FCC Group Information Security Monitoring 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

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 document is to detail the main aspects related to the definition, activation, retention, safeguarding, review, recording, and access to activity records (hereinafter logs) generated by FCC Group systems, with the aim of monitoring the use of information systems and the information stored within them.

1.2 Scope

This Standard applies to any log obtained from the monitoring of FCC Group systems, regardless of the tool used or the asset or resource affected. This Standard also applies to all internal personnel, external collaborators, and information systems involved in the monitoring and management of the logs described above. General Overview

2. Development

2.1 Principles

All FCC Group systems and applications must have security auditing enabled and generate event logs. These events shall be stored within the systems for subsequent analysis when an investigation is required, in accordance with the configured retention settings. Logs from systems that process sensitive data shall be sent in (pseudo) real time to the corporate log management platform, the SIEM (Security Information and Event Management).

2.2 Activation and Deactivation of Log Records

All information systems shall be synchronized with the same time source to enable the construction of an event timeline and proper event correlation. Events that must be recorded in information systems shall include at least the following information:

- Name of the system where the event was generated.
- Timestamp of the event, including date and time
- Event identifier, according to the technology used.
- Identification of the user who triggered the event.
- Identity or name of the data, system components, or resources affected.
- Result of the action performed.

Events that must be identified and recorded in all information systems include:

- Access or attempted access to systems and the information contained within them.
- All actions performed by user accounts with elevated privileges.
- Use and modification of identification and authentication mechanisms, including logon, creation and deletion of user accounts, and privilege escalation
- Modifications to security auditing: initialization, stopping, or deletion of logs.
- Creation and deletion of system-level objects such as database tables or stored procedures

Any new provisioning of on-premise or cloud-style systems must comply from the outset with the auditing and monitoring requirements established in this Standard. The Information Security Department shall coordinate with the Information Technology and Telecommunications departments to ensure the correct ingestion of logs into the security monitoring platform.

In the event of decommissioning information systems, the Information Technology and Telecommunications departments shall notify the Information Security Department of the asset's removal so that the security monitoring platform can be reconfigured accordingly.

Use cases shall be defined in the SIEM platform for generating real-time alerts or reports. The programmed logic in these use cases will serve to detect suspicious or malicious activity, which may indicate some type of attack or unauthorized access to systems and/or the information contained within them.

2.3 Retention and Unauthorised Access

To enable digital forensic analysis, log retention configured in the systems shall be at least 12 months and may be configured either within the information systems themselves or within the SIEM if collected through that platform.

Logs shall be protected to prevent any type of modification or unauthorized access. Protection of these files shall be managed through a monitoring process that performs file integrity monitoring. This process will verify that operating system programs and files have not been compromised.

3. Responsibilities

The Information Security Department shall:

- Verify that no conflicts arise between the rules established for log recording. When notified of alerts or suspicious activities occurring in information systems or the network environment, the party responsible shall take the appropriate measures to prevent any incident.
- Ensure that log generation and collection are conducted without issues and restore them as soon as possible in the event of any incident.

The IT Department shall:

- Enable auditing on all information systems where activity logging is required, in accordance with the guidelines of the Information Security Department.
- Inform the Information Security Department of the decommissioning of any information system.

Users shall:

- Immediately notify technical managers, the Information Security Department, or the user support service (Global ServiceDesk) of any suspicion of a security incident.
- Maintain a vigilant attitude to identify any potential security incident.

4. Normative reference

This document has been reviewed by the Information Security Department, and its drafting is based on the international standard ISO 27001:2022.

4.1 Regulatory controls ISO27001:2022 and ENS

ID Control ISO	ISO/IEC 27001:2022 control	ENS Correspondence
5.25	Evaluation and decision on information security events	[op.exp.7] Incident Management
5.33	Protection of records	[op.exp.8] Activity logging; [op.mon.3] Monitoring
6.8	Reporting information security events	[op.exp.7] Incident Management
8.15	Event logging	[op.exp.8] Activity logging