



FCC Group Vulnerability Management Standard

July 2026

ID	VULNERABILITY MANAGEMENT STANDARD	CLASSIFICATION	VERSION	DATE
IS_ST_23		FCC_INTERNAL	1.0	July 2026

Document Version Control				
Version	Date	Author	Detail	Approved by
1.0	July 2026	IS	Document creation	Chief Information Security Officer (CISO)

ID	VULNERABILITY MANAGEMENT STANDARD	CLASSIFICATION	VERSION	DATE
IS_ST_23		FCC_INTERNAL	1.0	July 2026

INDEX

1. Introduction 4

1.1 Purpose.....4
1.2 Scope.....4

2. Development.....5

2.1 Principles 5
2.2 Asset Identification and Scope 6
2.3 Asset Scanning 7
2.4 Classification 8
2.5 Reporting 9
2.6 Remediation 10

2.6.1 Patching.....10
2.6.2 Exceptions 11

2.7 Reassessment 11

3. Responsibilities 12

4. Normative reference.....14

4.1 Regulatory controls ISO27001:2022 and ENS.....14

ID	VULNERABILITY MANAGEMENT STANDARD	CLASSIFICATION	VERSION	DATE
IS_ST_23		FCC_INTERNAL	1.0	July 2026

1. Introduction

The FCC Group has an extensive technological infrastructure, as well as a large number of Information Systems. These systems are interconnected and, in some cases, are also connected to third-party Information Systems. They may be accessible from both public and private networks. Information assets may contain weaknesses that can be exploited by malicious actors with the aim of compromising the security of the Organisation's data and information.

The FCC Group's cybersecurity culture is based on the principle of prudence and acknowledges that zero risk does not exist when dealing with threats to information security. For this reason, it is essential for the FCC Group to have a policy and an established process for managing weaknesses or vulnerabilities affecting the organisation's information assets.

This Vulnerability Management Standard has been developed in response to the need to internally regulate the objectives, activities and responsibilities of personnel and systems involved in information security within the Group, regarding the detection, treatment and remediation of technical vulnerabilities present in the FCC Group's Networks, Infrastructure and Information Systems.

This Standard forms part of the FCC Group Information Security regulatory framework and provides guidance to the teams involved in the identification, monitoring and remediation of technical vulnerabilities.

1.1 Purpose

The purpose of this Standard is to establish the cybersecurity criteria that must be met in vulnerability management processes in order to ensure the confidentiality, integrity, authenticity, traceability and availability of information assets (whether owned by FCC Group or by third parties), as well as compliance with the applicable regulatory requirements in force.

1.2 Scope

This Standard applies to all companies in which the Group holds a majority shareholding, as well as to those companies or entities for which the Group is responsible for their operation and/or management.

It applies to any information, network or infrastructure asset that is related to or has any connection with the FCC Group, whether owned by the Group itself or by a third party providing services to the Group.

ID	VULNERABILITY MANAGEMENT STANDARD	CLASSIFICATION	VERSION	DATE
IS_ST_23		FCC_INTERNAL	1.0	July 2026

2. Development

2.1 Principles

Vulnerability management within the FCC Group is based on the following principles:

- Vulnerability management is a continuous process.
- A technical vulnerability is understood to be a weakness in an asset or the absence of a control that may be used by an attacker to damage or gain control over that asset.
- Technical and organisational measures shall be established to identify vulnerabilities affecting information, network and infrastructure assets that support FCC Group business activities.
- Vulnerabilities shall be classified and their remediation prioritised according to their criticality or risk level.
- All vulnerabilities shall be recorded, and the entire management process shall be documented until resolution, either through the implementation of corrective actions that mitigate the risk or through the formal acceptance of the risk where this is the approved option.
- Identified vulnerabilities shall be managed according to their level of criticality and risk to the FCC Group. Appropriate corrective or mitigating actions and the corresponding remediation timeframes shall be defined in each case. Exceptionally, where deemed appropriate following analysis and assessment, the associated risk may be formally accepted by the FCC Group Information Security Department in accordance with the established procedure (see section [2.6.2 Exceptions](#)).
- The identification of a technical vulnerability shall be communicated to the relevant stakeholders, and periodic updates on its remediation status shall be provided.
- Where required by applicable legislation, the existence of critical vulnerabilities shall be reported, and any information necessary to comply with the relevant regulatory requirements shall be provided.
- Periodic assessments of Systems, Networks and Technological Infrastructures shall be carried out to identify vulnerabilities, in accordance with vendor patching cycles and with a frequency determined by the criticality of each asset.
- Information Systems shall be assessed for technical vulnerabilities prior to being placed into production.
- Information Systems shall be assessed for technical vulnerabilities prior to the implementation of significant changes in production environments.
- Even where the infrastructure is not owned by FCC Group entities, if it contains information owned by, or under the responsibility of, the Group, or if it may affect the Group's Networks and/or Information Systems, periodic vulnerability assessments shall be ensured.
- Assessments shall be performed either using updated automated tools or through manual analysis.
- Assessments shall be formally conducted and properly documented.

