Information Security Policy of Digital Services Operations for ENS (Spain)

Type:	2 Policy
Version No.:	1
Reference No.:	15475
Scope:	FME CE/DSS/Digital Services Operations (All Fresenius Medical Care AG wholly or majority-owned entities and organizational units allocated to FME CE/DSS/Digital Services Operations)
Out of Scope:	n/a
Target Group:	All officers, directors and employees (full-time, part-time and dually engaged) involved in documentation and activities within the ISMS of Digital Services Operations
Publication Date:	09/December/2025
Effective Date:	4 weeks after publication
Status:	Published
Owner's Department:	Digital Services Operations
Approver's Position:	Head of Digital Services Operations
Approver's Position:	n/a

This document is internal and is the sole property of Fresenius Medical Care. It is issued by the Document Owner and is electronically published in the Policy Management database. Printouts of this document are for reference only. The user is always responsible for referring to the Policy Management database for the latest and valid version.

CONTENT

1 PURPOSE

This policy complies with Control 3.1 of the National Security Framework (ENS), having been established by the Information Security Committee and including all requirements mandated by the regulation. This document lays the foundation for the management of Information Security at Fresenius Medical Care (hereinafter, FMC) and expands the Information Security Policy of Digital Services Operations (18301) for Spain.

2 DEFINITIONS

The terms used throughout this document are defined as per the Common Definition Framework. The following definitions are specific to this document:

Term	Definition
BISO	Business Information Security Office
ISMS	Information Security Management System
DSO	Digital Services Operations
FME	Fresenius Medical Care
ICT	Information and Communication Technology
RAT	Record of Activities Tool

3 REQUIREMENTS / PROCESS

FME relies on ICT systems to achieve its objectives. These systems must be diligently managed, with appropriate measures taken to protect them against accidental or deliberate damage that may affect the availability, integrity, confidentiality, or traceability of the information processed or the services provided.

The purpose of information security is to ensure the quality of information and the continuous delivery of services, acting preventively, monitoring daily activity, and responding promptly to incidents.

3.1 Threat Landscape and Protection Requirements

ICT systems must be protected against fast-evolving threats with the potential to impact the confidentiality, integrity, availability, intended use, and value of information and services. To defend against these threats, a strategy is required that adapts to changing environmental conditions to ensure continuous service delivery.

This means departments must apply the minimum-security measures required by the ENS, as well as continuously monitor service performance levels, follow and analyze reported vulnerabilities, and prepare an effective response to incidents to ensure service continuity.

3.2 Security in the ICT System Lifecycle

Departments must ensure that ICT security is an integral part of every stage of the system life cycle, from conception to decommissioning, including development or procurement decisions and operational activities. Security requirements and funding needs must be identified and included in planning, requests for proposals, and procurement specifications for ICT projects.

Departments must be prepared to prevent, detect, respond, and recover from incidents.

3.3 Policy Foundations and Regulatory Basis

This policy is established in accordance with the basic principles of Chapter II of Royal Decree 311/2022 and will be developed by applying the following minimum requirements:

- Organization and implementation of the security process
- Risk analysis and management
- Personnel management
- Professionalism
- Authorization and access control
- Protection of facilities
- Procurement of security products and contracting of security services
- Principle of least privilege
- System integrity and updates
- Protection of stored and transmitted information
- Safeguards against interconnected information systems
- Logging of activity and detection of malicious code
- Security incidents
- Business continuity
- Continuous improvement of the security process

These minimum requirements are applied in proportion to the risks identified in our system, in accordance with Article 28 of Royal Decree 311/2022.

3.4 Scope of the Information System

Information system supporting advisory services, application development, import, sales, distribution, support, and technical assistance of solutions and equipment, in accordance with the current statement of applicability.

FME relies on ICT systems to achieve its service delivery objectives in advisory, application development, import, sales, distribution, support, and technical assistance of solutions and equipment.

These systems must be diligently managed, with appropriate measures taken to protect them against accidental or deliberate damage that may affect the availability, integrity, confidentiality, or traceability of the information processed or the services provided.

3.5 Guaranteeing Information Quality and Service Continuity

The purpose of information security is to guarantee the quality of information and the continuous delivery of services, acting preventively, monitoring daily activity, and responding promptly to incidents.

