email address will be permitted, without this implying the delegation of the responsibility of the administrative contact, which will remain with the person designated by the FCC Group.
- Personal or generic email services (for example, @gmail.com, @hotmail.com or similar) may not be used; an email address associated with a corporate or institutional domain must be used.
- It cannot be delegated to external providers.
- The use of the registrar agent's privacy mode is permitted in order to protect the personal data of the natural person designated as the administrative contact.

2.2.3 Technical Contact (Tech Contact)

The technical contact manages the operational aspects of the domain, including DNS administration and technical configurations.

Definition and function:

- Responsible for communication with the registrar and hosting services regarding technical incidents.
- Manages changes in DNS configurations, activation of security features (DNSSEC), locks, etc.

Limitations and requirements:

- The technical contact for the domain shall generally be the registrar itself, in its capacity as the entity responsible for the domain's technical aspects and DNS server management.
- The technical contact may be a legal entity (company or organization), in accordance with the usual definition of this role in domain registration systems.
- The email address associated with the technical contact must belong to a corporate domain of the registrar; the use of personal or generic email addresses (for example, @gmail.com, @hotmail.com or similar) is not permitted.
- In territorial or specific domains whose national regulations require the technical contact to be a natural person (for example, certain .es domains), the technical contact designated by the registrar must meet this requirement, ensuring in all cases compliance with applicable local laws and regulations. In other words, in these cases, the designation shall be carried out in accordance with the requirements established by the corresponding registry authority.

2.2.4 Billing Contact

The billing contact is responsible for the economic management of the domain, including payments, renewals, and invoices.

Definition and function:

- Receives and processes invoices, renewal reminders, and related financial documentation.
- Acts as the point of contact for providers regarding billing matters.

Limitations and requirements:

- The billing contact for the domain shall generally be the registrar itself, in its capacity as the entity responsible for invoicing and for the financial and contractual management associated with the domain.
- The email address associated with the billing contact must belong to a corporate domain of the registrar; personal or generic email addresses are not permitted.

2.3 Procedure for Domain Request, Registration, and DNS Changes

Formal request

- The requesting area must submit a request to the FCC Group Information Systems and Technologies Division through the Service Now catalog item created for this purpose.
- The request must include: purpose, proposed domain name, business owner, associated service, affected environment (development/pre-production or production), and estimated usage dates. This last item is mandatory for domains affecting development or pre-production environments.

Technical and brand evaluation

- The Information Systems and Technologies Division, through its Communications department, will review technical feasibility, domain availability, and compliance with the scope of this standard.
- Communications/Brand will validate proper use of the name and its consistency with the corporate identity, where applicable.

Approval

- The FCC Group Information Security Department will assess the security risks associated with the request and issue the final approval, proceeding with the domain registration when applicable.

Ownership and management

- All approved domains will be registered under the name of the FCC Group and managed exclusively by the FCC Group Information Systems and Technologies Division.
- The registration of domains linked to FCC by business units or third parties will not be permitted, unless expressly and formally authorized.

Configuration and deployment

- The FCC Group Information Systems and Technologies Division will perform the necessary technical configurations (domain creation in the registrar, DNS record changes, etc.).
- The requesting area will be responsible for the content and use of the domain, in accordance with internal policies.

2.4 Request for Changes to DNS Records

- Any request for the creation, modification, or deletion of DNS records associated with an FCC Group domain must be submitted exclusively through a formal request or change in the corporate ServiceNow platform, thereby ensuring traceability, historical logging, and proper process control.
- Any request received through unauthorized channels will be automatically rejected.
- DNS records whose purpose is to allow validation, verification, or integration of the domain with external services must first have the express and documented approval of the FCC Group Information Security Department. Such services include (but are not limited to):
    - Mailing services or mass-emailing platforms.
    - SaaS tools or external cloud services.
    - Technological tenants other than the corporate ones.
    - Authentication, verification, or domain-certification platforms.
    - Any third-party service that requires TXT, CNAME, or other records to prove ownership or enable functionalities.

The creation of these types of records will not be authorized without such approval, regardless of the requesting area or the purpose of the external service.

2.5 Renewal, Maintenance, and Decommissioning of Domains

- The FCC Group Information Systems and Technologies Division will be responsible for the annual renewal and lifecycle monitoring of each domain.
- If a domain is no longer required, the owning area must notify the FCC Group Information Systems and Technologies Division sufficiently in advance to manage its decommissioning or redirection.
- Domains linked to critical services may not be decommissioned without a prior impact assessment.

2.6 Defensive Domain Registration (Reserve Domains)

In order to protect the digital identity and corporate reputation of the FCC Group, domains that, while not intended for active use, **resemble, may cause confusion with, or could be used by third parties for illicit, fraudulent, or impersonation activities may be centrally registered.**

The decision to proceed with the registration of this type of domain shall be made at the request of the Internal and/or External Communications Department of the associated business unit, based on brand- and reputation-protection criteria.

The need for such registration may be raised by the business unit itself or may arise from a recommendation by the registrar or the Information Systems and Technologies Division.

This defensive registration shall be carried out under the following criteria:

1. **Objective of the Defensive Registration**

   Prevent third parties from acquiring domains that:

   - Include orthographic, phonetic, or abbreviated variations of the name “FCC”.
   - Use names of projects, trademarks, business areas, or subsidiaries of the FCC Group.
   - Pose a risk of phishing, fraud, typosquatting, or cybersquatting.

2. **Conditions of Use**

   Domains registered for defensive purposes:

   - Will not have active DNS resolution, nor contain any type of records (A, AAAA, MX, CNAME, TXT, or others).
   - Will not be used to host services, websites, email, or any operational function.
   - Will remain in an “inactive” state within the corporate inventory.

