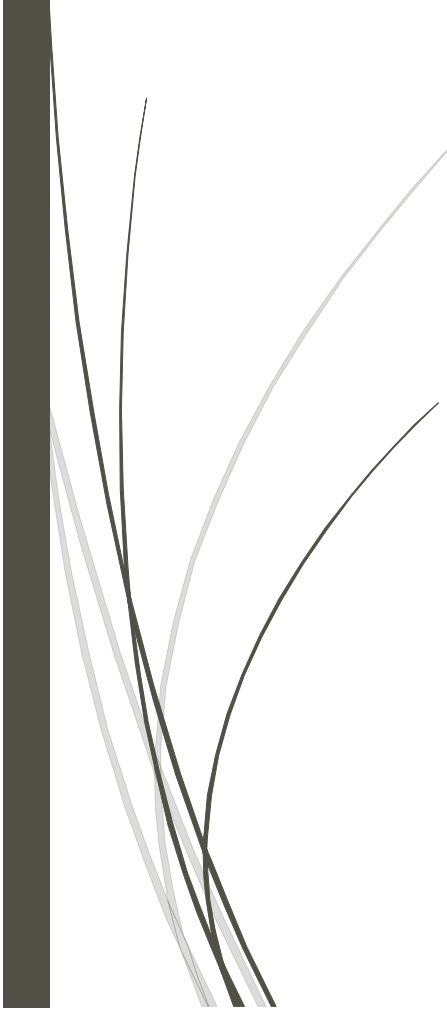
PUBLIC

Information Security Policy



MEDSIR
MEDICA SCIENTIA INNOVATION RESEARCH

APPROVAL SIGNATURES

DRAFT			
Name	Position	Signature	Date
Carlos Jiménez	IT & Information Security Manager		18/Sep/2024
Diego Espigado	Chief Ethics & Compliance Officer		18/Sep/2024

REVIEW			
Name	Position	Signature	Date
Gema Llorente	Chief Financial Officer		27/Sep/2024

APPROVAL			
Name	Position	Signature	Date
MAJ3 Capital, SL (P.p. María Campos)	Chief Executive Officer and Chair		27/Sep/2024
Diego Espigado	Chief Ethics & Compliance Officer		27/Sep/2024

VERSIONS

Version	Date	Description
1.0	September 2024	First version approved.
2.0	September 2024	Section 2 is split in two subsections to include a material scope of the policy. Table of contents consequently updated. Change in header and footer of the classification of the document (from internal to public). Inclusion of secure system architecture and engineering principles in section 3.

Table of Contents

1. Purpose

This Information Security Policy is the cornerstone of the Information Security Management System ("ISMS") of Medica Scientia Innovation Research SL and its controlled entities and, therefore, part of its Ethics and Compliance Program. This policy aims at establishing the framework and basic management approach for protecting the confidentiality, integrity, and availability of the information assets of and safeguard them from unauthorized access, disclosure, alteration, and destruction while ensuring compliance with relevant laws and regulations and standard requirements (such as [1] ISO 27001).

By means of this policy, the organization commits itself to:

a) Designing an ISMS presided by the principles of confidentiality, integrity, and availability;

b) Enforcing the ISMS's regulations;

c) Continuously improving the ISMS;

d) Properly disciplining any breach of the ISMS following the [2] Disciplinary System.

2. Scope

2.1. Personal Scope

This document applies, with different scopes, to the personnel of Medica Scientia Innovation Research SL and its controlled entities (together, "MEDSIR" or the "organization") and to third parties where expressly mentioned and if specifically required on a case-by-case basis, due to the business relationship with MEDSIR.

The term *personnel* includes:

a) Employees linked to the relevant entity by a labor contract;

b) Interns, trainees, internship students, or any equivalent, regardless of whether their services to MEDSIR are provided within or outside their education curricula;

c) Members of the relevant entities' governing body (sole director, Board of Directors, or other governing body);

d) Contractors developing activities included in the relevant entity's business purpose and working under the direct or indirect supervision, direction, or control of the people mentioned in letters *a*, *b*, or *c*.

A *controlled entity* is any organization, with or without legal personality (e.g., a joint venture), in which Medica Scientia Innovation Research SL has direct or indirect control, which includes the following situations:

a) Entities where it has, directly or indirectly, more than 50% of the share capital.

b) Entities where it has, directly or indirectly, most of the voting rights.

c) Entities where it has, directly or indirectly, the right to appoint or remove most of the members of the Board of Directors or equivalent governing body.

2.2. Material Scope

This policy and the whole ISMS apply to the information systems used by MEDSIR to provide the following services:

a) Design, development, and execution of clinical studies.

b) Strategic services provided to the life sciences industry.

c) Training in clinical studies design, development, and execution.

3. Key Principles of Information Security

Information security is presided by three characteristics:

a) Confidentiality: property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

b) Integrity: property that information has not been altered or destroyed in an unauthorized manner.

c) Availability: property of information or of resources being accessible and usable on demand by an authorized individual, entity, or process.

