POLICY

Document No.	Document Name
P90-003	**INFORMATION SECURITY COMMITMENT**

1 PURPOSE

This policy outlines the commitment of Methinks to protecting the confidentiality, integrity, availability, authenticity and traceability of all the physical and electronic information assets throughout the organization in order to preserve business functionality, profitability, customer confidence, legal, regulatory and contractual compliance. This requires everybody to be engaged, to understand their responsibilities and to be empowered to take action in upholding this commitment.

2 SCOPE

This policy applies to all employees, contractors, vendors, and any other parties who access, process, store, or manage the organization's information assets. It encompasses all forms of information, including digital, physical, and intellectual property.

3 REFERENCES

- ISO 27001:2022 – Section 5.2, 5.3 - Information Security Management System Requirements.
- ISO 27002:2022 - Information security, cybersecurity and privacy protection — Information security controls
- UNE-EN ISO /IEC 27001:2023/A1 - Information security, cybersecurity and privacy protection – Information security management systems Requirements - Amendment 1: Climate action changes
- Esquema Nacional de Seguridad (ENS) as regulated by Real Decreto 311/2022
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (hereinafter, "GDPR"), as well as with Organic Law 3/2018 of 5 December on the Protection of Personal Data and Guarantee of Digital Rights ("LOPDGDD")
- Health Insurance Portability and Accountability Act (U.S. HIPAA regulations)

4 DEFINITIONS

Acronym/Term	Definition
ISMS	Information Security Management System
SaMD	Software as a Medical Device, as defined by the International Medical Device Regulators Forum (IMDRF).
ENS	Esquema Nacional de Seguridad, the Spanish National Security Framework.

5 RESPONSIBILITIES

Role	Responsibilities and Authorities
CEO	• Ensure the availability of resources for the implementation and compliance with this policy. • Ensure that the Information Security Policy is available for all the interested parties.
Senior QA/RA Manager, Technical Manager and System Administrator	• Oversee the implementation and maintenance of the ISMS, ensuring alignment with ISO 27001 and ENS requirements. • Review and update the ISMS to address emerging threats and regulatory changes

6 RELATED DOCUMENTS

- WF90-020 – Master Document Register
- SOP42-001 - Document Control and Records Management
- 20211116 - Methinks Roles and Responsibilities
- SOP56-001 - Management Responsibility and Review
- SOP82-001 - Internal Audit
- SOP85-001 - Corrective and Preventive Action
- WF90-007 Information Security Objectives
- METHINKS Procedure Data Security Breach - June 2025
- P90-002 ISMS Scope
- SOP90-003 System Categorization
- P90-008 - ISMS Non conformities
- P90-007 - Information Security Awareness and Training
- P90-017 - Information Security Incident Management

7 PROCEDURE

7.1 PRINCIPLE

Methinks Software is committed to provide innovative, safe and high quality products with excellent after-sales services to meet and/or exceed customer expectations. Our information security is managed based on:

- **Risk:** Identifying, assessing, and mitigating risks to information assets.
- **Legal and Regulatory Requirements:** Ensuring compliance with ISO 27001, GDPR, HIPAA.
- **Business Need:** Aligning security efforts with the strategic objectives of the organization.

This commitment extends to ensuring the confidentiality, integrity, availability, authenticity, and traceability of all information, particularly sensitive health data, in compliance with ENS Article 5.

7.2 CHIEF EXECUTIVE'S STATEMENT OF COMMITMENT

The protection of information is a board-level priority. Methinks' senior management is committed to safeguarding the confidentiality, integrity, availability, authenticity and traceability of all physical and electronic information assets across the organization. This commitment ensures business continuity, profitability, customer trust, and compliance with legal, regulatory, and contractual obligations.

Our Information Security Management System (ISMS) aligns with Methinks' strategic goals, serving as a foundation for secure information sharing, electronic operations, and the mitigation of information-related risks to acceptable levels. Methinks ensures security measures are proportionate to the impact of information systems and complies with required regulatory audits, in accordance with ISO 27001, GDPR, HIPAA, and ENS.

Just like any other critical asset, the data we manage and the infrastructure that supports it must be protected. Therefore, the company is dedicated to the implementation and continuous improvement of an effective ISMS.

The ISMS establishes minimum security standards applicable to all information systems and the processes that support them. It also assigns key responsibilities to managers, who must ensure compliance within their areas of oversight. This approach maintains a balance between fostering an open and collaborative

environment, where information is accessible to employees with limited exceptions; while protecting our data from unauthorized access, loss, alteration, or disclosure.

