Information Security Policy

Your Partner for IT Security & Compliance

Valeri Milke

Datum: 21.10.2025

Document History

Version	Date	Type of Activity	Author	Approver
0.1	19.03.2025	Initial Creation	Koral Yücel	-
1.0	19.03.2025	Finalization	Koral Yücel	-
1.1	11.06.2025	Addition of Informations Security Goals	Valeri Milke	-
1.1	30.07.2025	Approval completed (author and approver roles separated, legitimization updated)	-	Valeri Milke
1.2	21.10.2025	Policy updated: integration of BSI IT-Grundschutz, inclusion of EU Cyber Resilience Act (CRA) and ISO/IEC 42001:2023 (AI Management System).	Lilia Dorofeeva	Valeri Milke

Document Owner	Valeri Milke
Document Classification	Internal
Author(s)	Koral Yücel
Version	1.2
Status	Final

Table of Content

1. Introduction

1.1. Purpose of the Policy

This Information Security Policy defines the main goals, strategies, and guidelines to ensure that company information is available, confidential, and protected from unauthorized changes. It provides a clear framework for all security-related processes by explaining how information security is managed, monitored, and continuously improved. This policy is the foundation of an effective and long-term Information Security Management System (ISMS).

1.2. Objective

The goal of this policy is to cover all important aspects of information security in the company and to structure them clearly. The key objectives include:

- Building an Information Security Management System (ISMS) that meets the company's business needs and follows legal requirements.
- Information Security Goals
- Leadership and commitment
- Embedding security into the company culture by ensuring clear responsibilities, sufficient resources, and open communication.
- Reducing risks and preventing damage, including financial loss and reputational harm caused by security breaches.
- Ensuring compliance with laws, regulations, and contractual obligations related to data protection and security.
- Continuously improving security processes so that new threats and changes in the business environment are identified and addressed in time.

1.3. Compliance with Normative and Regulatory Requirements

The Information Security Policy of VamiSec GmbH follows the requirements of ISO/IEC 27001:2022 and aligns with the BSI IT-Grundschutz framework issued by the German Federal Office for Information Security (BSI), as well as ISO/IEC 42001:2023 (AI Management System) and other relevant national and international regulations and standards.

This ensures a consistent and harmonized approach to establishing, implementing, maintaining, and continually improving the integrated management system that governs information security, AI governance, and business resilience.

The following frameworks and legal requirements are particularly implemented:

- **ISO/IEC 27001:2022[1]:** ISO/IEC 27001:2022 provides the recognized framework for an Information Security Management System (ISMS).
- **BSI IT-Grundschutz (German IT Baseline Protection)** [2]– Provides a modular and structured approach for identifying and protecting critical assets, threats, and processes.

[1] ISO/IEC 27001:2022
[2] BSI-Standard 200-2

- **ISO/IEC 42001:2023 (AI Management System)** [3]– Specifies requirements for responsible AI governance, risk management, and lifecycle control for AI-enabled processes and data.
- **EU General Data Protection Regulation (EU-GDPR)[4]:** The EU-GDPR sets binding rules across Europe for the protection of personal data.
- **NIS2 Directive (Directive (EU) 2022/2555)[5]:** The NIS2 Directive aims to improve cybersecurity and resilience for operators of essential services and other critical entities in the EU.
- **EU Artificial Intelligence Act (EU AI Act)[6]:** The EU AI Act provides the regulatory foundation for the safe and trustworthy use of Artificial Intelligence in the EU. It defines requirements for transparency, risk management, and oversight of AI systems to protect both individual rights and societal interests.
- **EU Cyber Resilience Act (CRA)** [7]– Defines cybersecurity requirements for digital and AI-enabled products and services across their lifecycle.

1.4. Context

This policy is considered a high-level strategic document within the company's rules and documentation structure. It reflects both internal and external requirements and aligns with existing standards, laws, and internal guidelines.

