02-ISMS Information Security Management System (ISMS) Policy

Policy Owner: Alexander Ruehle

Effective Date: 02/13/2026

Purpose

This policy provides a framework to be applied when establishing, implementing, maintaining, and continually improving the information security management system ("ISMS"), as defined in 01-ISMS Scope of the ISMS, in accordance with the requirements of the ISO/IEC 27001 ("ISO 27001") standard.

Leadership

Leadership and commitment

zapliance GmbH is dedicated to establishing, implementing, maintaining, and continually improving the ISMS. Leadership commitment is demonstrated by the ISMS Governance Council when carrying out their responsibilities as defined in the *03-ISMS Roles, Responsibilities, and Authorities* document. zapliance GmbH will establish an information security policy and set information security objectives that are fully aligned with our strategic direction. zapliance GmbH will ensure that sufficient resources are available for the effective establishment, implementation, maintenance, and improvement of our ISMS. These resources will include:

- Financial support
- Skilled personnel
- Facilities and technical infrastructure

Information Security Policy

zapliance GmbH's top management establishes and upholds a dedicated information security policy. This policy:

1. Aligns with the organization's purpose and mission.
2. Incorporates our information security objectives or sets the groundwork for determining such objectives.
3. Demonstrates a commitment to meeting all relevant information security requirements.
4. Emphasizes our continual dedication to enhancing our information security management system.

For transparency and awareness:

1. This policy is documented and readily accessible.

2. It is actively communicated across all levels within zapliance GmbH.
3. Furthermore, we ensure this policy is available to relevant external parties, demonstrating our commitment to information security.

Roles, responsibilities and authorities

zapliance GmbH has defined the roles, responsibilities, and authorities involved in establishing, implementing, maintaining, and continually improving the ISMS. zapliance GmbH has also defined how performance and competence will be measured and how competency gaps will be addressed. For further details, please refer to the 03-ISMS Roles, Responsibilities, and Authorities document.

Planning

General planning for the ISMS

zapliance GmbH prioritizes identifying key risks and opportunities, integrating solutions into our system, and continually monitoring and improving our approach.

Information security risk assessment

At zapliance GmbH, our consistent method for assessing risks ensures the identification of major security threats. We regularly evaluate and prioritize these risks and maintain documentation of all our findings. For further details, please refer to the *04-ISMS Risk Assessment and Risk Treatment Process* document.

Information security risk treatment

zapliance GmbH is committed to selecting the right solutions for identified risks, implementing necessary security controls, and thoroughly documenting our choices while obtaining essential approvals. For further details, please refer to the *04-ISMS Risk Assessment and Risk Treatment Process* document.

Setting & achieving security objectives

zapliance GmbH establishes clear, measurable security goals. We've developed a comprehensive plan detailing how to achieve them, allocating the needed resources and responsibilities, and continually monitoring our progress to make any necessary adjustments. Information security objectives are reviewed annually by zapliance GmbH's ISMS Governance Council based upon a clear understanding of business requirements. The current information security objectives are as follows:

1. Protect the confidentiality, availability, and integrity of company, customer, and employee data
2. Comply with applicable laws, regulations, and customer contractual obligations
3. Achieve and maintain ISO 27001 certification Action plans to achieve these objectives are maintained and reviewed annually by the ISMS Governance Council. Refer to *10-ISMS Information Security Objectives Plan* for further details.

Planning changes to the ISMS

When changes are deemed essential, zapliance GmbH ensures they are planned systematically, with careful consideration given to their potential impact on our overall security and the organization.

Support

Resources:

zapliance GmbH is committed to allocating the necessary resources to set up, execute, maintain, and consistently enhance our information security management system.

Competence:

1. We identify the expertise needed for roles impacting our information security performance.
2. Personnel are evaluated based on education, training, and experience to ensure they possess the required competence.
3. When necessary, zapliance GmbH will provide training, mentoring, or reassignment, or seek external expertise, while also maintaining evidence of such competencies.

Awareness:

1. All personnel are made aware of our information security policy and complete annual awareness training.
2. They understand their role in the success of the information security management system and the repercussions of non-compliance.