Our commitment is demonstrated through:

- Establishing and maintaining appropriate control of our processes and activities
- Providing adequate resources to implement and maintain an effective information security management system (ISMS), in accordance with ISO 27001, GDPR, HIPAA and ENS.
- Continually improving our ISMS to respond to emerging threats and business changes and regulatory requirements, as mandated by ISO 27001 Clause 5.2.
- Complying with applicable requirements related to information security.
- Setting measurable quality objectives at key functions and ensuring those objectives are met.

We ensure these commitments are adopted throughout the organization and reviewed on a regular basis for suitability.

This statement is available through our public website for all personnel who carry out work on behalf of Methinks including Methinks personnel, consultants, contractors, as well as people and entities that have a direct interest in the Information Security Management System of Methinks.

Methinks' Information Security Policy is implemented through the Information Security Management System.

7.3 INTRODUCTION

Information is a critical asset of Methinks. The security of this information is vital to maintaining the trust of our stakeholders and ensuring operational continuity. This policy sets the foundation for our ISMS and defines the organization's approach to managing information security. By having an effecting information management system, we can:

- Provide assurances for our legal, regulatory, and contractual obligations
- Ensure the right people have the right access to the right data at the right time
- Provide protection of personal data as defined by the GDPR and ENS.
- Be good data citizens and custodians

7.4 INFORMATION SECURITY OBJECTIVES

Our information security objectives are to:

1. Protect sensitive information from unauthorized access and disclosure, ensure the integrity of information to maintain its accuracy and reliability and guarantee the availability of information when needed for business operations, while ensuring authenticity and traceability.
2. Provide the resources required to develop, implement and continually improve the information security management system.
3. Effectively manage third party suppliers who process, store or transmit information to reduce and manage information security risks.
4. Implement a culture of information security and data protection through effective training and awareness.

For more details refer to **WF90-007 Information Security Objectives (DOC-1756)**.

7.5 INFORMATION SECURITY DEFINED

Information security is defined as preserving:

1. **Confidentiality:** Information is accessible only to authorized individuals.
2. **Integrity:** Safeguarding the accuracy and completeness of information.
3. **Availability:** Information is available when needed.
4. **Authenticity**: Ensuring the information is genuine and its source is verified.
5. **Traceability**: Maintaining records of information access and changes.

7.6 INFORMATION SECURITY POLICY FRAMEWORK

Methinks' topics specific policies are defined and available through Greenlight Guru. For further details refer to **SOP42-001 - Document Control and Records Management (DOC-18)**. Methinks' topic-specific policies are defined and available through Greenlight Guru. The complete list of controlled documents related to the ISMS is maintained in **WF90-020 – Master Document Register (DOC-2385)**.

7.7 INFORMATION SECURITY ROLES AND RESPONSIBILITIES

Information security is the responsibility of everyone to understand and adhere to the policies, follow process and report suspected or actual breaches. Specific roles and responsibilities for the running of the information security management system are defined in the **20211116 - Methinks Roles and Responsibilities (DOC-98)** document.

Specific roles related to ENS are defined and numbered:

- Service Manager (Responsable de la Información): Senior QA/RA Manager
- Security Manager (Responsable de Seguridad): Technical Manager
- Information Manager (Responsable de la Información): System Administrator
- System Manager (Responsable de Sistema): System Administrator.

Due to the current organizational structure and resource constraints, the roles System Manager (Responsable de Sistema) and Information Manager (Responsable de la Información) are assigned to the same individual (System Administrator). This consolidation is justified by the following compensatory measures:

1. Clear Role Definition: The responsibilities of each role are distinctly documented in the job description and internal policies to avoid ambiguity and ensure accountability.
2. No Hierarchical Conflict: The individual does not hold hierarchical authority over the Security Manager or Service Manager, preserving independence in decision-making and oversight.
3. Oversight Mechanisms: Security-related decisions and implementations are subject to periodic review by the Security Manager and internal audit processes.
4. Documentation and Traceability: All actions related to system configuration, maintenance, and incident response are logged and traceable, ensuring transparency and compliance.
5. Training and Certification: The individual holds relevant qualifications and receives ongoing training in cybersecurity and ENS compliance.

