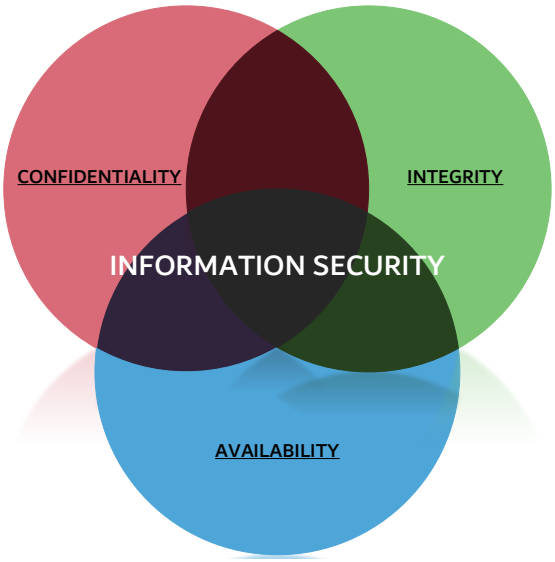
INFORMATION SECURITY POLICY



1. OPERATIVE FRAMEWORK

VisMederi operates in the Life Sciences and Public Health sectors, delivering analytical and scientific services supporting vaccine development and clinical trials. Due to the sensitive nature of its operations — including the processing of patient data, clinical data, proprietary scientific information and confidential customer data — information security is a strategic priority for the organization.
VisMederi applies an integrated Quality Management System (QMS) that includes a fully implemented and certified Information Security Management System (ISMS) based on UNI EN ISO/IEC 27001:2023, EU Regulation 2016/679 GDPR, ICH-GCP, EMA and FDA requirements.
The ISMS ensures the adoption of appropriate technical, organizational and procedural measures, proportionate to risks, threats and regulatory developments.

2. POLICY STATEMENT

The purpose of this Policy is to establish a structured security framework to protect VisMederi information assets from unauthorized access, loss, alteration or destruction, while enabling the Company to effectively support customers in vaccine development and clinical research.
The ISMS safeguards the CIA triad:

- **Confidentiality:** Protection of information from unauthorized or inappropriate access, disclosure or dissemination, including personal data, clinical information and proprietary scientific data;
- **Integrity:** Protection of data accuracy, completeness, traceability, readability, contemporaneousness and validity, in accordance with **ALCOA+** data integrity principles.
- **Availability**: Ensuring that information, systems and services are accessible when required to guarantee business operations, laboratory continuity and service provision.

This policy applies to all employees, collaborators, contractors, consultants, suppliers, partners, and any external entity involved in activities that may impact VisMederi's information security.

3. OBJECTIVES AND PRINCIPLES

VisMederi maintains an ISMS with the following macro-objectives:

- Meeting confidentiality, integrity and availability requirements for information related to business operations, clinical trials, partners and internal personnel.
- Maintaining complete awareness of the information lifecycle and its criticality.
- Ensuring clear allocation of responsibilities for information security.
- Developing and maintaining high awareness and competence in IS security for all personnel.
- Implementing secure access management to prevent unauthorized processing or misuse.
- Ensuring that VisMederi and its third parties adopt adequate levels of protection.
- Ensuring prompt detection, reporting and management of anomalies, vulnerabilities and security incidents.
- Protecting physical environments and critical infrastructures with adequate controls.
- Ensuring legal, contractual and regulatory compliance.
- Preserving business continuity through structured and tested procedures.
- Ensuring continuous improvement of the ISMS and alignment with ISO/IEC 27001:2023.

