Artificial Intelligence Policy

Your Partner for IT Security & Compliance

Valeri Milke & Koral Yücel

Datum: 29.05.2025

Document History

Version	Date	Type of Activity	Author
0.1	29.05.2025	Initial Creation	Koral Yücel
1.0	30.05.2025	Final	Valeri Milke

Document Information

Document Classification	Public
Author(s)	Koral Yücel
Version	1.0
Status	In Progress

Table of Content

1. Introduction

1.1. Purpose of the Policy

At VamiSec GmbH, we recognize the transformative potential of artificial intelligence (AI) to enhance the quality, efficiency, and impact of our consulting services and internal operations. This Policy articulates our commitment to the responsible use, advisory, and integration of AI technologies. It ensures that AI systems are developed, assessed, and deployed in alignment with ethical principles, clearly defined risk thresholds, and applicable legal and regulatory requirements, including the EU AI Act and ISO/IEC 42001:2023.

This policy serves as the cornerstone of our Artificial Intelligence Management System (AIMS) and defines the high-level governance structure for how AI is approached across our organization. It reflects our intent to balance innovation with accountability, and to ensure that the design, selection, and recommendation of AI systems meet the standards of transparency, fairness, privacy, and trust.

ISO 42001 provides a holistic, organization-wide governance framework that integrates best practices throughout the entire AI lifecycle — from design and development to deployment, monitoring, and decommissioning.

1.2. Objective

The objective of this policy is to define the foundation for an ISO 42001-compliant Artificial Intelligence Management System (AIMS). This includes:

- Establishing a documented, organization-wide commitment to ethical, secure, and transparent AI use.
- Ensuring that AI systems are aligned with internal strategic objectives and external regulatory expectations.
- Providing clear governance over AI risk management, data handling, and algorithmic transparency.
- Supporting continuous improvement and compliance with evolving legal and technological developments.
- Strengthening stakeholder trust and accountability through structured policies, roles, and controls.

This policy forms the backbone of the organization’s AI governance and risk management framework.

1.3. Compliance with Normative and Regulatory Requirements

The policy of VamiSec GmbH is aligned with the requirements of ISO/IEC 42001:2023, as well as applicable legal and regulatory frameworks governing the ethical and secure use of Artificial Intelligence. The following key frameworks are integrated into the AI Management System (AIMS):

- **ISO/IEC 42001:2023**[1]: Serves as the structural foundation for the organization's Artificial Intelligence Management System (AIMS), providing a recognized framework for the responsible governance, implementation, and continual improvement of AI systems.
- **EU General Data Protection Regulation (EU-GDPR)**[2]**:** Sets binding legal rules for the protection of personal data across the European Union, ensuring lawful, fair, and transparent processing, especially in AI contexts involving personal data.
- **EU Artificial Intelligence Act (EU AI Act)**[3]**:** Establishes the regulatory basis for the trustworthy and risk-based use of AI systems within the EU. It defines requirements for transparency, risk classification, accountability, and oversight to safeguard both individual rights and societal interests.

VamiSec GmbH continuously monitors legal and normative developments to ensure that its AI Policy remains up to date, auditable, and consistent with global best practices.

1.4. Context

This policy is considered a high-level strategic document within the company's governance and documentation framework. It reflects internal priorities as well as external legal and regulatory requirements, aligning with applicable standards and organisational principles.