MEDSIR is also committed to implementing secure system architectures and engineering practices to create a robust ISMS that protects our critical assets and maintains stakeholder trust. We apply these principles when procuring, implementing, and operating information systems:

a) Security by design: we incorporate security controls from the earliest stages of system planning.

b) Defense in depth: we employ multiple layers of security controls to provide comprehensive protection.

c) Least privilege: we grant access rights based on the minimum level necessary for job functions. policy on logical access control.

d) Separation of duties: we divide critical system functions among multiple users or processes.

e) Fail-safe defaults: we set systems to default to a secure state in case of failures.

f) Complete mediation: we check every access to system resources for proper authorization.

g) Open design: we use well-established, peer-reviewed security mechanisms.

h) Psychological acceptability: we implement user-friendly security mechanisms to encourage compliance.

i) Secure system lifecycle: we maintain security throughout the entire system lifecycle.

j) Continuous monitoring: we regularly assess and improve security controls and architectures.

k) Vendor security assessment: we evaluate vendors' security practices before procurement and require our applicable minimum standards in our [3] Vendor Information Security Policy.

4. MEDSIR's Information Security Management System

MEDSIR's ISMS is a set of interrelated elements (policies, procedures, bodies, tools, responsibilities, activity planning, etc.) aiming at establishing an information security policy and objectives, and creating the framework to achieve them, based on a risk management and continuous improvement approach.

The key elements of the ISMS are:

a) The [4] Code of Ethics and Business Conduct. It is the foremost internal regulation of MEDSIR, by which it sets its values, mission, and vision of business.

b) The rest of the internal regulations (policies, procedures, working instructions, etc.) and tools.

c) The managerial roles responsible for its implementation, as described in section 6.

d) The culture of compliance. Values, ethics, beliefs, and behaviors that exist throughout the organization and interact with the organization's structures and control systems to produce behavioral norms that are conducive to compliance outcomes.

5. Risk Management Approach

MEDSIR applies risk management approach to detect information security risks, assess if and, eventually, how to prevent them or, otherwise, how to control them to avoid nonconformities.

MEDSIR considers the processes where the risks can appear, the seriousness and the probability of the consequences if an information security risk materializes and set the necessary controls to ideally prevent them or, at least, significantly reduce the probability or severity of an eventual risk materialization, to comply with MEDSIR's due diligence.

6. Roles and Responsibilities

Information security is a shared responsibility and all members of the personnel, and eventually third parties involved, must manage the information they access according to the principles set out in this policy and in the rest of the ISMS's regulations. Specifically, vendors must comply with the minimum standards set in the [3] Vendor Information Security Policy.

The governing body and the top management are responsible for delegating authority to administer the ISMS, providing resources to maintain and improve the ISMS, communicating the importance of information security, and fostering a compliance culture.

The information security manager ("ISM") is responsible for operating, managing, and supervising the effectiveness of the information security framework by delegation of the top management.

The management system officer ("MSO") is responsible for integrating the information security framework within the Integrated Compliance Management System of the organization and overseeing its effectiveness.

Both the ISM and the MSO inform, directly or indirectly, top management on their areas of delegation.

7. Training in Information Security

The ISM will liaise with Ethics & Compliance and People & Culture to prepare trainings that will address the necessary concepts and aspects of the ISMS that the personnel need to know, based on their roles within MEDSIR.

The personnel must be trained in the following topics:

a) Overview of the ISMS, especially the Information Security Policy, and the relevant internal regulations to perform their role within MEDSIR without compromising information security;

b) Information security risk and damage, and the personnel contribution to the ISMS's effectiveness, including advantages of continuous improvement;

c) How they can detect situations when an information security risk can materialize during the performance of their duties;

d) Eventual consequences of nonconformities;

e) How and to whom they must raise their queries and concerns regarding information security compliance and nonconformities.

These trainings will be compulsory where necessary. MEDSIR will keep documented prove of the content of the trainings and of the members of the personnel who attended them.

8. Performance Evaluation and Continual Improvement

8.1. Monitoring and Evaluation

The performance of the ISMS will be continuously evaluated following the annual evaluation plan containing:

a) What needs to be monitored, why, and who will be responsible for it;

b) The methods for monitoring, measurement, analysis, and evaluation, as applicable, to ensure valid results;

c) When the monitoring and measurement should be performed; and

d) When the results from said monitoring and measurement should be analyzed, evaluated, and reported.

8.2. Information Security Objectives

Specific information security objectives will be set yearly in writing. These objectives must:

a) be consistent with the Information Security Policy;

b) be measurable (preferably);

c) consider applicable requirements and risk management approach;

d) not be a legal requirement;

e) be monitored;

f) be communicated; and

g) be updated or revised as appropriate.

8.3. Annual Report

The ISM and the MSO must raise to top management an annual report including:

a) the status of actions from previous management reviews;

b) changes relevant to the ISMS and to stakeholders;

c) data on information security performance, including the results of the annual evaluation plan of the previous year, nonconformities and corrective actions, audits, the results of the risk assessment and the status of the risk treatment, opportunities for continuous improvement; and

d) the information security objectives for the ensuing year.

9. Reports of Nonconformities and Violations

Nonconformities and information security risks must be communicated to the ISM or the MSO. When a nonconformity amount to a violation of MEDSIR's Ethics and Compliance Program according to the [5] Speak Up Policy, it must be communicated according to it and be properly addressed, eventually, under the [2] Disciplinary System.

10. References

[1] ISO/IEC 27001:2022, Information security, cybersecurity and privacy protection. Information security management systems. Requirements.

[2] Disciplinary System.

[3] Vendor Information Security Policy.

[4] Code of Ethics and Business Conduct.

[5] Speak Up Policy.