PUBLIC

Vendor Information Security Policy

MEDSIR

MEDICA SCIENTIA INNOVATION RESEARCH

APPROVAL SIGNATURES

DRAFT			
Name	Position	Signature	Date
Carlos Jiménez	IT Manager / IS Manager		26/Jun/2024

REVIEW			
Name	Position	Signature	Date
Diego Espigado	Chief Ethics & Compliance Officer		12/Sep/2024
Gema Llorente	Chief Financial Officer		12/Sep/2024

APPROVAL			
Name	Position	Signature	Date
Diego Espigado	Chief Ethics & Compliance Officer		13/Sep/2024
MAJ3 Capital SL (p.p. María Campos)	Chief Executive Officer and Chair		13/Sep/2024

VERSIONS

Version	Date	Description
1.0	September 2024	First version approved.

Table of Contents

1. Purpose

This policy establishes minimum information security requirements and commitments that all vendors must comply with and assume when processing, storing, or transmitting data pertaining to Medica Scientia Innovation Research SL or its controlled entities (together, "**MEDSIR**" or the "**organization**") or when accessing their information systems. Vendors with a higher risk profile may be held to a higher standard, which will be set contractually.

This policy helps protect the confidentiality, integrity, and availability of our information assets.

2. Scope

This policy applies to all vendors, contractors, consultants, or collaborators that have access to MEDSIR's data or systems (indistinctly referred to as "**vendors**"). Any reference to a vendor includes said vendor's contractors, subcontractors, agents, or any other third party used by the vendor to provide services to MEDSIR.

3. Requirements and Commitments

a) Access control and identity management:

   a. Vendors must implement role-based access controls and follow the principle of least privilege.

   b. Multi-factor authentication is required for all vendor accounts accessing MEDSIR systems.

   c. Vendors must regularly review and promptly revoke access rights when no longer needed.

   d. Vendor access must be promptly revoked when no longer needed.

   e. Vendor's premises must have controlled access.

b) Information classification and use:

   a. Vendors must comply with MEDSIR's Information Classification and Use Policy. Specifically, vendor must respect MEDSIR confidential information and use it for the sole purpose of providing the services contracted.

   b. Vendors must encrypt MEDSIR data at rest and in transit using industry standard encryption.

   c. Vendors must securely delete or return all MEDSIR data upon contract termination, depending on the nature of the data and service contracted.

c) Network security:

   a. Vendors must implement firewalls, intrusion detection/prevention systems, and other network security controls.

b. Remote access to MEDSIR systems must use secure VPN connections.

c. Vendor will employ network segmentation to protect sensitive environments if risks so recommend it and will be able to justify when this was not done.

d. Vendor must disable manufacturer-supplied defaults for system passwords and security parameters

d) Vulnerability management:

a. Vendors must regularly patch and update all systems processing MEDSIR data.

b. Conduct vulnerability scans and penetration tests at least annually.

c. Vulnerability scans and penetration tests must be conducted at least annually.

e) Incident response and business continuity:

a. Vendors must have a documented incident response plan.

b. Security incidents impacting MEDSIR data must be reported within 24 hours to the organization (itsupport@medsir.org).

c. Vendors must develop business continuity and disaster recovery plans.

f) Security awareness and training:

a. Vendors must provide regular security awareness training to all employees and contractors.

b. Vendors must conduct specialized training for personnel with significant security responsibilities.

g) Third-party compliance: Vendor must maintain oversight of supply chain's information security framework.

h) Compliance with the law: Vendors must comply with all applicable laws and regulations, especially data protection and privacy laws.

i) Audits: MEDSIR may conduct security assessments or audits on the vendor with 72 hours' notice.

4. Queries and Violations

Compliance with this policy is required as a condition of doing business with MEDSIR. Therefore, failure to comply with this policy may result in immediate termination of the vendor relationship. Exceptions to this policy require written approval from MEDSIR'S Information Security Manager.

Queries must be addressed to the Information Security Manager at itsupport@medsir.org.