ID	VULNERABILITY MANAGEMENT STANDARD	CLASSIFICATION	VERSION	DATE
IS_ST_23		FCC_INTERNAL	1.0	July 2026

- Assessment results shall be communicated to the relevant parties and/or stakeholders, including any public or private authorities where required by applicable legislation.
- Prior to implementing a corrective action, testing shall be performed to ensure that such action does not adversely affect any System and does not compromise the security controls in place.
- All systems shall operate on the latest stable version available in order to minimise exposure to high and critical vulnerabilities reported by vendors.

2.2 Asset Identification and Scope

The identification of FCC Group assets and the definition of the scope of vulnerability assessments shall comply with the following principles:

- Vulnerability management shall cover all servers, desktops and infrastructure owned by or managed on behalf of the FCC Group, including assets managed by third parties.
- All servers and equipment within the scope of this Standard shall be included in a Configuration Management Database (CMDB), which shall be reviewed at least monthly.
- All servers and equipment shall be added to the CMDB referred to above prior to being placed into production or delivered to the end user and shall be prepared for vulnerability scanning activities.
- Any application meeting one or more of the following criteria shall be subject to a vulnerability assessment:
 - Applications that process personal data.
 - Applications that process confidential or restricted information.
 - Applications classified as critical by the business lines.
 - Applications exposed to the Internet.
 - Applications that could have a significant reputational impact in the event of a security incident.

ID	VULNERABILITY MANAGEMENT STANDARD	CLASSIFICATION	VERSION	DATE
IS_ST_23		FCC_INTERNAL	1.0	July 2026

2.3 Asset Scanning

FCC Group vulnerability scanning activities shall comply with the following principles:

- Vulnerability scans of servers and end-user devices shall be performed automatically at a frequency aligned with applicable regulations and requirements, but no less frequently than once per month.
- A vulnerability assessment shall be carried out on any application that meets one or more of the following conditions:
 - A change has been made to the application's source code.
 - A change has been made to the application's configuration or to the infrastructure hosting the application.
 - A module, plugin or API has been added or removed.
 - The application has undergone a migration process.
 - The hardware hosting the application has been modified.
 - The existence of a vulnerability is suspected.
 - Applicable regulations require the assessment to be performed.
- Application scans shall be conducted upon request, and at least the following information shall be provided:
 - Application name.
 - Application owner.
 - Business line to which the application belongs.
 - Type of assessment to be performed: Dynamic Application Security Testing (DAST) or Static Application Security Testing (SAST).
 - For DAST assessments, the URLs, access details and any necessary instructions required to perform the assessment shall be provided.
 - For SAST assessments, the application's source code and the instructions required for its compilation shall be provided.
 - Credentials, where required.
 - Any other information considered necessary to perform the vulnerability assessment.
- Vulnerability scans of infrastructure belonging to the FCC Group shall be performed on demand.
- A start date shall be assigned to all vulnerability scans requested on demand.

ID	VULNERABILITY MANAGEMENT STANDARD	CLASSIFICATION	VERSION	DATE
IS_ST_23		FCC_INTERNAL	1.0	July 2026

2.4 Classification

The classification of vulnerabilities identified during FCC Group vulnerability scanning activities shall comply with the following principles:

- Vulnerabilities shall be classified taking into account factors such as:
 - The severity associated with the relevant CVE or CVSS score.
 - The likelihood of exploitation.
 - The exposure of the affected asset.
 - The criticality of the asset.
 - The potential business impact.
- Based on the assessment of the above criteria, vulnerabilities shall be classified from highest to lowest criticality according to the following categories:
 - Critical.
 - High.
 - Medium.
 - Low.
 - Informational.