Communication:

1. zapliance GmbH identifies and acts on the need for both internal and external communications concerning our information security practices.
2. Decisions encompass what, when, how, and with whom to communicate.

Relevant information security policies will be communicated to all in-scope personnel at least annually after review and approval, or after any significant changes occur to the policy. The policy will be made available in the company's Vanta system accessible by all zapliance GmbH personnel. For further details, please refer to the *06-ISMS Information Security Communication Plan* document.

Control of documented information

Documented Information:

- Our system comprises information explicitly mandated and any other documentation we deem crucial for the effectiveness of our security measures.
- Documentation creation and updates consider proper identification, format, and approval mechanisms.
- To maintain the integrity of our documentation, we have protocols in place to control distribution, access, storage, changes, and preservation.
- External documentation, deemed essential, is identified and managed effectively within our system.
- zapliance GmbH has defined a procedure for the control and protection of documented information. For further details, please refer to the *05-ISMS Procedure for the Control of Documented Information* document.

Operation

Operational planning and control

zapliance GmbH will plan, execute, and oversee the processes vital to satisfy requirements and actions outlined in Clause 6. zapliance GmbH will maintain necessary documented information. Planned modifications will be overseen, and the implications of unplanned changes will be evaluated. Appropriate actions will be taken to counteract any negative effects. Externally sourced processes, products, or services crucial to the information security management system will be governed by zapliance GmbH.

Information security risk assessment

zapliance GmbH will conduct risk evaluations at scheduled intervals or in light of significant alterations, adhering to the criteria highlighted in 6.1.2 a). A record of the outcomes of these risk assessments will be preserved.

Information security risk treatment

zapliance GmbH is committed to executing the information security risk treatment plan. For accountability, documented information on the outcomes of the risk treatment will be maintained.

Performance evaluation

Internal audit

zapliance GmbH performs internal audits of its ISMS on a recurring basis and has defined an ISMS Internal Audit Procedure. For further details, please refer to the *07-ISMS Procedure for Internal Audits* document.

Management review

zapliance GmbH has defined an ISMS Management Review Procedure consisting of the necessary inputs and outputs to ensure that the company's ISMS is operating effectively, as intended, and is continually improving. For further details, please refer to the *08-ISMS Procedure for Management Review.*

Improvement

Continual Improvement

zapliance GmbH is dedicated to perpetually enhancing the relevance, sufficiency, and efficiency of our information security management system.

Nonconformity and corrective action

In case of any deviation from established standards, zapliance GmbH commits to:

- Address the nonconformity, manage its effects, and implement necessary corrections.
- Evaluate the root cause, ensuring it doesn't repeat or emerge in other areas.
- Act upon any required changes and validate the efficacy of those changes.
- All measures taken will be proportionate to the severity of the nonconformities identified.

For transparency and due diligence, zapliance GmbH will document:

- The specifics of any nonconformity and the corrective measures applied.
- The outcomes of those corrective actions. zapliance GmbH has defined an ISMS Corrective Action and Continual Improvement Procedure when non-conformities are identified. Non-conformities may be identified during internal audits, external audits, management reviews, or ongoing monitoring of the ISMS. For further details, please refer to the *09-ISMS Procedure for Corrective Action and Continual Improvement* document.

Policy violation

All zapliance GmbH personnel (including employees, contractors, and applicable third parties) must maintain the security, confidentiality, availability, integrity, and privacy of zapliance GmbH assets. Violations of ISMS policies and procedures may be considered serious breaches of trust, which can

result in disciplinary action up to and including termination of employment or contract and prosecution in accordance with applicable federal, state, and local laws.

ISO 27001 coverage

ISO 27001 4.1; 4.2; 4.3; 5.1

Version history

Version	Date	Description	Author	Approver
1.0	02/13/2026	Version 1.0	Mukesh Yadav	**Alexander Ruehle**

27701 Privacy Information Management System (PIMS) Addendum

This addendum is automatically applicable for organizations implementing ISO 27701 and optional for organizations who are implementing ISO 27001 only.

- All references to "ISMS" in this document are changed to "IS&PMS"
- All references of ISO 27001 in this document are changed to "ISO 27001/27701"
- All references to "information security management system" are changed to "information security and privacy management system"