FCC Group Incident Management Standard

January 2026

Document Version Control				
Version	**Date**	**Author**	**Detail**	**Approved by**
1.0	April 2009	IS	Document creation	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

This Standard establishes the necessary criteria for conducting actions aimed at resolving any security incident in a rapid and effective manner, reducing, or eliminating the potential or actual impact that such an incident could have on the business of the FCC Group.

1.2 Scope

This Standard applies to any security incident, whether materialized or attempted, that occurs in the FCC Group’s systems or facilities, regardless of where they are located and of the resources or information affected.

This Standard also applies to all internal personnel, collaborators, and information systems involved in the security incident.

2. Security in Incident Management

2.1 Principles

Incident Management must not be confused with Incident or Problem Management, since, unlike the latter, it does not focus on identifying and analyzing the underlying causes of a specific hardware or software issue. In the context of this document, the objective is exclusively to define the restoration of information technology service activity.

This Standard establishes the activities related to the detection, assessment, and resolution of an information security incident, while the processes governing the recovery of activity after such incidents will be developed in the corresponding documents that FCC may issue.

- The management of an information security incident must encompass all phases of its lifecycle, from the moment there is suspicion or awareness of its existence, through its resolution, recording, and the implementation of corrective actions derived from the analysis of its causes.
- In the event of suspicion that an incident may be occurring, it shall be treated as confirmed until it is verified otherwise.
- When there is no reasonable assessment of the potential impact of an incident, the worst-case scenario shall be assumed until a more detailed analysis is conducted.
- Priority-setting when concurrent incidents occur shall be based on their seriousness or criticality for the FCC business or for the user.
- When the type of incident is not included in the corresponding service level agreement, the priority of action shall be evaluated as objectively as possible based on the impact or on the urgency or acceptable delay in the operation of the business process.
- Participation in the different stages that make up the resolution cycle of Incident Management and Response Plans shall depend on the responsibilities assigned according to the roles and duties defined for this purpose.
- FCC personnel must be familiar with the procedures related to Incident Management for each of the security areas for which they hold responsibility, to ensure the most effective incident management possible.
- The classification level of FCC Information will determine the extent of the security measures required to prevent, detect and correct incidents affecting the security of such information.
- There is a Procedure for the Management and Notification of Personal Data Breaches for security incidents that affect personal data pertaining to any of the companies that make up the FCC Group. This Procedure governs the notification, management, and response to incidents that may impact the security of personal data processed under the responsibility of those companies.
- Any incident involving a loss of confidentiality of FCC Information handled by companies external to the Group must be reported as quickly as possible to the IS department, in accordance with the External Companies Standard.

When technically feasible, the following shall be ensured:

- Systems and applications shall be configured to automatically detect and notify incidents and/or alerts.
- Systems shall be monitored, scanned, and behavioral patterns established to enable the early detection of any anomaly in the behavior of information systems.
- A record of system and application file signatures shall be maintained to allow rapid verification of their integrity.

Figure 1: Incident Management Principles

2.2 Prior Preparation for Incidents

FCC's ability to respond to security incidents will depend largely on its capacity to prevent them, on the preparation of response actions, and on the agility with which these actions are executed at the moment the incident occurs.

In addition to establishing security controls over the Group's systems, networks, and applications, it is necessary to consider all training, logistical, and technical actions that facilitate a rapid, effective, and efficient response to any security incidents that may occur.

Experience, organization, and knowledge of information technology services and the threats they face are key to Incident Management that minimizes impacts on business processes. For this reason, the FCC information security department and other departments involved in this management must have defined:

- The development of a typology of possible incidents for each specific system and the acceptable risks in each scenario.
- The development of an Incident Response Plan for each defined scenario.
- The definition of combinations of indicators or precursors that generate the necessary signals to conclude that an incident may be materializing.
- The assignment of functions and tasks for each type of anticipated incident.
- Technical and legal training, specifically on the implications and potential violations of privacy rights that may arise from tasks associated with incident resolution.
- The allocation of the availability of technical and professional resources assigned to incident resolution.

2.3 Detection and Logging of Incidents

- Any information security incident for which there is suspicion, doubt, or knowledge of its existence must be reported with sufficient detail and urgency.
- The IS department shall be responsible for convening the members of the Incident Management Team who will participate, as a whole or in part, in the management activities.
- The Incident Management Team shall consist of a member of the IS department, the person(s) responsible for the information affected by the incident, and the DPO in cases where personal data is involved.
- The existence of a security incident within the information systems may be detected and reported by internal personnel or collaborators of the FCC Group.
- Internal personnel or collaborators of the FCC Group who suspect or identify a possible incident shall not perform any action other than immediately reporting the incident to the technical managers, the IS department, or the user support service (Global ServiceDesk), upon any suspicion of a security incident.
- The individuals responsible for Incident Management, as the FCC Group's point of contact regarding information security incidents, must be available and able to provide appropriate and timely responses.
- Once identified as such, all information security incidents must be logged and classified by the IS department. The classification of an incident is determined based on the severity or potential impact resulting from the preliminary analysis performed.
- Maintaining this log is essential for analyzing potential attacks on the FCC Group's systems and information assets, as well as for identifying those responsible for them.
- The procedures developed under this Standard must establish the minimum content of the information that must be recorded for each incident.
- When incidents affect the security of personal data owned by FCC, the Procedure for the Management and Notification of Personal Data Breaches must be followed.