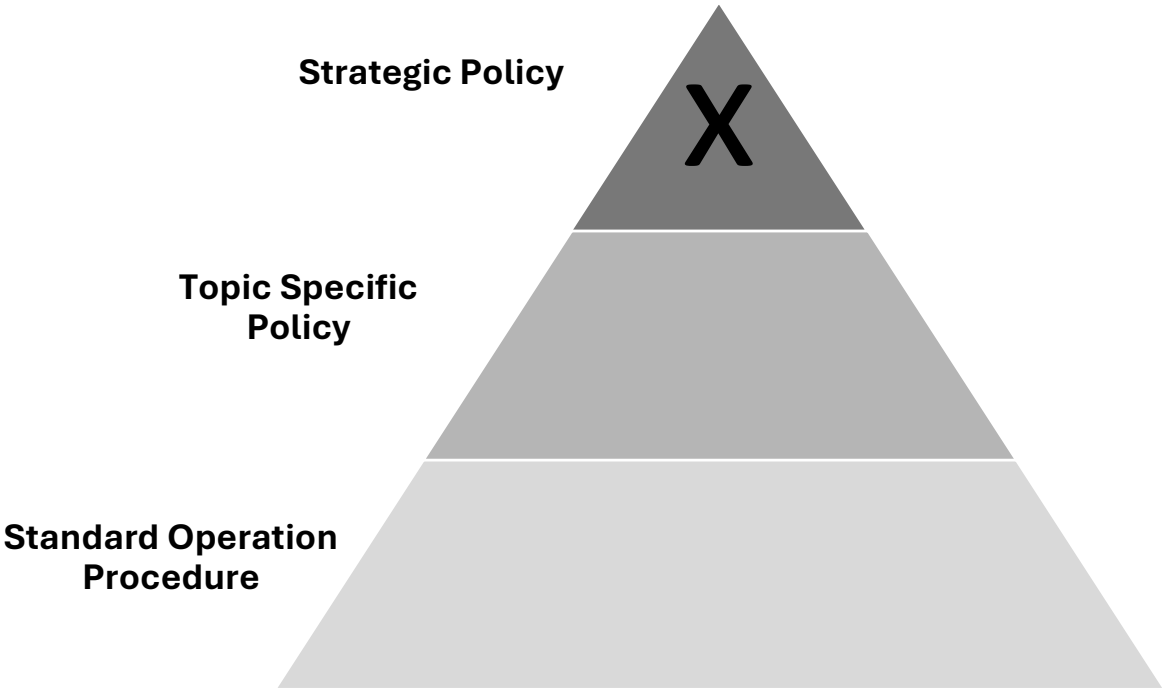
VamiSec GmbH operates in a dynamic environment shaped by rapid technological progress, evolving client demands, and increasing regulatory oversight. As artificial intelligence becomes more embedded in business processes, responsible and transparent AI use is essential for maintaining trust, ensuring compliance, and gaining competitive advantage. This policy supports a consistent and structured approach to managing AI across the organisation.

1.4.1. Document Hierarchy

This AI Policy is a core document of the Artificial Intelligence Management System (AIMS) at VamiSec GmbH. It defines the organization's strategic direction for the governance and responsible use of AI technologies.

Within the company's document architecture, this policy is classified as a strategic, high-level policy, forming a foundational layer of the AIMS. It provides overarching principles and requirements to govern the responsible use, integration, and oversight of AI systems, guiding the development and improvement of related operational controls, including procedures, standards, and technical documentation.

[1] ISO/IEC 42001:2023
[2] EU General Data Protection Regulation (EU-GDPR)
[3] EU Artificial Intelligence Act (EU AI Act)



1.5. Scope

This AI Policy applies to all departments, employees, and organizational units of VamiSec GmbH. It covers the responsible use, procurement, and governance of artificial intelligence (AI) systems across all business processes and services.

The scope includes all AI tools, platforms, and services used or managed by the company, regardless of whether they are developed internally or procured externally. It extends to all physical and virtual environments, including office locations and remote work settings.

Any exclusions or limitations must be explicitly justified, formally approved by management, and clearly documented. Regular reviews ensure the scope remains appropriate and up to date in accordance with the continuous improvement of the AI Management System (AIMS).

2. Terms and Definitions

Understanding key terms is vital for the consistent application of this policy. The following definitions apply:

Term	Definition
Artificial Intelligence (AI)	▪ The capability of a system to perform tasks that would typically require human intelligence, such as learning, reasoning, or decision-making.
AI Management System (AIMS)	▪ A structured framework of policies, processes, and procedures used to ensure effective governance, control, and continual improvement of AI-related activities.
High-Risk AI System	▪ AI systems classified as high-risk according to the EU AI Act and internal risk assessments due to their potential impact on individuals, fundamental rights, or society.
Stakeholder	▪ Any person or organization that may affect, be affected by, or perceive themselves to be affected by AI systems used or provided by the organization.