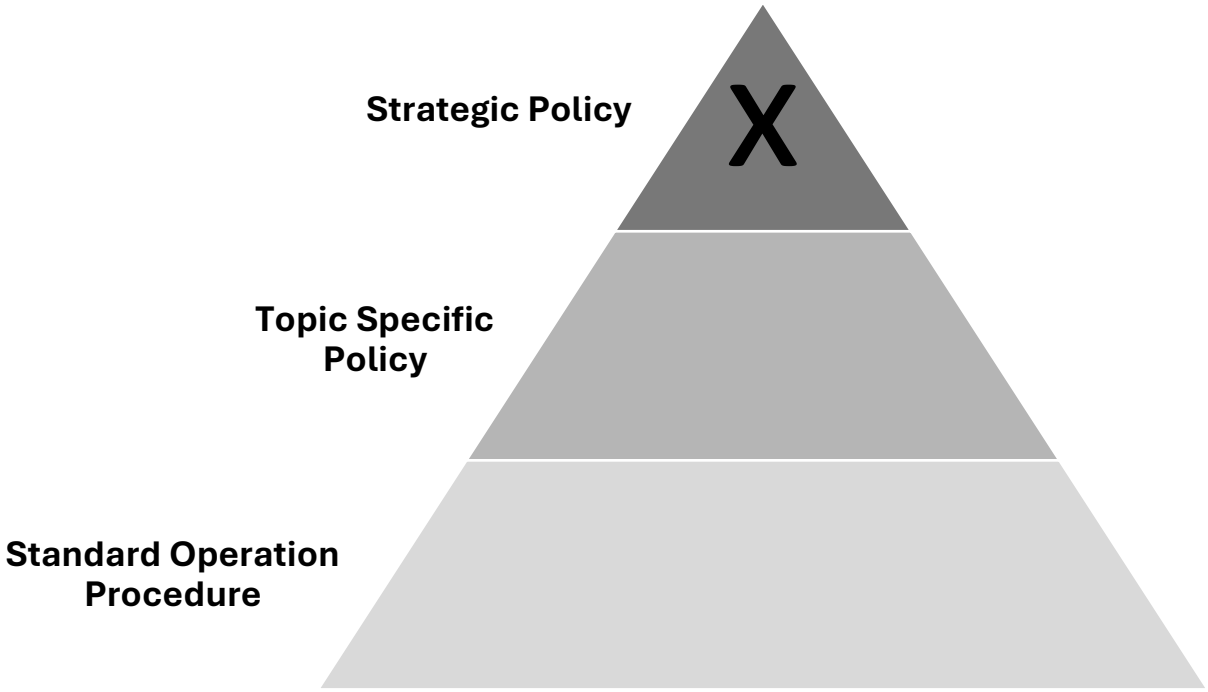
The company operates in a fast-changing environment influenced by technology advancements, shifting customer needs, and regulatory changes. Because many business processes rely heavily on IT services and digital tools, information security is a key competitive factor. To meet the expectations of customers, partners, and regulators, the company must take a consistent and structured approach to security.

1.4.1. Document Hierarchy

Within the company's document structure, this policy is classified as a Strategic Policy under the company's general rules (see Document Hierarchy).

In the ISMS document structure of VamiSec GmbH, this is considered a Strategic Policy.

[3] ISO/IEC 42001:2023
[4] EU General Data Protection Regulation (EU-GDPR)
[5] NIS2 Directive (Directive (EU) 2022/2555)
[6] EU Artificial Intelligence Act (EU AI Act)
[7] EU Cyber Resilience Act (CRA)



1.5. Scope

This policy applies to all business areas, locations, departments, and employees of the company. It also applies to all information, applications, systems, and processes under the company's control.

External service providers and suppliers working on behalf of or in cooperation with the company are also subject to this policy if they handle company information or IT systems.

The focus is on preventing and managing security risks throughout the entire lifecycle of information processing—from planning and procurement to operation, maintenance, modification, decommissioning, and disposal of assets. The specific requirements and processes are outlined in related policies and work instructions.

1.6. Risk Environment

In today's business environment, the company faces many risks, including technical weaknesses, cyberattacks, and human errors. Additional risks may come from natural disasters, power outages, strikes, or failures of key partners.

To prevent such events from affecting the security of sensitive data or the operation of critical processes, active risk management is required. This policy ensures that risks are regularly identified, analyzed, and addressed. The results of risk assessments are incorporated into appropriate risk mitigation measures and emergency plans. This approach helps the company remain resilient against both known and new threats.