The services provided result in improved infrastructure performance, increased productivity of technical staff, and a significant reduction in investment costs. In other words, the goal is to maximize uptime and the security of information systems without having to invest in equipment, software, or staff training.

3.6 Role of the Information Security Policy

The Information Security Policy provides the basis for defining and delimiting objectives and responsibilities for the technical, legal, and organizational actions required to guarantee information security and privacy, complying with applicable legal frameworks and the organization's global and specific policies, as well as the defined procedures.

These actions, from the perspective of security and privacy, are selected and implemented based on risk analysis and the balance between acceptable risk and the cost of measures.

The purpose of the Security Policy is to establish the necessary framework to protect information resources and data against threats, whether internal or external, deliberate or accidental.

Information and data may exist in various formats, both electronic and paper or other media, and may include critical data about the company's and clients' operations, strategies, or activities, and, where applicable, sensitive personal data as established by personal data protection laws. The loss, corruption, or theft of information or the systems managing it has a major impact on our organization.

FME is convinced that effective management of Information Security and Privacy enables the organization to fully understand and appropriately address the risks to which information is exposed, and to respond and adapt efficiently to increasing regulatory, legal, and client requirements.

We adopt values that are essential to achieving our objectives, such as the preservation of information and personal data, both our own and that of stakeholders, and the professional and personal development of our team members.

3.7 Protection of Information as a Strategic Asset

Information is a highly valuable asset for our organization and therefore requires appropriate protection and management to ensure business continuity and minimize potential damage caused by failures in the integrity, availability, and confidentiality of information. Likewise, current legislation on personal data protection (GDPR and LOPDGDD), as well as our commitment to clients, makes us particularly sensitive to the handling of personal data we access in the course of our activity.

We establish management activities aimed at preserving the principles of Confidentiality, Integrity, Availability, Authenticity, Traceability, and Regulatory Compliance. These principles are defined as follows:

- **Confidentiality:** The property that ensures access to information is only granted to authorized persons.
- **Integrity:** The property of safeguarding the accuracy and completeness of information assets.
- **Availability:** The quality that guarantees authorized persons can access and process information whenever necessary.
- **Authenticity:** The property ensuring that an entity is who it claims to be or that the source of data can be verified.
- **Traceability:** The property that ensures the actions of an entity can be attributed exclusively to that entity.
- **Regulatory Compliance:** The property ensuring that information is managed in accordance with ethical, professional, and legal principles established by applicable regulations.

Systems must be protected against fast-evolving threats with the potential to impact information and services. To defend against these threats, a strategy is required that adapts to changing environmental conditions to ensure continuous service delivery.

3.8 ENS Compliance Requirements

Departments must apply the minimum-security measures required by the ENS, continuously monitor service performance levels, analyze vulnerabilities, and prepare effective responses to incidents to ensure continuity of services provided.

Departments must ensure that security is an integral part of every stage of the system life cycle, from conception to decommissioning, including development or procurement decisions and operational activities. Security requirements and funding needs must be identified and included in planning, requests for proposals, and procurement specifications for ICT projects.

Departments must be prepared to prevent, detect, respond, and recover from incidents, in accordance with Article 8 of the ENS.

3.9 Privacy Integration in the ISMS

Within this framework, privacy protection is embedded. Our systems process sensitive personal data, and therefore, privacy protection is considered a fundamental pillar of the ISMS, as well as a social necessity that companies must respect and protect, and which is also the subject of specific legislation and/or regulation worldwide.

The purpose of the Information Security Management System (ISMS) is to ensure that information security and privacy risks are known, assumed, managed, or minimized in a documented, systematic, structured, repeatable, manageable manner, and adapted to changes in risks, the environment, and technologies.

3.10 GDPR Data Protection Principles

With regard specifically to the protection of personal data, FME undertakes to comply with the principles established in the relevant legislation. These are:

- **Principle of lawfulness, transparency, and fairness:** Data must be processed lawfully, fairly, and transparently for the data subject.
- **Principle of purpose limitation:** Data must be processed for one or more specific, explicit, and legitimate purposes. Data collected for such purposes must not be further processed in a way incompatible with those purposes.
- **Principle of data minimization:** Apply technical and organizational measures to ensure that only the data strictly necessary for each specific processing purpose is processed, reducing the extent of processing, limiting retention periods, and restricting accessibility.
- **Principle of accuracy:** Implement reasonable measures to keep data accurate and up to date, and ensure data is deleted or corrected without delay when inaccurate in relation to the purposes for which it is processed.
- **Principle of storage limitation:** Data retention must be limited to the time necessary to achieve the purposes of the processing.
- **Principle of security:** Conduct a risk analysis to determine the necessary technical and organizational measures to guarantee the integrity, availability, and confidentiality of personal data.
- **Principle of accountability:** Maintain ongoing due diligence to protect and guarantee the rights and freedoms of individuals whose data is processed, based on an analysis of risks

to those rights and freedoms, ensuring and demonstrating that processing complies with GDPR and national regulations.