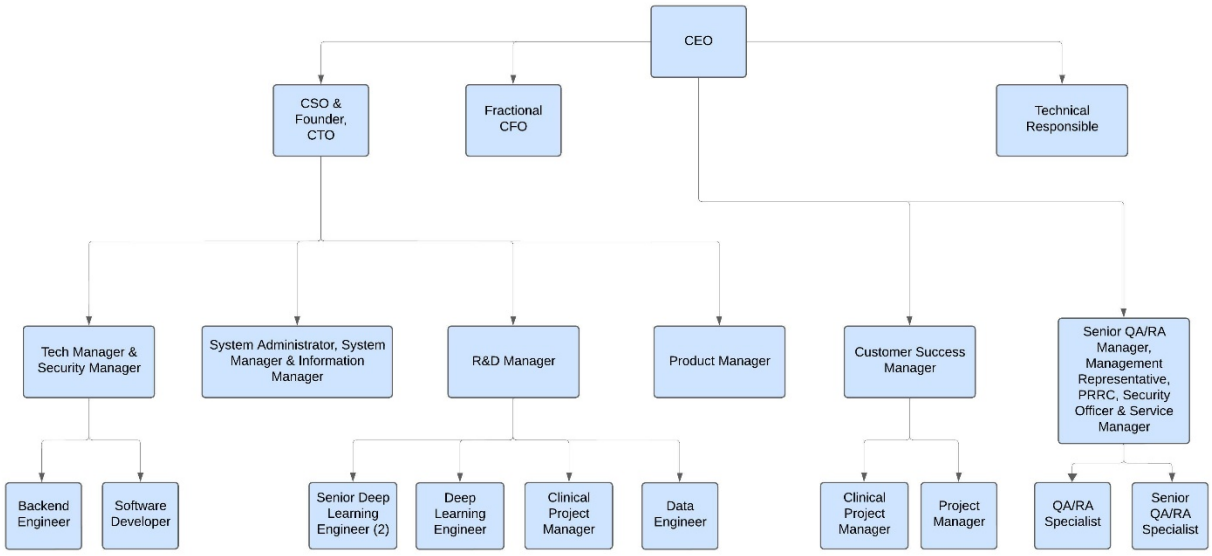
This arrangement is temporary and will be reevaluated annually to ensure continued alignment with ENS principles and organizational needs.

These individuals will also be part of the Information Security Committee, together with the Senior QA/RA Specialist. The Information Security Committee is meeting periodically, with a scheduled meeting at least once per month.

The roles and responsibilities of the Information Security Committee are:

- Coordination of ISMS activities across departments.
- Monitoring and review of key ISMS indicators (KPIs)
- Oversight of improvement actions, OFIs, and CAPAs.

The organizational chart is shown below:



7.8 MONITORING

Information security performance will be monitored regularly through:

- Audits and assessments.
- Analysis of incidents and near misses.
- Periodic management reviews.

For further details please refer to **SOP82-001 - Internal Audit (DOC-23), SOP56-001 - Management Responsibility and Review (DOC-19), P90-017 - Information Security Incident Management (DOC-2110)**, **and METHINKS Procedure Data Security Breach (DOC-787)** and **P90-008 - ISMS Non conformities (DOC-1991).**

7.9 LEGAL AND REGULATORY OBLIGATIONS

The organization is committed to complying with all relevant legal, regulatory, and contractual requirements, including GDPR, HIPAA, ISO 27001 standards, and ENS. These requirements are recorded using the document **WF-003 List of Applicable Regulations Guidance Documents (DOC-319)**.

7.10 TRAINING AND AWARENESS

All personnel will receive regular training to ensure they understand their information security responsibilities and are aware of emerging threats and best practices according to **P90-007 - Information Security Awareness and Training (DOC-1769)**. Training needs are identified, and relevant training requirements are captured in the document **WF62-004 Training Matrix (DOC-97)**

7.11 CONTINUAL IMPROVEMENT OF MANAGEMENT SYSTEM

Our ISMS is subject to continual improvement through:

- Regular management reviews.
- Feedback from audits and assessments.
- Analysis of incident trends and risk assessments.

The **SOP56-001 - Management Responsibility and Review (DOC-19)** sets out the company approach to continual improvement and there is a continual improvement process in place. For further details please refer to **SOP56-001 - Management Responsibility and Review (DOC-19)** .

7.12 POLICY COMPLIANCE

7.12.1 Compliance Measurement

Compliance with this policy will be measured through:

- Regular internal and external audits.
- Performance metrics.
- Incident analysis.
- Business tool reports
- Feedback to the policy owner

7.12.2 Exceptions

Exceptions to this policy must be formally documented, reviewed, and approved by senior management and reported to the Management Review Team.

7.12.3 Non-Compliance

Non-compliance will result in corrective actions, which may include training, disciplinary measures, or termination of access to information assets or employment.
For more details please refer to **SOP85-001 - Corrective and Preventive Action (DOC-9)**.

7.12.4 Continual Improvement

Annually, the policy is reviewed and updated (as necessary) as part of the continual improvement process, ensuring alignment with ISO 27001, ENS, and emerging regulatory requirements.