1.7. Importance of Information Technology and Information Security

Information Technology (IT) is a key driver of innovation and value creation in the company. From product development and customer management to working with partners and suppliers,

business processes rely heavily on digital systems and IT solutions. A secure and reliable IT infrastructure is essential for smooth operations.

Because of this, information security is highly important for the company. It is not only a technical issue—it also includes organizational, legal, and cultural aspects.

All levels of the company must support information security measures to maintain the trust of customers, employees, partners, and regulatory authorities in the long term.

1.8. Leadership and Commitment

The management team strongly supports this policy and commits to providing:

- Clear security objectives that are regularly reviewed.
- Company-wide communication about the importance of information security.
- Training so all employees and managers understand their security responsibilities.
- Active promotion of continuous improvement in the Information Security Management System (ISMS).

Through regular management reviews and budget and personnel approval, the management ensures that information security is effectively implemented and continuously improved.

2. Information Security Objectives

The objective of this Information Security Policy is to define a comprehensive and risk-based framework that ensures the confidentiality, integrity, and availability of all information assets managed by VamiSec GmbH. As a consulting company specialized in IT security and regulatory compliance, we are entrusted with sensitive client data, subject to extensive legal obligations, and dependent on the secure operation of our own infrastructure. This policy aims to protect these values while enabling operational excellence and long-term trust.

2.1. Protection of Client Information

A primary goal is the protection of client-related information, such as audit findings, compliance roadmaps, incident reports, and other confidential deliverables. This includes ensuring secure handling, storage, and transmission of sensitive data in accordance with legal and contractual requirements. Clients must be able to trust that their information is treated with utmost confidentiality and protected against unauthorized access or manipulation.

2.2. Compliance with Legal, Regulatory, and Contractual Obligations

VamiSec GmbH ensures that all applicable national and international regulations are consistently implemented. This includes compliance with ISO/IEC 27001, the NIS2 Directive, GDPR, the EU AI Act, and financial-sector regulations such as DORA. Contractual security obligations from customer agreements, NDAs, and service-level expectations are also binding and must be reflected in internal processes and controls.

2.3. Operational Resilience and Availability of Internal Systems

Our consulting services depend on the availability and integrity of internal tools such as secure file exchange platforms, collaboration systems, and customer support infrastructure. Business continuity must be ensured through secure IT operations, disaster recovery plans, and emergency response capabilities. System failures or unavailability could lead to delays, reputational harm, or breach of contract.

2.4. Information Security by Design in Service Delivery

All consulting and advisory services are delivered under strict adherence to information security best practices. Security must be integrated into our methods, tools, and communication processes to ensure that we not only advise on compliance but also lead by example. Our engagements must not introduce additional risks to our clients or their environments.

2.5. Risk-Based Security Management

Information security risks are identified, assessed, and addressed using a structured and documented risk management process. This applies to both internal operations and client-facing activities. Risk mitigation measures are prioritized based on likelihood and business impact, ensuring a proportional and transparent security strategy.

2.6. Trustworthiness and Reputation

As a service provider in a highly sensitive field, our long-term success depends on our reputation and credibility. Demonstrating security leadership, transparency, and accountability is key to maintaining client trust, securing long-term partnerships, and standing up to scrutiny from auditors, regulators, and third-party assessments.

2.7. Security Awareness and Competence

A strong security culture is promoted within the organization through regular training, awareness campaigns, and role-specific guidance. All employees and external collaborators must understand their responsibilities and act in accordance with our security principles. Awareness is not treated as a one-time task, but as an ongoing process that adapts to new threats and regulatory developments.

2.8. Continuous Improvement and Adaptability

The information security landscape is evolving rapidly. VamiSec GmbH commits to regularly reviewing and improving its policies, controls, and procedures. Lessons learned from audits, incidents, and client feedback are integrated into our ISMS to ensure we remain effective, relevant, and resilient.

3. Areas of Information Security

Information security relies on different areas that together ensure a strong and complete security level. These areas cover both strategic and operational aspects to meet the company's security needs for information and IT systems. They also form the foundation for an integrated Information Security Management System (ISMS) that can quickly adapt to new threats and changes in the business environment.