4. INTEGRATION OF NIS2 REQUIREMENTS

VisMederi acknowledges the applicability of EU Directive 2022/2555 (NIS2) for operators handling critical or sensitive data and implements the following principles:

a. Governance and Accountability

Appointment of responsible roles for cybersecurity and ISMS governance.
Periodic reporting to Top Management regarding risk exposure, incidents, KPIs and compliance.

b. Cybersecurity Risk Management

Annual risk assessment including cyber threats, supply-chain risks and ICT service dependencies.
Documentation and mitigation of risks according to ISO/IEC 27005 and aligned with NIS2.

c. Incident Detection and Reporting

Strengthened monitoring and detection mechanisms (EDPR, SIEM-like processes, logs).
Requirement to report significant incidents within the timelines defined by national CSIRT/ACN.

d. Business Continuity and Disaster Recovery

Updated and tested plans in compliance with NIS2 requirements (resilience, redundancy, fallback mechanisms).

e. Supply Chain Security

Security assessment of critical suppliers and service providers.
Inclusion of IS and cybersecurity clauses in contracts.

f. Policy Review Against NIS2

Annual evaluation of compliance and alignment with ACN guidance.

5. INTEGRATION OF AI ACT REQUIREMENTS

Given the progressive introduction of artificial intelligence tools in corporate processes, VisMederi applies the following principles according to the EU AI Act (2024/2025 applicable requirements):

a. Classification and Register of AI Uses

Identification and assessment of AI systems used internally (e.g., data processing, automation tools, LLMs). Classification according to AI Act risk categories: unacceptable, high-risk, limited-risk, minimal-risk.

b. Controls on High-Risk AI Systems

For any high-risk AI system used in clinical, laboratory or data processing contexts:

- Documentation of training data sources and data governance.
- Validation and monitoring of system performance and bias.
- Logging, traceability and human oversight.
- Periodic conformity assessments.

c. Use of General-Purpose AI (GPAI) and Generative AI

Internal rules restricting use for:

- personal data processing
- confidential or proprietary information
- non-authorized datasets

Requirement of human validation for outputs used in business-critical processes.

d. Transparency and Acceptable Use

Clear communication to personnel regarding acceptable and prohibited uses of AI tools.
Mandatory training on AI-related risks and data protection.

e. Integration into ISMS

AI risk assessment integrated into the ISMS risk management process.
Update of SOPs involving data use, IT systems and cybersecurity.

6. RESPONSIBILITY AND REVIEW OF THE INFORMATION SECURITY POLICY

Management is responsible for:

- Ensuring the ISMS is correctly implemented, updated and resourced.
- Authorizing policy updates based on business changes, new threats, regulatory developments (including NIS2 and AI Act), incidents or critical findings.

The Information Security Policy is reviewed at least annually or whenever relevant changes occur.
The Policy is publish on Vismederi websites and intranet, distributed to:

- internal personnel
- suppliers and third parties where relevant
- customers upon request

7. REFERENCES

- UNI EN ISO/IEC 27001:2023
- UNI ISO/IEC 27002:2023
- EU Regulation 2016/679 GDPR
- EU Directive 2022/2555 NIS2
- EU AI Act (2024–2026)
- EMA Guidance on computerized systems (2023)
- FDA 21 CFR Part 11
- VisMederi SOPs (MDDZ, DPPR, CTSZ, ISMS, ASIL, BCPZ, IMIS, PDBP, etc.)

8. APPROVAL

Full Name	Fabio Vedovi	**Signature and Date**
Role	Head of Quality – Responsible for ISMS and Cybersecurity (ISO/IEC 27001)	Digitally signed by: VEDOVI FABIO Reason: Reason: APPROVAL Date: 06/02/2026 12:08:18

Appendix 1: TECHNICAL AND ORGANIZATIONAL MEASURES (TOMs)

VisMederi implements a comprehensive set of Technical and Organizational Measures (TOMs) designed to ensure the confidentiality, integrity and availability of information, in alignment with ISO/IEC 27001:2023, GDPR, NIS2 Directive and the EU AI Act. These measures are periodically reviewed, tested and improved as part of the ISMS continuous improvement cycle.

1. Information Governance & Data Protection

1.1. Data Classification & Handling

Adoption of a structured data classification model: Strictly Confidential, Confidential, Internal Use, Public. Mandatory handling rules for each class, including storage, transfer, retention and disposal.
Controlled use of removable media; USB storage disabled except for authorized exceptions.