ID	VULNERABILITY MANAGEMENT STANDARD	CLASSIFICATION	VERSION	DATE
IS_ST_23		FCC_INTERNAL	1.0	July 2026

2.5 Reporting

The reporting of vulnerabilities identified during FCC Group vulnerability scanning activities shall comply with the following principles:

- Critical vulnerabilities, zero-day vulnerabilities, or vulnerabilities for which there is evidence of active exploitation shall be communicated through an early warning notification to the owners of the affected asset and to the Information Security Department for assessment and priority management.
- Vulnerabilities identified during periodic and automated assessments shall be reported through a report format agreed with the Information Security Department and shall include, at a minimum, the following information:
 - Affected asset. The hostname of the affected asset shall be specified.
 - Vulnerability name and description.
 - CVSS score and vulnerability criticality.
 - Date of the most recent detection.
 - Vulnerability impact.
 - Vulnerability remediation guidance, including vendor recommendations where applicable.
- Following the completion of an on-demand vulnerability assessment, a technical report detailing the identified vulnerabilities shall be issued. Additionally, where the results must be presented to Management, Business personnel, or where the assessed asset is subject to a security certification audit, an executive report shall also be prepared.
 - Technical report, containing a detailed description of the identified vulnerabilities:
 - Vulnerability name.
 - CVSS score and criticality.
 - Potential impact in the event of exploitation.
 - Recommendations for remediation.
 - Comments regarding the vulnerability.
 - Current status of the vulnerability.
 - Executive report, containing:
 - Assessment scope.
 - Assessment description.
 - Application risk assessment.
 - Breakdown of vulnerabilities by criticality, type and status.

ID	VULNERABILITY MANAGEMENT STANDARD	CLASSIFICATION	VERSION	DATE
IS_ST_23		FCC_INTERNAL	1.0	July 2026

2.6 Remediation

2.6.1 Patching

The patching of vulnerabilities identified during FCC Group vulnerability scanning activities shall comply with the following principles:

- Action plans shall be established to remediate identified vulnerabilities.
- Action plans shall include the identified vulnerabilities, the remediation actions defined, the persons responsible for their implementation, and the planned remediation deadlines.
- The deployment of patches or application updates to devices shall always be carried out in waves.
- The first patching wave shall be deployed to a limited group of devices for testing purposes. Subsequent waves shall be implemented incrementally across devices with different use cases and characteristics. A wave shall only be deployed if the previous wave has been successfully completed and no issues have been identified.
- Emergency patches shall be those intended to remediate actively exploited vulnerabilities, zero-day vulnerabilities, or vulnerabilities which, due to their level of risk, require accelerated remediation. The implementation period for such patches shall not exceed two weeks.
- Operating system patches for Windows servers shall be applied monthly.
- Operating system patches for Linux servers shall be applied quarterly.
- Compliance with remediation deadlines shall be periodically monitored by the Information Security Department Technical Office.
- Patch implementation timeframes for vulnerabilities detected through DAST or SAST assessments shall be as follows, according to their criticality:
 - Critical: 2 weeks.
 - High: 1 month.
 - Medium: 3 months.
 - Low: 6 months.
 - Informational: no remediation timeframe is established.
- Vulnerabilities that exceed the established remediation deadlines shall be reported to the owner of the affected asset for regularisation or, where appropriate, for formal risk acceptance.

ID	VULNERABILITY MANAGEMENT STANDARD	CLASSIFICATION	VERSION	DATE
IS_ST_23		FCC_INTERNAL	1.0	July 2026

2.6.2 Exceptions

In cases where compliance with the requirements of this Standard is not possible, the agreed exceptions shall be documented in accordance with the following principles:

- For vulnerabilities that cannot be remediated within the timeframes established by this Standard due to complexity, resource availability or implementation window constraints, a revised implementation deadline for the corresponding countermeasures shall be agreed with the Information Security Department.
- For vulnerabilities that will not be remediated, a risk acceptance statement shall be prepared and the document, signed by the owner of the relevant system, shall be retained as evidence.