2.4 Identification and Analysis of Incidents

- Registered incidents must be identified and assessed to determine their impact on the normal operation of business processes.
- To evaluate this impact, the criticality of the affected assets and business processes shall be used as a reference, based on the expected downtime and associated costs.
- When the information reported about the incident is insufficient to carry out its assessment and classification, the IS department or, failing that, the Information Owners may undertake any actions they deem appropriate to expand the available information on the incident.
- Incident management shall begin with a rapid analysis of the situation to determine the scope of the incident, its causes, and the scenario in which it is unfolding.
- As a preliminary step before applying containment, response, or recovery measures that must be adopted in the event of a security incident, it must be determined whether a similar previously resolved incident can be identified in order to apply analogous measures.
- Incidents occurring at the same time shall be prioritized according to their severity. The criterion for establishing this prioritization shall be the previously indicated criticality level of the information for business processes.
- Once the priority of a security incident has been assessed, the management procedures related to the specific incident shall be initiated, and all the steps taken shall be properly documented.
- Once analyzed and prioritized, the incident must be notified to the relevant FCC functions or personnel, as well as to external companies and/or third parties concerned.
- Whenever technologically feasible, logs and documentation related to incident management shall follow a common and uniform format, with consolidated entries and a single retention policy, so that they may be accepted by any national legal entity or other disciplinary bodies.

2.5 Incident Containment

- Once the incident has been identified, the Incident Management Team must decide whether to proceed with containing the incident in order to prevent its impact from increasing.
- To do so, where applicable, the team must assess how to ensure the validity of the chain of custody of the evidence for its possible later submission for legal or disciplinary purposes, as well as the implications this may have in terms of risk.
- Activation of the Incident Response Plan shall involve implementing a containment strategy for each specific incident.
- Incident Response procedures must ensure segregation of duties and dual control, in order to reinforce the integrity of the evidence obtained.

2.6 Incident Resolution and Recovery

After resolving an incident, the person responsible for its management must ensure:

- That all affected systems have been properly sanitized.
- That the likelihood of a future incident of similar characteristics has been minimized.
- Those security controls have been reviewed in order to assess whether they need to be corrected, expanded, or supplemented with new controls.
- That the incident has been recorded along with its analysis, assessment, and specific containment strategy.

During recovery, actions shall be guided by the operational procedures approved by the Information Technology Services managers.

2.7 Incident Closure

- Once systems have returned to normal operation, the Incident Management Team shall notify all interested parties, as well as the functions and departments involved in the incident.
- Incident closure shall include verifying that the information gathered is sufficient to properly understand its progress, the effectiveness of the measures adopted, and the time required for its resolution.
- It must be ensured that the origin of the incident is unequivocally identified and that controls mitigating the threat that caused the incident are incorporated or updated.
- During the incident closure process, the original classification of the incident shall be reviewed and updated if it is determined that the characteristics of the incident do not match the initial classification.
- After closing an incident, it is advisable to conduct an evaluation of incident management with the aim of assessing the completeness and maturity of the current process and producing a list of lessons learned to help improve the existing incident management model.
- After the formal closure of the incident, knowledge transfer obtained during incident management shall be promoted to train FCC Group employees and collaborators in case similar situations arise in the future.

2.8 Incident Monitoring

- Information obtained from information security incidents shall be documented to identify those that are recurrent or of high impact. Its analysis may result in the need to improve or introduce controls that limit the frequency and damage of future cases.
- Given the rapid technological evolution of information systems, the Incident Management Team must hold periodic meetings to discuss new threat scenarios.
- This team shall meet after significant incidents have occurred, or when new attack techniques emerge, in order to analyze them and identify improvements to the existing information security measures.
- Information obtained from these meetings shall support enhancements to incident management processes, information security policies and procedures, and the content of information security training programs, both for users and technical personnel.

3. Responsibilities

The IS Department shall:

- Identify any security incident during the monitoring activities carried out on the critical systems under its supervision.
- Periodically review audit logs in search of evidence or indications of suspicious behavior.
- Oversee the resolution of information security incidents, as well as the implementation of any corrective or preventive measures that may be adopted.
- Submit status reports on incident resolution to the Senior Management of the FCC Group.
- Maintain relationships with all organizations and legal representatives that may cooperate in resolving security incidents. Develop and update the Incident Response Plans.
- Promote sufficient training and coaching for FCC technical personnel in Incident Management so that incidents can be identified and reported as effectively as possible.
- Carry out tests to verify Incident Management procedures and Response Plans and identify any shortcomings within them.

The Information Security Incident Management Team shall be responsible for:

- Coordinating the interested parties during incident management.
- Periodically informing stakeholders of the status of incident resolution, as well as the damage and impact caused.
- Effectively managing the professional and material resources assigned for incident resolution.
- Making decisions that lead to the resolution of the incident in accordance with the service levels in place prior to its occurrence.
- Classifying, or if necessary, reclassifying the incident according to the established incident classification criteria.
- Coordinating activation of the Continuity Plan when necessary.

The Information Owners shall:

- Ensure that all personnel who access information under their responsibility have received the necessary training to recognize and respond to any security incident.
- Ensure that roles and responsibilities related to managing incidents affecting the information assets under their responsibility have been assigned, communicated, and understood.
- Cooperate with those responsible for Incident Management in resolving incidents and provide any information that may be required.

The users shall:

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

Depending on the type of incident, collaboration from other areas or departments—such as Legal, Human Resources, Marketing, etc.—may also be required.

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
5.24	Planning and Preparation for Information Security Incident Management	[op.exp.7] Incident Management
5.25	Assessment and Decision on Information Security Events	[op.exp.7] Incident Management
5.26	Response to Information Security Incidents	[op.exp.9] Incident Management Logging
5.27	Learning from Information Security Incidents	[op.exp.7] Incident Management; [op.exp.9] Incident Management Logging
5.28	Evidence Collection	[op.exp.7] Incident Management; [op.exp.9] Incident Management Logging
5.29	Information Security During Disruption	[op.cont.1] Impact Analysis; [op.cont.2] Continuity Plan
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