3. Roles and Responsibilities

Effective AI governance requires a clear allocation of roles and responsibilities. The following outlines the key functions involved in the management of AI systems:

Role	Responsibilities
Employees and Contractors	▪ Are required to follow the AI Policy and associated procedures. They are responsible for participating in mandatory AI awareness and training programs and for promptly reporting any concerns or incidents involving AI systems.
Top Management	▪ Provides strategic direction and oversight for the AIMS. They ensure that the AI Policy and defined AI Objectives are aligned with the organization's strategic vision, allocate sufficient resources for implementation, and ensure compliance with applicable legal and regulatory requirements. They also foster a culture of ethical and responsible AI use.
AI Officer	▪ Is responsible for the coordination, implementation, and ongoing maintenance of the AIMS. This includes ensuring adherence to the AI Policy and relevant legal obligations, managing AI risk and impact assessments, regularly reporting on AIMS effectiveness to Top Management, and reviewing and updating internal AI-related policies as needed.

4. Responsible AI Use and Governance

Our commitment to responsible AI is founded on a set of core principles and governance commitments that guide our AI practices. VamiSec GmbH actively uses Artificial Intelligence technologies, including generative AI tools such as large language models and conversational systems, to enhance internal processes and client-oriented services. We recognize the associated risks and opportunities, and ensure that all AI systems are deployed transparently, ethically, and securely. VamiSec GmbH is committed to the continual improvement of its AI Management System (AIMS) in line with applicable regulations, emerging technologies, and evolving business objectives.

4.1. Core Principles

We are dedicated to upholding the following fundamental principles in all AI-related activities at VamiSec GmbH:

Core Principle	Implementation
Transparency and Explainability	▪ We strive to ensure that our AI systems — including generative models and chatbots — are transparent and that their decision-making processes are explainable. This means providing clear and accessible information about how AI systems operate, enabling stakeholders to understand and trust the outcomes.
Fairness and Non-Discrimination	▪ We are committed to developing and using AI systems that are free from unfair bias and do not discriminate against individuals or groups. We implement technical and procedural measures to detect and mitigate biases and regularly evaluate AI outputs to ensure fairness and inclusivity.
Human Oversight	▪ Maintaining appropriate human oversight over AI systems is essential, especially for high-risk or sensitive applications. We ensure that AI technologies support human decision-making and never override critical human judgment in core business or advisory processes.
Technical Robustness and Safety	▪ We ensure that the AI systems we use or recommend are dependable

	secure, and resilient. As part of our consulting services, we evaluate AI solutions for functional integrity, conduct due diligence on reliability and testing practices, and consider cybersecurity safeguards to minimize risks and vulnerabilities for our clients and internal use.
Privacy and Data Governance	▪ We respect privacy and process personal data in accordance with the General Data Protection Regulation (GDPR) and other applicable laws. Strong data governance ensures that all AI systems operate on high-quality, lawfully obtained, and well-managed data.
Environmental Sustainability	▪ We recognize the ecological footprint of AI technologies and promote energy-efficient, sustainable practices in the selection, recommendation, and use of systems. As a consulting organization, VamiSec GmbH advises clients on sustainability risks and encourages the adoption of environmentally responsible AI solutions across the lifecycle. AI
Accountability	▪ We establish clear accountability for all AI systems in use. Roles and responsibilities are defined within the AI Management System (AIMS), and all key decisions and system actions are documented to ensure traceability, compliance, and oversight.

5. Risk Environment and Management Commitments

The use of Artificial Intelligence (AI) at VamiSec GmbH introduces a dynamic and evolving risk landscape. These risks may arise from the integration of third-party AI tools, limited transparency of AI models, data quality issues, ethical considerations, and compliance challenges related to emerging regulatory frameworks. VamiSec GmbH recognizes that AI-specific risks may affect individuals, clients, or society at large. These include unintended bias, lack of explainability, security vulnerabilities, or regulatory non-compliance. Over-reliance on automated outputs without appropriate human oversight can further increase exposure.

The AI risk environment is shaped by factors such as:

- Rapid technological development and shifting industry standards
- Uncertainty in regulatory frameworks (e.g., EU AI Act, ISO/IEC 42001)
- Dependence on external AI providers and cloud-based platforms
- Complexity and limited interpretability of some AI models
- The operational use of generative AI systems and chatbots in both client and internal contexts
- Variability in client-specific requirements, data quality, and privacy expectations in consulting engagements

To address these risks, VamiSec GmbH applies structured risk management practices in both its internal AI use and its advisory services, as part of the AI Management System (AIMS). Risk identification, evaluation, and control activities are conducted regularly and reviewed as part of the AIMS improvement cycle.

