StrategyFrame GmbH

Information Security

Classification - Public

Last Reviewed: 01.08.2025

Document Owner: Daniel Theobald

Document Properties

Sr. No.	Type of information	Description
1	Document Title	Information Security
2	Document Code	POL-01
3	Document Owner	Daniel Theobald
4	Document Approver	Christian Underwood
5	Document Version Number	1.0
6	Date of Release	01.08.2025
7	Nature of Change	Initial Release
8	Classification	Public

Version History

Version	Document Title	Change Description	Approved On
1	Information Security		10.09.2025

Table of Contents

1. Policy Statements

StrategyFrame GmbH is committed to preserving the confidentiality, integrity, and availability of its information and information systems. To support this, we have established and maintain a risk-based Information Security Management System (ISMS) aligned with ISO/IEC 27001:2022.

This policy reflects top management's commitment to:

- Protecting organizational, customer, and stakeholder information;
- Ensuring compliance with legal, regulatory, and contractual obligations;
- Minimizing business disruption from information security threats;
- Promoting continual improvement of our ISMS.

2. Information Security Objectives

Our Information security objectives are to:

1. Maintain full compliance with GDPR and applicable data protection laws through regular verification and control reviews.

2. Ensure critical vendor and supplier risks are regularly assessed and managed through documented security reviews.

3. Achieve and maintain high platform availability to support uninterrupted secure service delivery.

4. Ensure all personnel receive current and complete ISMS awareness training to reduce human error and support compliance.

5. Maintain current and effective policies across the ISMS by ensuring timely reviews and updates.

6. Successfully implement the ISMS and meet all planned milestones to achieve certification-readiness and operational security.

7. Ensure that audit findings are minimized and addressed through proactive control implementation and internal audit quality.

8. Detect, classify, and contain information security incidents in a timely and effective manner to prevent escalation.

9. Ensure that application-level security requirements are reviewed and approved in collaboration with development vendors.

10. Monitor and review high-rated risks quarterly to ensure they remain within acceptable treatment timelines.

These objectives are continuously monitored and reviewed as part of the operation of the ISMS.

3. Scope

This policy applies to:

- All employees, contractors, consultants, and third-party users;
- All organizational units, systems, locations, and data assets;
- All forms of information (digital, physical, verbal) and processing environments.

It encompasses all activities that involve the creation, processing, storage, communication, and disposal of information under the organization’s control.

4. Leadership Commitment

Top management shall:

- Establish and maintain an ISMS in line with ISO/IEC 27001:2022;
- Define and communicate roles, responsibilities, and authority for information security;
- Allocate appropriate resources to achieve ISMS objectives;
- Lead by example in promoting a security-aware culture;
- Integrate information security into strategic and operational planning.

5. Risk Management

Information security risks shall be:

- Identified, assessed, and treated in accordance with our Risk Assessment and Treatment Procedure;
- Managed continuously to reflect changes in threats, vulnerabilities, and business priorities;
- Aligned with our overall business risk management framework.

---

6. Compliance

The organization is committed to fulfilling:

- Applicable legal, regulatory, and contractual obligations related to information security;
- Internal requirements, including policies, standards, and procedures;
- Monitoring and audit processes to ensure adherence.

All personnel are expected to comply with this policy and associated requirements. Non-compliance may result in disciplinary action.

7. Continual Improvement

The ISMS shall be continually improved through:

- Regular internal audits and management reviews;
- Risk and performance monitoring;
- Prompt and effective treatment of incidents, nonconformities, and opportunities for improvement.

8. Communication

This policy shall be:

- Approved by top management;
- Communicated to all personnel and relevant external parties;
- Available to interested parties upon request;
- Reviewed annually or following significant changes to business, risk, or compliance context.