1.2. Data Integrity & Validation

Enforcement of ALCOA+ principles for paper records and electronic data.
Application of CSV (Computer System Validation) requirements for all GxP-relevant systems (EMA 2023, FDA 21 CFR Part 11).

1.3. Data Minimization, Pseudonymization & Anonymization

Application of GDPR-compliant data minimization practices.
Mandatory pseudonymization/anonymization of customer/patient data in analytical activities.

2. Identity, Access & Privilege Management

2.1. Physical Access Controls

Electronic access badges with role-based permissions.
Restricted access to sensitive areas: server rooms, datacenter, archives, laboratories handling confidential data.

2.2. Logical Access Controls

Role-based access control (RBAC) and least-privilege enforcement.
Centralized identity and credential management.
Multi-Factor Authentication (MFA) for VPN, privileged accounts and sensitive applications.

2.3. Admin & Privileged Accounts

Strict segregation between standard users and administrators.
Periodic review of admin accounts and access rights (annual at minimum, NIS2-aligned).

3. Network & Infrastructure Security

3.1. Network Segmentation

Segmented VLAN architecture separating servers, workstations, laboratory devices, IoT/peripherals, guest network and DMZ.

3.2. Perimeter & Internal Network Protection

Firewalls deployed at each company facility, following secure configuration baselines.
EPDR (Endpoint Protection & Detection Response) with automated alerting and reporting.

3.3. Encryption & Secure Transmission

Full-disk encryption on laptops and servers.
Encrypted communication channels for remote access and data transfers.

3.4. Patch & Vulnerability Management

Centralized automated patch deployment.
Periodic vulnerability assessments coordinated with IT and QA.

4. Business Continuity, Availability & Resilience

4.1. Backup Strategy & Redundancy

Multi-location backup strategy: daily, weekly, monthly, yearly backups with integrity verification tests.
Redundant storage for servers and virtual machines (RAID/replicas).
Failover internet connectivity.

4.2. Business Continuity & Disaster Recovery

Business Continuity Plan (BCP) covering critical processes, infrastructures and laboratories.
Periodic BCP/DR drills in accordance with NIS2 expectations.
UPS and generator infrastructure to ensure continuity of critical systems.

5. Cybersecurity Monitoring & Incident Management

5.1. Security Monitoring

Automated logs and security event collection for servers, network devices and EPDR tools.
Periodic manual review of anomalous events, authentication attempts and system alerts.

5.2. Incident & Breach Management

Established procedures for handling Information Security Incidents, Data Breaches and Fraud (aligned with GDPR and supervisory authority reporting timelines).
Structured root cause analysis and CAPA approach for significant events.

5.3. Phishing & Social Engineering Protection

Regular phishing simulation campaigns.
Mandatory training for personnel on cyber hygiene and threat awareness.

6. Secure System Management & Operational Controls

6.1. Change Management

Formal change control process requiring risk assessment, testing and approval.

6.2. Asset Management

Complete asset inventory, including hardware, software, virtual assets and cloud services.
Controlled onboarding/offboarding process for personnel and assigned assets.

6.3. SaaS, Cloud & Third-Party Management

Authorization and monitoring of Cloud/SaaS adoption.
Supplier due-diligence including cybersecurity clauses, following NIS2 requirements.

7. Artificial Intelligence (AI) Governance

7.1. AI System Classification

Registry and classification of AI tools according to AI Act risk categories.
Restriction on high-risk AI unless validated, documented and authorized.

7.2. Use of Generative AI

Strict prohibition on inputting confidential, personal or proprietary information into external AI tools. Mandatory human oversight and validation of AI-generated outputs.

7.3. AI Security & Compliance

Security controls for AI systems integrated into the ISMS risk assessment.
Periodic review of training data governance, bias and transparency requirements.

8. Training, Awareness & Continuous Improvement

Mandatory onboarding training for all employees on ISMS, cybersecurity, privacy and AI risks.
Annual retraining and ad-hoc refreshers after significant changes.
Periodic internal audits and Management Review to evaluate TOM effectiveness and compliance.

END OF DOCUMENT