5.1. Commitment to Impact Assessment

We support and conduct AI System Impact Assessments (AIIAs) for high-risk AI systems—whether used internally or assessed for clients. These evaluations address ethical, social, and environmental impacts and serve as a foundation for risk mitigation and responsible recommendations.

Risk-Based Approach:

A risk-based approach is used to allocate attention and controls proportionally. AI systems are classified according to the risk levels defined in the EU AI Act. We focus on identifying and managing high-risk use cases, both in our internal operations and client-facing work.

Stakeholder Engagement:

Engaging with stakeholders is essential to understanding expectations and managing concerns. We consult actively with employees, clients, affected parties, and relevant partners to incorporate their perspectives into tool selection, system evaluation, and AI governance strategies.

Supply Chain Governance:

We monitor AI-related risks across our value chain, including technology providers and data processors. We ensure that AI systems used or recommended by VamiSec GmbH align with our ethical principles, legal obligations, and governance expectations.

Incident Management:

Defined procedures are in place for responding to AI-related incidents, whether they occur in our own systems or in client engagements. Incidents are documented, assessed, and escalated as needed. Corrective actions are taken to reduce recurrence and improve risk controls.

Documentation Requirements:

We maintain comprehensive documentation of all AI-related activities, including assessments, evaluations, client advice, and internal use cases. This ensures accountability, traceability, and readiness for audits and regulatory inquiries.

5.2. Governance Commitments

Our governance commitments ensure that all AI-related activities at VamiSec GmbH comply with applicable legal obligations, ethical standards, and internal accountability frameworks. These commitments apply to both our internal use of AI systems and the AI solutions we evaluate, recommend, or support in client environments.

Compliance with Prohibited AI Practices:

VamiSec GmbH refrains from using, recommending, or enabling AI systems that engage in practices prohibited under applicable regulations, such as social scoring, manipulative behavioral targeting, or the exploitation of vulnerabilities in specific groups. We actively assess AI use cases to ensure alignment with these ethical boundaries.

High-Risk Systems Requirements:

Where high-risk AI systems are used internally or addressed in client advisory projects, we apply enhanced oversight measures. These include documentation reviews, transparency checks, human supervision, and monitoring protocols. We ensure that the deployment or recommendation of high-risk systems is accompanied by appropriate risk mitigation and compliance verification steps.

Conformity Assessment Commitment:

VamiSec GmbH supports and, where appropriate, conducts or advises on conformity assessments for high-risk AI systems in line with the requirements of the EU AI Act. These assessments ensure that such systems meet legal, technical, and ethical standards. Our involvement reflects our commitment to high-quality AI governance — both internally and in the services we deliver to our clients.

6. Leadership and Commitment

The executive leadership of VamiSec GmbH is committed to the responsible and transparent use of Artificial Intelligence (AI) across the organization. Top management acknowledges the strategic relevance of AI and the associated risks, and actively supports the establishment, implementation, and continual improvement of the AI Management System (AIMS). Leadership ensures that:

- Adequate resources, competencies, and structures are in place to manage AI-related risks and opportunities,
- Ethical principles and regulatory requirements are integrated into all AI-related activities,
- Roles and responsibilities are clearly defined for the governance and oversight of AI systems,
- Continuous improvement and stakeholder engagement are promoted throughout the AI lifecycle.

The leadership team at VamiSec GmbH demonstrates its commitment through regular reviews, strategic direction, and by ensuring that all employees understand the importance of responsible AI use in their daily work.

7. Awareness and Training

To ensure that all personnel at VamiSec GmbH understand and comply with the AI Policy, we place strong emphasis on structured awareness and continuous training.

Awareness and training are integral components of the AI Management System (AIMS) and support our commitment to the ethical, secure, and responsible use of Artificial Intelligence — including tools such as generative AI (e.g., ChatGPT) and chatbots.