3.1. Information Security Governance

Effective **information security governance** creates **clear rules and structures** for setting, reviewing, and improving security goals. It ensures that **responsibilities, escalation paths, and decision-making processes** are clearly defined so that all areas of the company follow the same policies.

3.1.1. Security Objectives and Risk Management

The three main security objectives are:

- Confidentiality
- Integrity
- Availability

These are the core requirements for an appropriate security level. To achieve them, a risk management system is used to identify, analyze, and evaluate possible threats and weaknesses. Based on this evaluation, security measures are planned, implemented, and checked for effectiveness. Measures are prioritized based on risk levels and the importance of business processes.

3.1.2. Regulatory, Legal, and Contractual Compliance

VamiSec GmbH ensures that all regulatory, legal, and contractual security requirements are met. This includes:

- Regular review and updates of ISMS policies and processes to follow current laws and standards.
- Collaboration with relevant departments to identify security requirements and integrate them into security measures.
- Regular training and audits to ensure compliance awareness.

3.1.3. Internal Control System

An Internal Control System (ICS) ensures that company rules, policies, and processes are followed and continuously monitored. It uses key performance indicators (KPIs) to measure the effectiveness of security measures and the maturity of processes. This allows the company to identify and fix weaknesses systematically.

3.1.4. Continuous Improvement Process

Information security is not a fixed goal but an ongoing process. Regular risk assessments, internal audits, and security reviews help identify areas for improvement. Actions are adjusted keep security levels high and adapt to new risks and challenges.

3.1.5. Management Review

In regular management reviews, company leadership evaluates the status of information security. This includes:

- Audit results
- Security incidents
- Risk assessments
- Improvement suggestions

Based on these findings, management sets new goals, strategies, and resources or updates existing policies. The management review is the main tool for steering the ISMS strategically.

3.1.6. Communication

Internal and external communication is key to making security goals clear, gaining support, and involving all stakeholders. To achieve this:

- Policies, processes, and ISMS results are shared in an understandable way.
- Training and awareness programs are conducted.
- Clear reporting and communication processes ensure that security incidents or changes are quickly addressed.

3.2. Information Security Policies

Information security policies turn the strategic policy into specific guidelines and procedures. They help employees and managers understand what security measures apply in different areas and what behavior is expected. These policies are regularly updated to reflect new technologies, methods, and regulations. Additional topic-specific policies may be created for specific areas, such as access control, server security, or network segmentation.

3.3. Auditmanagement

A structured audit management process ensures that the ISMS is regularly reviewed for effectiveness. This includes:

- Internal audits by company security teams.
- External audits, such as for certifications.

Audit results help improve the security structure. Any weaknesses found in audits are addressed as part of the continuous improvement process.

3.4. Security Incident Management

The Security Incident Management process defines how security-related incidents or attacks are handled, such as:

- Malware detection
- Unauthorized data access

It ensures that there are clear reporting channels and responsibilities so that incidents can be quickly detected, analyzed, and resolved. After an incident, causes are investigated, and improvements are made to prevent future issues.

3.5. IT Emergency and Crisis Management

The IT Emergency and Crisis Management process ensures that the company is prepared for major security incidents or disruptions, such as:

- Extended IT system failures
- Natural disasters

Emergency plans are developed together with general crisis management to allow rapid recovery of key IT systems and business processes. These plans must also ensure that confidentiality, integrity, and availability are maintained, even in extreme situations.

3.6. Business Continuity Management (BCM)

While IT Emergency Management focuses on specific security incidents, Business Continuity Management (BCM) looks at the overall company operations.

BCM identifies potential risks to business continuity and develops strategies to handle disruptions. This ensures that VamiSec GmbH can continue operating during crises or major disruptions.

3.7. Awareness

The best security setup will not work if employees do not understand how to follow security rules. That's why security awareness is a key part of the ISMS.

Training programs such as:

- Workshops
- Awareness campaigns
- E-learning modules

help employees understand how to handle sensitive information and react to security threats. A strong security culture happens when security becomes a natural part of daily work.

3.8. Security Requirements in Projects

Projects that involve IT systems, applications, or digital processes can create significant security risks.