3. **Management and Documentation**

   - They will be administered exclusively by the Information Systems and Technologies Division.
   - They will be explicitly documented as a “reserve domain” in the inventory.
   - The need to maintain, renew, or decommission them will be reviewed periodically.

2.7 Cleanliness, Order, and Permitted Use of DNS Records

In order to ensure the security, efficiency, and proper administration of the FCC Group's domains, it is established that **all DNS records associated with corporate domains must correspond to a real and verified operational need.**

2.7.1 Prohibition of Unused DNS Records

No FCC Group domain may retain **DNS records that are not in use** or that do not serve an active technical function. This prohibition applies to **all types of records**, including but not limited to:

- A
- AAAA
- CNAME
- MX
- TXT
- SRV
- NS (except those defined for the domain and its correct delegations)
- ANY other existing or future record type defined by DNS standards.

2.7.2 Effective Use Criterion

A DNS record shall be considered **not usable or not permitted** when:

- It does not point to an active or configured service, except in the cases described in subsection "2.6 Defensive Domain Registration (Reserve Domains)".
- It was created for temporary testing purposes and is no longer needed.
- It has become obsolete after a migration or infrastructure change.
- It is duplicated, redundant, or has no identified purpose.
- It was created by third parties without authorization or is not documented.

2.7.3 Principle of Order and Cleanliness

For all FCC Group domains, it must be ensured that:

- **There are no orphaned, incorrect, or expired records**.
- Any inactive or unauthorized record is **removed immediately**.
- DNS records in force are fully **documented and traceable.**
- **Naming consistency** is maintained, avoiding incoherent or confusing entries.
- **Periodic reviews** are carried out to verify that all records serve their intended function.

2.8 Security and Compliance

- All domains must comply with the FCC Group's information security, cybersecurity, and digital asset protection policies.
- Web services associated with the domains included in this standard must be exposed through the FCC Group's corporate WAF, which will apply the security controls inherent to this platform. These controls include, by way of guidance and not limitation:
    - Inspection and filtering of HTTP/HTTPS traffic.
    - Protection against injection attacks (SQLi, XSS, Command Injection, etc.).
    - Mitigation of denial-of-service attacks (DoS/DDoS).
    - Detection and blocking of anomalous traffic patterns or malicious behaviour.
    - Application of security rules based on OWASP and other recognized standards.
- The WAF may restrict access to web services by filtering source IP address ranges when required for security, compliance, confidentiality, or operational restriction purposes.
- As with web services, if an FCC Group domain uses email services, all DNS records associated with the sending and receiving of email must be configured to point to the FCC Group's corporate email security services and tools. The use of email services provided by third parties is not permitted unless expressly and formally approved by the FCC Group Information Security Department.
- In the event of a security incident, the FCC Group Information Security Department shall be empowered to request any measures it deems appropriate from the Information Systems and Technologies Division regarding DNS services, including the temporary or permanent unpublishing of sites, domains, or associated services, in order to contain the incident, protect corporate assets, and prevent greater impact, without prior notice.
- Any non-compliance may result in the suspension or removal of the domain.

3. Responsibilities

In order to ensure effective, secure, and consistent management of the FCC Group's internet domains, specific responsibilities are defined for the different areas involved in their request, approval, administration, and use. The proper allocation of these responsibilities ensures process traceability, protection of the corporate brand, and compliance with applicable internal policies and legal requirements.

The FCC Group Information Systems and Technologies Division – Communications Department shall:

- Register and maintain ownership of the domains within the scope.
- Technically manage the domains (DNS, security, renewals, coordination with the registrar, etc.).
- Maintain an up-to-date inventory of all managed domains.

The FCC Group Information Security Department shall:

- Evaluate and approve requests for new domains related to the FCC Group.
- Evaluate and approve requests for the creation or modification of DNS records.

The following tasks shall be the responsibility of the business units and associated departments.

- Local Internal and/or External Communications Department:
- Request new domains through the established procedure.
- Justify the purpose and necessity of the domain.
- Ensure that the use of the domain complies with corporate, legal, and brand policies.
- Request the decommissioning of domains that are no longer required, either due to functional reasons or the release of defensive domains.

Local IT Department:

- Coordinate with the FCC Group Information Systems and Technologies Division when the domain is linked to internal or external IT services.
- Request the creation or modification of DNS records.
- Request the removal of DNS records that are no longer in use.

4. Normative Reference

This document has been reviewed by the IS Department, and its drafting is based on the international standard ISO 27001:2022 and 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
5.4	Management responsibilities	[org.1] Security policy; Art. 13. Organization and implementation of the security process
5.9	Information inventory in project management	[op.exp.1] Asset inventory; [op.pl.2] Security architecture
5.10	Acceptable use of information and other associated assets	[org.2] Security regulations; [org.3] Security procedures; [mp.si.3] Custody
5.15	Access control	[op.acc.2] Access requirements
5.18	Access rights	[op.acc.4] Access rights management process
5.19	Information security in supplier relationships	[op.ext.1] Contracting and service level agreements
5.23	Information security for cloud service use	[op.nub.1] Cloud Services Protection
5.31	Identification of legal, regulatory, and contractual requirements	[org.1] Security policy; [mp.info.3] Electronic signature
5.36	Compliance with information security policies and standards	Art. 31 Security Audit; Annex III Security Audit; [org.4] Authorization Process; [op.exp.3] Security configuration management; [op.exp.4] Security maintenance and update
8.32	Change management	[op.exp.5] Change Management