Key elements of our training framework include:

- Regular awareness sessions covering AI ethics, fairness, transparency, accountability, and compliance with applicable legal frameworks (e.g., EU AI Act, ISO/IEC 42001, GDPR)
- Role-specific training for employees involved in the procurement, operation, evaluation, or oversight of AI systems
- Clear guidance on detecting and reporting AI-related incidents, risks, or ethical concerns
- Integration of AI-relevant topics into onboarding processes and professional development activities
- Communication of updates related to regulatory changes, new policies, or relevant incidents involving AI
- Evaluation of training effectiveness through feedback, assessments, and periodic content reviews

All relevant employees, consultants, and contractors are required to complete AI training and act in accordance with the principles and responsibilities defined in the AIMS. The AI Policy and training materials are made accessible to all staff and are continuously improved to ensure alignment with current risks, technologies, and regulatory expectations.

8. Compliance and Enforcement

Maintaining compliance with this policy and applicable legal and regulatory requirements is essential to the integrity and trustworthiness of AI practices at VamiSec GmbH. Compliance is enforced through structured monitoring, auditing, continuous improvement, and corrective measures.

8.1. Monitoring and Measurement

We monitor and evaluate the performance of AI systems and the effectiveness of the AI Management System (AIMS) by:

- Collecting data on AI system performance, legal compliance, and ethical indicators using predefined AI Metrics and documentation templates.
- Conducting regular internal audits in accordance with the Internal Audit Plan, with outcomes documented in formal Audit Reports.
- Performing periodic management reviews, taking into account audit results, stakeholder feedback, and risk or performance metrics.

8.2. Continuous Improvement

VamiSec GmbH is committed to the continual improvement of its AI practices and governance by:

- Addressing identified nonconformities using Nonconformity Reports and Corrective Action Records.
- Updating policies, procedures, and controls based on audit outcomes, feedback, and changes in applicable regulations or standards.
- Logging all improvements and suggestions in the Register of Non-Conformities and Opportunities for Improvement to support accountability and learning.

8.3. Incident Management

In the case of AI-related incidents — including failures, ethical concerns, or misuses — VamiSec GmbH:

- Activates its Incident Response Plan to ensure timely and effective handling.
- Reports significant incidents to regulatory authorities and affected stakeholders, where legally required.
- Conducts root cause analysis and implements corrective measures to prevent recurrence and improve system robustness.

8.4. Non-Compliance

Non-compliance with this AI Policy or applicable regulations is taken seriously. VamiSec GmbH maintains procedures to address such violations:

- Investigations are carried out to determine the scope, causes, and consequences of the non-compliance.
- Corrective actions are applied to resolve the issue and mitigate future risks.

- Disciplinary measures may be taken where appropriate, following internal company rules and in accordance with applicable laws.

9. Exception Handling and Risk Acceptance

VamiSec GmbH defines a structured process for handling exceptions to AI-related policies, procedures, or controls within the AI Management System (AIMS). Exceptions may be granted in justified cases, provided that associated risks are identified, assessed, and formally accepted by authorized personnel. The exception process includes:

- Submission of a documented exception request, including rationale and scope
- Evaluation of potential impacts on security, compliance, ethics, and operational reliability
- Risk assessment including residual risk and mitigation measures
- Formal approval by designated roles (e.g. Risk Owner, Compliance)
- Defined time limits and conditions for exception validity
- Documentation and auditability of all granted exceptions.

Risk acceptance is only permitted if residual risks remain within the defined risk appetite of VamiSec GmbH. All exceptions and accepted risks are reviewed periodically and revoked if conditions change or new information becomes available.

10. Review and Approval

This AI Policy is reviewed at least once per year, or sooner if there are significant changes in VamiSec GmbH's operations, applicable laws and regulations, or relevant industry standards. The objective of the review is to ensure the continued relevance, effectiveness, and compliance of the policy.

The policy must be formally approved by Top Management. All revisions are documented in the Revision History section to ensure traceability. The latest approved version of the policy is communicated to all relevant stakeholders and made accessible through internal platforms and, where applicable, published on the VamiSec GmbH website.

11. Legitimization

This policy comes into effect on 1.7.2025.

12. Further Documents and References

To ensure that all aspects of artificial intelligence governance are consistently managed and maintained within VamiSec GmbH, this policy refers to additional documents that define specific requirements, procedures, and responsibilities related to AI, information security, and regulatory compliance. The following table provides an overview of key reference documents and their respective purposes:

Document	Content/Purpose
AIMS Scope Definition	Definiert den Geltungsbereich des AI Management Systems (AIMS), einschließlich organisatorischer Einheiten, Prozesse, Standorte sowie eingesetzter KI-Systeme innerhalb der VamiSec GmbH