Security requirements must be considered in project management policies. This includes:

- Early involvement of IT security teams.
- Risk analysis during the project.
- Implementation of security measures.

By integrating security from the beginning, risks are minimized, and security is not just an afterthought.

3.9. Customers, External Service Providers, and Supply Chains

Information security extends beyond the company itself. Relationships with customers and suppliers often involve data exchange, shared processes, or outsourced services.

To maintain a consistent level of security, VamiSec GmbH ensures that:

- Security requirements are included in contracts.
- Service-Level Agreements (SLAs) are in place.
- Regular security reviews of external providers are conducted.

If external providers handle company data or operate critical IT systems, clear security responsibilities, audit rights, and reporting obligations must be established.

3.10. Reporting Obligations and Documentation

Depending on the industry and regulations, companies may have legal obligations to report security incidents to authorities or regulatory bodies.

A structured reporting system ensures that:

- Audit results, incident statistics, and risk assessments are documented.
- Management stays informed about the company's security status.
- Decisions on security improvements can be made based on real data.

3.11. Cooperation with Authorities

Collaboration with government agencies and regulatory bodies is an important part of a strong security strategy.

Legal requirements may include:

- Reporting serious security incidents.
- Participating in security exercises.

Sharing threat intelligence with law enforcement, regulatory agencies, and security organizations can help identify risks early and prevent attacks.

3.12. Data Protection and Security

Protecting personal data is closely linked to information security. To ensure compliance with data protection laws, technical and organizational measures (TOMs) must be in place.

This includes:

- Encryption and data deletion policies.
- Access control and permission management.
- Review procedures to ensure only authorized employees access sensitive data.

In some cases, data protection impact assessments may be required before new data processing activities begin.

4. Exception Handling and Risk Acceptance

There may be situations where certain policy requirements cannot be fully met, for example, in a project or supplier relationship.

In such cases, a formal exception must be documented, accepted by the risk owner, and recorded in the risk register (see also the Asset and Risk Management Policy).

The potential risks of these exceptions, as well as the reasons for the deviations, must be documented and reviewed regularly (annually).

5. Roles, Responsibilities, and Authorizations

According to ISO/IEC 27001, roles related to information security must be clearly assigned. Detailed descriptions of all tasks and committees can be found in the separate document "Roles and Committees Structure in the ISMS."

Below are the two key roles highlighted in this policy.

5.1. Management Team

The management team has overall responsibility for the ISMS and ensures that information security is part of all strategic decisions. The management team:

- Appoints the Chief Information Security Officer (CISO) or Information Security Officer (ISB) and confirms their authority.
- Defines and monitors the company's high-level information security goals.
- Provides budgets and resources to meet all ISMS requirements.
- Participates in management reviews (see Section 2.1.5).
- Approves important policies and changes in the ISMS.

5.2. Chief Information Security Officer (CISO)

The CISO, also known as the Information Security Officer (ISB), is responsible for developing, maintaining, and continuously improving the ISMS. The CISO:

- Supports the management team in setting and monitoring information security goals.
- Coordinates the creation, alignment, and publication of all relevant security policies.
- Initiates and monitors all actions to reduce information security risks.
- Acts as the main contact person for internal and external stakeholders on security matters.
- Regularly reports to the management team on the status of the ISMS, incidents, improvements, and audit results.
- Leads awareness and training programs to ensure strong security knowledge across the organization.

6. Legitimization

This policy comes into effect on 30.07.2025.

Approval by CEO Valeri Milke 30.07.2025.

7. Further Documents and References

To ensure that all aspects of information security are consistently managed and maintained, this policy refers to additional policies and documents that provide more details on specific topics. The following table gives an overview of key reference documents and their purpose:

Document	Content/Purpose
ISMS Roles and Committees Structure Policy	Describes all roles involved in the ISMS (e.g., IT Security Team, SOC, Incident Response Team, Asset Owner) as well as their responsibilities and committees. This document complements Section 4, which defines the key roles of management and CISO, by adding operational and technical responsibilities.
Information Security Orgnization Policy	Defines the principles for structuring and managing information security. It includes detailed rules on responsibilities, areas of authority, and decision-making powers. This policy serves as a link between this strategic policy and topic-specific policies within the ISMS.