2.7 Reassessment

The reassessment process to verify the mitigation of vulnerabilities identified during FCC Group vulnerability scanning activities shall comply with the following principles:

- Following the remediation of a vulnerability, a new assessment of the affected asset shall be performed. This reassessment shall be requested by the asset owner and shall have the same scope as the original assessment.
- A vulnerability shall not be considered resolved until the implemented remediation measures have been successfully verified through reassessment.

ID	VULNERABILITY MANAGEMENT STANDARD	CLASSIFICATION	VERSION	DATE
IS_ST_23		FCC_INTERNAL	1.0	July 2026

3. Responsibilities

The Information Security Department shall:

- Verify the proper implementation of this Standard.
- Define and oversee the vulnerability management process.
- Consolidate technical vulnerability records from the different FCC Group Business Units in order to maintain a common database of technical weaknesses affecting the FCC Group technological environment.
- Periodically monitor the overall status of technical vulnerabilities across the FCC Group technological environment.
- Periodically report on the state of vulnerability management within the FCC Group to the relevant stakeholders and interested parties.
- Communicate the existence of critical vulnerabilities representing a high security risk to the organisation to the appropriate business units and entities, and ensure that suitable mitigation measures are implemented.

The Information Systems and Technology Division (DSTI) shall:

- Coordinate, plan and, where appropriate, execute the process of monitoring and identifying technical vulnerabilities affecting FCC Group information assets.
- Provide, maintain and operate the infrastructure, technologies and/or tools required to support effective vulnerability management across FCC Group entities.
- Establish and maintain relationships with public and private authorities, institutions, industry groups and working groups actively involved in the identification and assessment of new technical vulnerabilities, in order to maintain an up-to-date knowledge base regarding vulnerabilities that may affect FCC Group Systems, Networks and Technological Infrastructure.

FCC Group Business Units are responsible for:

- Receiving and reviewing the various reports issued by the technical vulnerability identification team and the Cyber Intelligence service, analysing their content to support decision-making and the implementation of technical and/or organisational measures required to remediate identified weaknesses.
- Performing, or requesting, a vulnerability assessment of newly implemented Information Systems prior to their deployment into production.
- Performing, or requesting, a technical vulnerability assessment before significant changes to existing Information Systems are deployed into production.
- Remediating vulnerabilities affecting their assets and Information Systems within the established deadlines.
- Ensuring proper vulnerability management for third-party information assets that may have any impact, regardless of degree or nature, on the infrastructure, networks and/or Information Systems used within their Business Unit.

ID	VULNERABILITY MANAGEMENT STANDARD	CLASSIFICATION	VERSION	DATE
IS_ST_23		FCC_INTERNAL	1.0	July 2026

- Periodically informing the Information Security Department of the remediation status of identified technical vulnerabilities, as well as the activities planned for their proper resolution.
- Notifying the Information Security Department of any technical weaknesses identified through means other than the vulnerability management service established by the Information Security Department.
- Informing the Information Security Department of their specific vulnerability management requirements relating to their Information Systems.

ID	VULNERABILITY MANAGEMENT STANDARD	CLASSIFICATION	VERSION	DATE
IS_ST_23		FCC_INTERNAL	1.0	July 2026

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
5.2	Information Security Roles and Responsibilities	[org.4] Authorization Process
5.5	Contact with Authorities	Art. 25 Security Incidents [op.exp.7] Incident Management
5.6	Contact with Special Interest Groups	Art. 13 Organization and Implementation of the Security Process [org.1] Security Policy
5.7	Threat Intelligence	[op.mon.3] Monitoring
5.9	Inventory of Information and Other Associated Assets	[op.exp.1] Asset Inventory [op.pl.2] Security Architecture
8.8	Technical Vulnerability Management	[op.mon.3] Monitoring [op.exp.4] Security Maintenance and Updates
8.15	Event Logging	[op.exp.8] Activity Logging
8.16	Monitoring Activities	[op.mon.3] Monitoring [mp.s.4] Protection Against DoS Attacks
8.31	Segregation of Development, Test and Production Environments	[mp.sw.2] Acceptance and Deployment
8.32	Change Management	[op.exp.5] Change Management