FUJIFILM
Value from Innovation

FUJIFILM PORTUGAL, S.A.

COMPANY POLICY

ISMS POLICY

Rev.00

DOCUMENT FILE NAME

ISMS Policy_rev.00

Approval

Approved by	Position	Signature	Date
Élio Santos	ISMS Manager		26/11/2025

DOCUMENT REVISION HISTORY

REVISION	DATE	CHANGE	Author
Rev.00	24/11/2025	First release	Mariana Barros

DOCUMENT CONFIDENTIALITY

CLASS	DISTRIBUTION (*)	NOTES
Restricted	Stakeholder	Dissemination of the document to all the stakeholder of FFPT is permitted.

(*) For regulatory reasons (such as performing an Audit), the document may be made available to other persons, including those outside the FUJIFILM Portugal, S.A. Manufacturer Organization (MDSW-M), as long as they are subject to the constraint of confidentiality in the performance of their duties.

REFERENCE DOCUMENTS

- ISO 9001:2015 standard
- ISO 13485:2016/A11:2021 standard
- ISO 27001:2022 standard
- ISO 27017:2015 standard
- ISO 27018:2025 standard
- Regulation (UE) 2016/679 (GDPR)
- P.01 Document Control Procedure

TABLE OF CONTENTS

1. PURPOSE

The purpose of this Information Security Policy is to provide a clear framework for the management of information security within FFPT, defining the principles, objectives, and direction for protecting information and related assets.

This policy reflects the FFPT's commitment to ensuring the confidentiality, integrity, and availability of information and to meeting applicable legal, regulatory, and contractual requirements.

It also supports the establishment, implementation, maintenance, and continuous improvement of the Information Security Management System (ISMS).

2. SCOPE

This policy applies to all employees and, where applicable, third parties, including contractors, partners, and service providers who have access to the FFPT's information and systems.

It covers all information assets, including digital and physical information, systems, infrastructure, and processes as defined and maintained in the FFPT's asset inventory and within the scope of the Information Security Management System (ISMS).

3. ROLES AND RESPONSIBILITIES

3.1. ALL EMPLOYEES

All employees within and third parties acting for or on behalf of FFPT are responsible for IT System Security and shall:

- comply with this policy and applicable information security requirements;
- protect and handle information and assets in accordance with its classification and applicable rules;
- report information security incidents, weaknesses or suspicious activities;
- participate in security awareness and training activities.

3.2. INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS) MANAGER

The ISMS Manager shall:

- ensure the ISMS Policy and its objectives are established and are compatible with the strategic direction of the organization;
- review and approve the FFPT ISMS Policy;
- establish, implement, maintain and improve the ISMS;
- monitor ISMS performance and report to top management;
- ensure risks are identified, assessed and treated;
- ensure that information security incidents are appropriately managed and reported to FFPT management, including, where applicable, communication with relevant authorities;
- ensure appropriate protection of information assets within the organization;

- ensure the integration of the security requirements into the organization's processes;
- support the IT System Security principles.

3.3. COMPLIANCE AND LEGAL DEPARTMENT

The compliance and legal function shall:

- ensure that applicable legal, regulatory and compliance requirements related to information security and IT systems are identified and addressed, including those concerning privacy and administrative law;
- monitor regulatory developments and support their integration into the ISMS;
- provide guidance on legal obligations and compliance risks in relation to data protection and general legal requirements as required.

3.4. QARA TEAM

The QARA team shall:

- ensure alignment of the ISMS with applicable standards and regulatory requirements;
- review the content and format and maintain this policy to ensure consistency, adequacy and scope coverage;
- monitor the implementation of compliance requirements within the ISMS;
- support audits and continuous improvement of the ISMS.

3.5. TOP MANAGEMENT

Top Management shall ensure the availability of resources and demonstrate commitment to the effectiveness of the ISMS and support this policy.

4. ABBREVIATIONS ADOPTED IN THE DOCUMENTS

4.1. ACRONYSM

FFPT	Fujifilm Portugal, S.A.
ISMS	Information Security Management System
QARA	Quality Assurance & Regulatory Affairs
SLA	Service Level Agreement

4.2. DEFINITIONS

Software as a Service (SaaS): Cloud service model in which customers use software applications hosted and managed by a service provider over a network.