P90-003 - Information Security Commitment (DOC-1755) Ver. 5

Approved By:

(CO-931) Update of ISO 27001 Procedures IV

Description

The following procedures have been updated: * P90-001 - Context of Organisation (DOC-1752), Section 7.3: according to ISO 27001:2022/A1:2023, the following risk has been added to reflect the climate change topic specific document:"Climate Changes Climate change may indirectly affect Methinks' information security environment through environmental disruptions such as extreme weather events, energy supply instability, or impacts on critical infrastructure. These factors could potentially affect the availability of cloud services, internet connectivity, or physical facilities supporting company operations. As Methinks relies primarily on cloud-based infrastructure (e.g., Microsoft Azure), environmental risks related to climate change are largely managed through the resilience, redundancy, and disaster recovery capabilities implemented by the cloud service providers. At present, climate change is not considered a direct or high-impact issue for the organization's ISMS. However, it is monitored as part of the external context of the organization and may be reassessed if environmental risks begin to affect operational continuity, infrastructure reliability, or regulatory expectations.". * P90-003 - Information Security Commitment (DOC-1755), Section 7.6: the following has been added: "Methinks' topic-specific policies are defined and available through Greenlight Guru. The complete list of controlled documents related to the ISMS is maintained in WF90-020 – Master Document Register. " Consequently, the WF90-020 - Master Document Register has been uploadced as well as the corresponding record (20260306 - Master Document Register). * P90-002 - ISMS SCOPE (DOC-1754), section 7.1: The following has been added: Spanish (SPA) El alcance del Sistema de Gestión de Seguridad de la Información (ISMS) de Methinks incluye todos los procesos, sistemas, activos y personal relacionados con la entrega y gestión de los productos software, incluyendo procesos clave como el diseño y desarrollo de software, pruebas, distribución, instalación y despliegue, soporte y gestión del cumplimiento regulatorio. El ISMS garantiza que los riesgos de seguridad de la información se gestionan de acuerdo con ISO 27001:2022 y el Esquema Nacional de Seguridad (ENS), protegiendo la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de toda la información dentro del alcance, especialmente los datos sensibles de salud procesados por el Software como Dispositivo Médico (SaMD) de Methinks. La implementación de controles se detalla en WF90-009 – Declaración de Aplicabilidad (DOC-1926) y se adapta a las categorizaciones del sistema (Básico, Medio, Alto) según los artículos 40–41 del ENS para proteger toda la información crítica. El alcance está determinado por los factores internos y externos de la organización, así como por los requisitos de las partes interesadas (para más detalles, véase P90-001 – Contexto de la Organización (DOC-1752)). * 20251009 - Internal Audit Plan Form (DOC-2000), Section Audit methods: The following has been added: "Internal audits are conducted through a combination of document review, interviews with relevant personnel, and observation of activities where applicable. The audit approach is based on sampling of the organization's activities and records, with the objective of evaluating the fulfilment of the requirements of ISO 27001:2022 and other applicable normative documents, as well as confirming the conformity, effectiveness, and continued relevance of the Information Security Management System (ISMS) within the defined scope. As the audit process is based on sampling techniques, the audit findings and conclusions represent the activities and records reviewed during the audit and do not necessarily include all possible issues within the management system." * SOp82-001, the following has been added: Audit methods, including sampling of documentation, on-site or remote audit activities, and the review of Annex A controls in the case of ISMS audits where the audit criteria includes ISO/IEC 27001 (when applicable);

Justification

These updates were implemented following observations raised during the ISO 27001 Stage I audit. The purpose of the changes is to improve alignment with ISO 27001:2022 requirements and Amendment 1 (Climate Action), as well as to enhance the clarity, completeness, and traceability of ISMS documentation. Specifically, the updates address: - The explicit consideration of climate change as an external issue within the organizational context in accordance with ISO 27001:2022/A1:2023. - The identification of WF90-020 – Master Document Register as the central reference for controlled ISMS documentation. - The inclusion of the ISMS scope in Spanish to complement the English version and improve accessibility and clarity of the scope definition. - The clarification of the internal audit methodology, including the use of sampling techniques, within the Internal Audit Plan to ensure transparency of the audit approach. These updates do not modify the scope or operation of the ISMS but strengthen documentation alignment with ISO 27001 requirements and audit expectations.

Assigned To:	Initiated By:	Priority:	Impact:
Anna Jordà	Anna Jordà	Medium	Critical

Version History:

Author	Effective Date	CO#	Ver.	Status
Anna Jordà	March 16, 2026 3:21 PM CET	CO-931	5	Published
Adrián Alvarez	January 8, 2026 2:57 PM CET	CO-840	4	Superseded
Anna Jordà	November 25, 2025 9:38 AM CET	CO-815	3	Superseded
Anna Jordà	October 29, 2025 11:25 AM CET	CO-755	2	Superseded
Anna Jordà	October 13, 2025 11:03 AM CEST	CO-719	1	Superseded
Anna Jordà	July 2, 2025 1:00 PM CEST	CO-632	0	Superseded