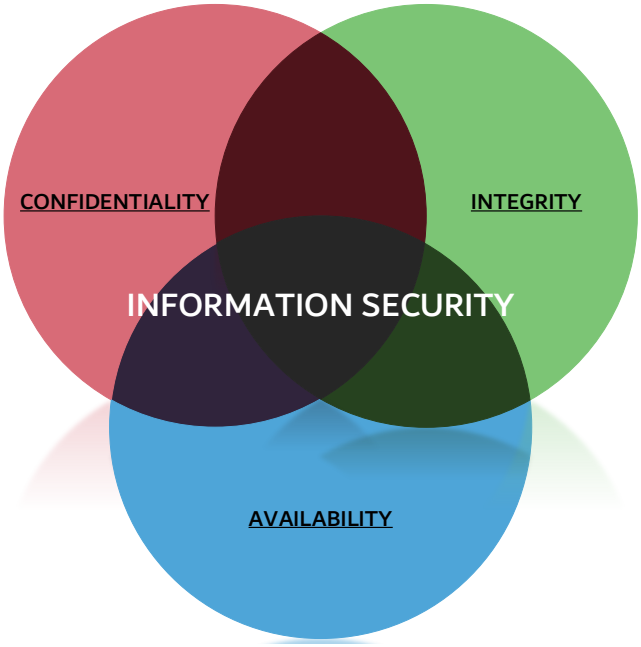
INFORMATION SECURITY POLICY



1. OPERATIVE FRAMEWORK

VISMEDERI is a company that operates in the field of Life Sciences and Public Health performing vaccine's efficacy assessment as part of clinical trial. Given the nature of its activities, information security is a core crucial aspect in which adequate resource are committed with the aim to protect patient sensible data, customer data as well as any other relevant aspect labelled as confidential.
An integrated QMS (Quality Management System) that includes ISMS (Information Security Management System) is applied to all the relevant departments and divisions as to adopt the measures, both technical and organizational, necessary to best guarantee full confidentiality, integrity and availability of information assets as per UNI ISO/IEC 27001, EU Regulation 2016/679 GDPR and Good Clinical Practiced (GCP) requirements.

2. POLICY STATEMENT

The present policy aims to provide a security framework to ensure the protection of VISMEDERI Information from unauthorized access, loss or damage while supporting its Customers on Vaccine Development. Aim of the Information Security Management System is the constant preservation of data:

- **Confidentiality:** processes aiming to protect data from unauthorized access and disclosure, including means for protecting personal privacy and proprietary information;
- **Integrity:** processes aiming to ensure the attributability, accuracy, readability, completeness, contemporaneousness, originality consistency, and validity, endurance of an organization's data. (ALCOA+ principles of Data Integrity);
- **Availability**: processes aiming to ensure that all of business-related data is available to the organization, partners, or end-users at any time of the day, whenever and wherever required.

The present policy applies to all the employees and externals involved within VISMEDERI processes.

3. OBJECTIVES AND PRINCIPLES

The objective of the VISMEDERI ISMS is to ensure an adequate level of data and information security through the identification, assessment and treatment of the risks associated to its services.

The macro-objectives that VISMEDERI intends to achieve with the implementation of the ISMS are:

- Meeting the requirements of confidentiality, integrity and availability of information relating to business, customers, suppliers and internal personnel;
- Guarantee the organization full knowledge of the information managed and the assessment of its criticality, in order to facilitate the implementation of adequate levels of protection;
- Ensure clear allocation of authority and accountability for information security;
- Ensure that internal staff have a high degree of awareness and competence on the subject of information security;
- Ensure secure access to information, so as to prevent unauthorized processing or carried out without the necessary rights;
- Ensure that the organization and third parties collaborate in the processing of information by adopting procedures aimed at respecting adequate levels of security;
- Ensure that the organization and third parties that collaborate in the processing of information, have full awareness of security issues;
- Ensure that anomalies and incidents affecting the information system and corporate security levels are promptly recognized and correctly managed through efficient prevention, communication and reaction systems in order to minimize the impact on the business;
- Ensure that access to the offices and individual company premises takes place exclusively by authorized personnel, to guarantee the safety of the areas and assets present;
- Ensure compliance with legal requirements and compliance with security commitments established in contracts with third parties;
- Ensure the detection of anomalous events, incidents and vulnerabilities of information systems in order to respect the security and availability of services and information;
- Ensure business continuity through the application of established security procedures;
- Ensure compliance with ISO/IEC 27001:2017, and its continuous improvement;
- Ensure compliance with all mandatory, applicable legal Italian regulations;

4. RESPONSIBILITY AND REVIEW OF THE INFORMATION SECURITY POLICY

The Management coordinates and is responsible for the compliance with the principles and the correct implementation of the ISMS, in line with the evolution of the business and the market context; it is also responsible for evaluating any actions to be taken in the face of events such as:

- significant business developments;
- significant changes in the context in which the company operates;
- significant changes with respect to the expectations and needs of the parties involved in the company's activities;
- New threats compared to those considered in the risk analysis activity;
- Significant security incidents;
- Evolution of the regulatory or legislative environment regarding the secure processing of information.

The Information Security Policy is periodically reviewed and updated to ensure its continuous improvement and is shared with internal staff, customers, suppliers and relevant third parties.