Check the D.01 Abbreviations adopted in the QMS Documents for the whole list of all abbreviations and acronyms adopted in the management system of FFPT

5. BACKGROUND AND OBJECTIVES

FFPT operates in the Medical Systems sector, providing integrated products and services in line with its defined business objectives.

Information, in all its forms, is recognized as a key business asset and shall be classified and protected according to its sensitivity and criticality.

FFPT interacts with internal and external stakeholders whose expectations include the secure management of the information.

To support these objectives, FFPT establishes, implements, maintains and continuously improves and ISMS aligned with its business context and applicable requirements.

6. POLICY DESCRIPTION

6.1. POLICY STATEMENT

FFPT shall establish, implement, maintain, and continually improve an Information Security Management System (ISMS) aligned with its business context and applicable requirements.

Information security shall be managed through a structured and risk-based approach, ensuring that risks are identified, assessed, and treated to acceptable levels.

For FFPT, the primary objective of information security is the protection of data and information, including personal data processed as Data Controller and Data Processor.

To support this objective, FFPT protects its technological infrastructures, physical assets, logical systems, and internal organization to ensure the secure management of the information within its business activities, preserving:

Confidentiality: that information is accessible only to duly authorized individuals and/or processes;

Integrity: protecting the consistency of information from unauthorized modification;

Availability: that authorized individuals have access to information and associated architectural elements when they request it;

Authenticity: the reliable origin of information;

Accountability: the ability to trace actions and activities to a responsible individual or entity;

Privacy: the protection and control of personal data.

Appropriate organizational, people, physical, and technological controls shall be implemented to support the secure management of information across the FFPT's activities and services.

Information security incidents and vulnerabilities shall be identified and managed in a timely manner to minimize their impact.

6.2. INFORMATION SECURITY COMMITMENTS

To ensure the effectiveness of the ISMS, FFPT is committed to:

- protecting information and associated assets against unauthorized access, disclosure, alteration, and destruction;
- ensuring compliance with applicable legal, regulatory, and contractual requirements;
- implementing, maintaining, and continuously improving an effective ISMS;
- adopting a risk-based approach to identify, assess, and treat risks;
- ensuring awareness and training of employees and stakeholders;
- maintaining security across suppliers and cloud services;
- maintaining service quality and meeting agreed service levels (SLA);
- ensuring adequate resources for information security;
- promoting a culture of information security;
- defining clear roles and responsibilities;
- continually improving ISMS effectiveness.

6.3. INFORMATION SECURITY PRINCIPLES

To ensure the effectiveness of the ISMS, FFPT shall ensure that:

- information is identified, classified, and protected according to its criticality;
- access to information and systems is restricted to authorized users;
- information security incidents and vulnerabilities are identified and managed to minimize impact;
- physical and logical access are controlled;
- business continuity and recovery capabilities are maintained;
- cloud services in Software as a Service (SaaS) modality are used securely;
- documented information is maintained and controlled to support ISMS effectiveness;
- Continuous improvement shall be achieved through the application of the use of the "Plan Do-Check-Act (PDCA)" cycle.

6.4. POLICY COMMUNICATION

This policy shall be communicated to all employees and made available to relevant third parties as appropriate.

Awareness of this policy shall be supported through internal communication.

The Information Security Policy is publicly available through the official FUJIFILM Portugal website (https://www.fujifilm.com/pt/). Interested parties, including customers, suppliers, partners and other external stakeholders, may access the policy through the corporate website.

References to the policy may also be included in contractual documentation and other relevant communications, where appropriate.

7. POLICY REVIEW AND UPDATE

This policy shall be reviewed periodically and updated as necessary to ensure its continued suitability, adequacy and effectiveness, considering changes in the context in which FFPT operates, as well as the evaluation of actions required in response to events such as:

- significant developments in business activities;
- emerging threats in addition to those identified in risk management;
- significant information security incidents;
- changes in the internal or external context of the organization;
- changes in applicable regulatory or legislative requirements related to information security.

Changes to this policy shall be approved by top management.