3.11 Management Responsibilities

Management will direct, support, and oversee the ISMS in accordance with Royal Decree 311/2022 and subsequent amendments, and will ensure that the system's objectives are achieved.

The company's management commits to supporting and promoting the principles established in this Policy, and requires FME staff to comply with the documented ENS management system.

3.12 Departmental Security Responsibilities

All departments must avoid, or at least prevent to the greatest extent possible, information or services from being compromised by security incidents. To this end, departments must implement the minimum security measures determined by the ENS, as well as any additional controls identified through threat and risk assessments. These controls, along with the security roles and responsibilities of all staff, must be clearly defined and documented.

To ensure compliance with the policy, departments must:

- Authorize systems before they go into operation.
- Regularly assess security, including evaluations of routine configuration changes.
- Request periodic reviews by third parties to obtain an independent assessment.

3.13 Continuous Monitoring Requirements

Since services can quickly deteriorate due to incidents ranging from slowdowns to full outages, operations must be continuously monitored to detect anomalies in service performance levels and respond accordingly, as set out in Article 8 of the ENS.

Monitoring is particularly relevant when defense lines are established in accordance with Article 9 of the ENS. Detection, analysis, and reporting mechanisms will be implemented to ensure that responsible parties are regularly informed and alerted whenever significant deviations occur from pre-established normal parameters.

3.14 Incident Response Requirements

Departments must:

- Establish mechanisms to effectively respond to security incidents.
- Designate a contact point for communications related to incidents detected in other departments or organizations.
- Establish protocols for the exchange of incident-related information, including two-way communications with Computer Emergency Response Teams (CERT).

To guarantee the availability of critical services, departments must develop ICT continuity plans as part of their overall business continuity and recovery framework.

FME is committed to delivering managed services in compliance with the requirements of its Integrated Management System, ensuring uninterrupted service delivery in accordance with availability, security, and quality requirements for clients.

3.15 Documentation Structure

This Information Security Policy complements security procedures and policies in different areas. Documentation related to Information Security will be classified into three levels, where each document at a given level is based on those at the higher level:

- **First level:** Security Policy
- **Second level:** Security procedures and policies
- **Third level:** Reports, records, and electronic evidence

This Policy will be developed through specific security regulations addressing particular aspects. Security regulations will be available to all members of the organization who need to be aware of them, particularly those who use, operate, or administer ICT systems.

3.16 Applicable Data Protection Legislation

In the area of personal data, the following applies:

- **Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 (GDPR)** on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, repealing Directive 95/46/EC.
- **Organic Law 3/2018 of December 5** on the Protection of Personal Data and guarantee of digital rights.

3.17 Applicable ENS Legislation

In the context of the ENS, this policy is governed by the following regulations:

- **Royal Decree 311/2022 of May 3**, regulating the National Security Framework, developing Laws 39 and 40 of 2015.
- **Law 39/2015 of October 1** on the Common Administrative Procedure.
- **Law 40/2015** on the Legal Regime of the Public Sector.
- **Technical Instructions of the CCN (CCN-STIC).**

3.18 Responsibilities of the Security Committee

The Information Security Committee will have the following functions:

- Regularly inform Senior Management about the state of information security.
- Promote continuous improvement of the ISMS.
- Develop the organization’s security strategy.
- Coordinate efforts of different areas in information security to ensure consistency, alignment with the decided strategy, and avoid duplication.
- Draft (and regularly review) the Information Security Policy for approval by Management.
- Approve information security regulations.
- Coordinate all security functions of the organization.
- Ensure compliance with applicable legal and sectoral regulations.
- Ensure security activities are aligned with organizational objectives.
- Coordinate Business Continuity Plans across different areas to ensure seamless action in case of activation.
- Coordinate and approve, where appropriate, security project proposals, ensuring regular reporting on progress and highlighting deviations.
- Receive security-related concerns from Management and forward them to the relevant departmental managers, collecting their responses and solutions, and reporting them back to Management.

