INFORMATION SECURITY MANAGEMENT POLICY
FCC INDUSTRIAL

Information Security Management Policy, the Security System and the National Security Scheme

FCC Industrial uses and processes a large amount of information in its daily activity in order to meet its business objectives. The Management of FCC Industrial, aware of the need to promote, maintain and improve the customer focus in all its activities, has implemented an Integrated Management System (SGSI, Security and ENS) in accordance with standards whose ultimate objective is to ensure that we understand and we share the needs and goals of our clients, trying to provide services that meet their expectations by working on continuous improvement. This Information Security Management Policy, the Security System and the National Security Scheme, integrated in this document, and the regulations related to it, establish a framework that allows information to be managed securely, real and effective and according to the purpose of the organization. For this purpose, **the involvement of all the organization's personnel** is sought in the application of the measures that are determined. For this reason, one of the primary objectives of this policy is to publicize both the guidelines adopted and the objectives they seek to cover with all of this, given the active role that all the people in the company will play in achieving them.

FCC Industrial expressly states its commitment to enhance the Security and Cybersecurity of the Information of the service provided, and undertakes to satisfy the needs and expectations of the interested parties, and to maintain our competitiveness high in the services and products detailed in the **scope,** accordin to the **legal and regulatory framework** in which the activities are developed, and which are specified in the MCMA_ FCC Industrial Quality Management System Manual.

FCC Industrial is aware of both the importance of the security of the information it processes and the importance of ensuring the **confidentiality, integrity, availability, authenticity and traceability** of its **information** systems, as well as the irreplaceable and inherent nature of work on a daily basis day-to-day and an essential part of the service provided to our clients, within parameters that ensure the quality and effectiveness of the information technology service, under the following basic principles:

- Security management must be in accordance with the **requirements** of the information security management system and the ENS and must comply with the provisions of current legal regulations.
- Information is a strategic resource for FCC Industrial and, therefore, its adequate **protection** must be guaranteed in the performance of daily activity and in relations with external entities.
- Information security and cybersecurity are tasks that involve all FCC Industrial personnel, both individually and through cooperation between the different departments, services and units. It is necessary to have **personnel sensitive** to the needs of a good information security system.
- Disseminate and ensure compliance with the **mandatory information** security, security system and ENS regulations among all FCC Industrial personnel at different levels.
- Identify and consider **risks and opportunities** in order to ensure that the information security management system can achieve its intended results, prevent or reduce undesirable effects and achieve continual improvement. Identify risks and adopt protective measures against **threats** to information security proportional to the value of the assets to be protected, the existing risks and the impact of possible security failures, including the risks arising from the processing of personal data (according to the FCC Group's internal regulations on the LOPD).
- Preserve the **confidentiality, integrity, availability, authenticity and traceability** of the information during its treatment, regardless of the medium in which it is contained, and of the place where it is located.

INFORMATION SECURITY MANAGEMENT POLICY
FCC INDUSTRIAL

Information Security Management Policy, the Security System and the National Security Scheme

- Commitment to **continuous improvement** of the information security management system, and that this policy be re-examined at Management meetings for this purpose.
- FCC Industrial adheres to the information security **policies** of the FCC Group.

MISSION and OBJECTIVES:

FCC Industrial also defines these **general objectives** for the application of these policies:

- Establish a risk analysis and management strategy aimed at better understanding them and their safeguards.
- Establish basic protection needs, security plans to apply the safeguards.
- Organize security based on criteria for classifying information, responsibility of its owners, descriptions of tasks and procedures, procedures for security violations, disciplinary consequences for non-compliance with security standards, security compliance checks and configuration and change management.
- Promote the continuous improvement of services and customer support.
- Continue positioning FCC Industrial as a benchmark in the sector.
- Provide solutions to transform data and information to help our clients make decisions.
- Provide clients with the most professional equipment and immediately and for as long as necessary have highly qualified technicians, experts in the required disciplines and accustomed to working as a team.
- Have a service provision based on our commitment to the continuous improvement of our systems, with information security and cybersecurity as a central pillar and by default.

The ultimate goal of information security is to ensure that an organisation can meet its objectives using information systems. The following **Basic Principles** should be taken into account in security decisions:

a. Security as an integral process.

b. Risk-based security management.

c. Prevention, detection, response and maintenance.

d. Existence of lines of defence.

e. Continuous surveillance.

f. Periodic reassessment.

g. Differentiation of responsibilities.

INFORMATION SECURITY MANAGEMENT POLICY
FCC INDUSTRIAL

Information Security Management Policy, the Security System and the National Security Scheme

Our **mission** and objectives will be achieved through compliance with the following **Minimum Requirements:**

- Organisation and implementation of the security process.
- Risk analysis and management.
- Personnel management.
- Professionalism.
- Authorisation and control of access.
- Protection of installations.
- Procurement of security products and contracting of security services.
- Least privilege.
- System integrity and updating.
- Protection of stored and in-transit information.
- Prevention of other interconnected information systems.
- Logging of activity and detection of malicious code.
- Security incidents.
- Business continuity.
- Continuous improvement of the security process.

- A system of **objectives**, metrics and indicators of continuous improvement, monitoring, measurement of our internal processes, as well as the satisfaction of our customers. Establishing and supervising compliance with contractual requirements to ensure an efficient and safe service.
- Continually training and raising awareness of our team to have the highest degree of **professionalism** and specialization possible, in addition to having our infrastructures in an adequate state and in accordance with the requirements of our clients.
- With a secure product acquisition management procedure.
- Complying with the requirements of current legislation, especially with the General Data Protection Regulations and compliance with our **Security Documentation**. The guidelines for the structuring of **the system security documentation**, its management and access are detailed in PR_FCCIND_120_01 Information Management and Security.
- Introducing continuous improvement processes that allow permanent progress in our Information Security management.

INFORMATION SECURITY MANAGEMENT POLICY FCC INDUSTRIAL

Information Security Management Policy, the Security System and the National Security Scheme

- Managing and preparing plans for the management and treatment of risks with an analysis and risk management methodology used, based on standards.
- Managing internal and external communications and information stored and in transit.
- Ensuring interconnection with other information systems
- Managing and monitoring activity with log management.
- With special attention to the management of **security incidents.**
- Ensuring the **continuity** and availability of business and services.
- Ensure that our Assets and Services comply with the ENS measures of the level established for the dimensions of **Confidentiality, Integrity, Availability, Authenticity and Traceability.**

Likewise, these principles must be considered in the following security areas:

- **Physical:** Comprising the security of dependencies, installations, hardware systems, supports and any asset of a physical nature that processes or can process information, as well as physical access.
- **Logic:** Including aspects of protection of applications, networks, electronic communication, computer systems and logical access.
- **Political-corporate:** Formed by security aspects related to the organization itself, internal rules, regulations and legal regulations.

Roles or security functions:

At FCC we have an information manager, systems manager, information security manager and a service manager, whose functions and responsibilities have been accepted by the respective managers.

The Information Security Committee of FCC Industrial is the coordination and conflict resolution mechanism

The functions of those responsible and of the Committee itself are reflected in Procedure PR_FCCIND_120_01 Information Management and Security.

All the regulations that are issued in order to achieve these objectives will bind the people responsible for their application, and in general the entire organization in their compliance.

INFORMATION SECURITY MANAGEMENT POLICY
FCC INDUSTRIAL

Information Security Management Policy, the Security System and the National Security Scheme


Approved by

Miguel Ángel Mayor Gamo

General Manager FCC Industrial I.E

Edition **10** **30/01/2024**