5. TECHNICAL AND ORGANIZATIONAL MEASURES (TOMs)

VisMederi appropriately secure data and informations from unauthorized access, loss or damage through the following technical and organization measures in accordance with EU 2016/679 GDPR:

- ✓ Data classification and handling procedure for Documents and Data: (strictly confidential, confidential, internal use, public);
  Ref: MP-MDDZ

- ✓ Customer anonymization
  Ref: MP-MDDZ

- ✓ Adoption of Data Integrity Principle for both, paper documents (ALCOA+) and electronic data (CSV for EMA and FDA CFR 21-part 11 compliance);
  Ref: MP-MDDZ, SOP-CSVZ, GEN-VMPZ

- ✓ Privacy regulations and procedures according to GDPR requirements
  Ref: SOP-DPPR, EU GDPR

- ✓ Data Backup Policy: include three different locations at daily, weekly, monthly, yearly frequency and readability tests
  Ref: SOP-CTSZ

- ✓ Identity and Access Management (IAM) to physical premises: electronic fobs are used to access premises; the management of the permission; (it includes, server rooms, data centers, archives for clinical study, personnel confidential documentation and any other relevant data);
  Ref: SOP-WARZ

- ✓ Identity and Access Management (IAM) to internal servers based on a hierarchical management of user's privileges;
  Ref: SOP-ASIL, SOP CTSZ

- ✓ Physical network security: firewall at each company facility;
  Ref: SOP-CTSZ

- ✓ Business Continuity and Disaster Recovery Plan; including periodic testing;
  Ref: GEN-BCPZ

- ✓ Provision of Uninterruptible Power Supply (UPS) and emergency generator for the continuity of servers and critical equipment;
  Ref: SOP-CTSZ

- ✓ Redundancy: "Availability" for hardware and data storage (internal server data and virtual machines);
  Ref: SOP-CTSZ

- ✓ Redundancy: "Failover" for internet connection;
  Ref: SOP-CTSZ

- ✓ Procedure for the management of incident related to Information Security, Data Breach/Fraud/Withdrawn informed consent, unblinding;
  Ref: SOP-IMIS, SOP-HBMZ, SOP-PDBP

- ✓ Clear Definition of roles and responsibilities of Personnel;
  Ref: SOP-ISMS

- ✓ Encryption policy: laptops and server encrypted;
  Ref: SOP-ISMS

- ✓ Multifactor Authentication (MFA): to access VPN or new devices;
  Ref: SOP-ISMS

- ✓ Network segmentation: for data (DMZ), laptops and lab computers (vLAN 1), external devices (such as printers, scanners, cam, etc.) (vLAN 10), guest (vLAN 20); NAS;
  Ref: SOP-CTSZ

- ✓ Password policy: complexity criteria, re-use, user lock;
  Ref: SOP-ISMS

- ✓ Remote access: via secure VPN through MFA via second authorization channel;
  Ref: SOP-ISMS

- ✓ Data retention policy: lock of USB ports for mass storage drive; general internal data management;
  Ref: SOP-ISMS

- ✓ Clean Desk policy;
  Ref: SOP-ISMS

- ✓ Controlled SaaS and Cloud policy;
  Ref: SOP-ISMS

- ✓ Malicious Code Protection: through a Last Gen EPDR Antivirus and deprivation of user privileges on personal laptops and lab workstations;
  Ref: SOP-ISMS SOP-ASIL

- ✓ Automatic patching governed centrally by the IT;
  Ref: SOP-ISMS

- ✓ Acceptable use policies (AUPs): for email, websites, networks, data, etc.;
  Ref: SOP-ISMS

- ✓ Periodic phishing assessment to the internal/external personnel;
  Ref: SOP-ISMS

- ✓ Admin Management
  Ref: SOP-ISMS

- ✓ *Periodic Management review*
  Ref: SOP-LAPZ

- ✓ Continuous training to internal/external employees and periodic assessment against ISO/IEC 27001 requirements
  Ref: SOP-ISMS

- ✓ Employee on/offboarding and periodic alignment;
  Ref: SOP-ASIL

REFERENCES

- ❖ UNI EN ISO/IEC 27001: Information Security Requirements
- ❖ European Regulation 2016/619 GDPR
- ❖ EMA EMA-CHMP-ICH-135-1995 - Guideline for good clinical practice E6
- ❖ EMA/INS/GCP/112288/2023 Guideline on computerized systems and electronic data in clinical trials
- ❖ FDA-2003-D-0143 Guidance for Industry Part 11, Electronic Records; Electronic Signatures – Scope and Application CFR Code of Federal Regulation – Title 21
- ❖ MP-MDDZ "Management of Documents and Data" – VisMederi SOP
- ❖ SOP-DPPR "Data Privacy Protection Regulation" – VisMederi SOP
- ❖ SOP-CTSZ "Computer Technology System" – VisMederi SOP
- ❖ SOP-WARZ "Working Areas" – VisMederi SOP
- ❖ SOP-ASIL "Asset identification and Labelling" – VisMederi SOP
- ❖ SOP-LAPZ "Leadership and Planning" – VisMederi SOP
- ❖ GEN-BCPZ "Business Continuity Plan" – VisMederi Quality Document
- ❖ SOP-IMIS "Incident and Accident Management" – VisMederi SOP
- ❖ SOP-HBMZ – Handling of Biological Materials – VisMederi SOP
- ❖ SOP-ISMS – Information Security Management System – VisMederi SOP
- ❖ SOP-PDBP - Personal Data Breach and Cooperation with the Supervisory Authority – VisMederi

APPROVAL

Full Name	Fabio Vedovi
Role	Head of Quality – Responsible for ISMS and Cybersecurity (ISO/IEC 27001)
Signature & Date	Digitally signed by: VEDOVI FABIO Reason: Approval Date: 12/10/2023 10:33:53