- Collect regular reports from departmental security managers on the organization’s security status and potential incidents. These reports will be consolidated and summarized for communication to Management.
- Coordinate and respond to security concerns raised through departmental security managers.
- Define, within the Corporate Security Policy, the assignment of roles and criteria for achieving guarantees in segregation of duties.
- Develop and approve training and qualification requirements for administrators, operators, and users from an information security perspective.
- Monitor key residual risks assumed by the organization and recommend potential actions.
- Monitor the performance of incident management processes and recommend possible improvements, ensuring coordination of security areas in managing incidents.
- Promote periodic audits to verify compliance with security obligations.
- Approve information security improvement plans and coordinate different plans across areas.
- Prioritize security actions when resources are limited.
- Ensure that information security is considered in all ICT projects, from initial specification to operation. In particular, ensure the creation and use of shared services that reduce duplication and support consistent functioning across ICT systems.
- Resolve responsibility conflicts between different managers and/or organizational areas.

The Business Information Security Officer is appointed by the Information Security Committee. The appointment will be reviewed every two years or when the position becomes vacant.

Other roles mentioned above will likewise be designated by the Committee through formal meeting minutes.

3.19 Record of Processing Activities

The RAT, to which only authorized people will have access, collects the activity logs of the data processing operations concerned and the corresponding data controllers.

All the company's information systems will comply with the security levels required by the regulations for the nature and purpose of the personal data collected in the above-mentioned document.

3.20 Risk Analysis Requirements

All systems subject to this Policy must undergo a risk analysis, evaluating the threats and risks to which they are exposed. This analysis will be repeated:

- Regularly, at least once a year
- When the information processed changes
- When the services provided change
- When a serious security incident occurs
- When serious vulnerabilities are reported

To harmonize risk analyses, the Information Security Committee will establish a reference assessment for the different types of information handled and the services provided.

The Information Security Committee will promote the availability of resources to meet the security needs of the different systems, encouraging horizontal investments.

3.21 Obligations of Personnel

All FME members are required to be aware of and comply with this Information Security Policy and Security Regulations. The Information Security Committee is responsible for ensuring that the information reaches those affected.

Additionally, all staff must attend an information security awareness session at least once a year. A continuous awareness program will be established for all organization members, especially newcomers.

People responsible for the use, operation, or administration of ICT systems will receive training in the secure handling of systems, as necessary to perform their duties. Training will be mandatory before assuming responsibilities, whether it is their first assignment or a change in role or responsibilities.

3.22 Third-Party Security Requirements

When third-party services are used, or information is transferred to third parties, they will be made aware of this Security Policy and the Security Regulations applicable to those services or information. Third parties will be subject to the obligations established in these regulations and may develop their own operating procedures to meet them. Specific reporting and incident resolution procedures will be established. Third-party personnel must receive appropriate security awareness training, at least at the same level established by this Policy.

When any aspect of the Policy cannot be met by a third party as required above, the Business Information Security Officer must issue a report specifying the risks incurred and how to address them. This report must be approved by those responsible for the affected information and services before proceeding.

3.23 Security Management for External Clients

When FME provides services to, or handles information from, other public or private organizations, these organizations will be made aware of this Information Security Policy. Communication channels will be established for reporting and coordination between the respective Information Security Committees, and procedures will be defined for responding to security incidents.

3.24 Consequences for Non-Compliance

Failure to comply with this Information Security Policy may result in the initiation of appropriate disciplinary measures, without prejudice against any applicable legal responsibilities.

3.25 Review and Maintenance of the Policy

The Information Security Committee is responsible for the annual review of this Information Security Policy and for proposing its revision or maintenance.

The Policy will be approved by the Governing Body and disseminated so that all affected parties are aware of it.

This Policy will be developed through specific security regulations addressing particular aspects. These regulations will be made available to all organization members who need to be familiar with them, particularly those who use, operate, or administer ICT systems.

4 RELATED INTERNAL CONTROLS

Subject	Title
3.1 ENS	Politica de Seguridad ENS

5 RELATED DOCUMENTS

Document	Title
18301	Information Security Policy of Digital Services Operations

6 ANNEXES

Document	Title
None	