



We record & analyze communications

Information Security and Privacy Policy

Table of Contents

- 1. Vision**2
- 2. Mission**2
- 3. Principles**2
 - Policy Objectives2
 - Risk Management2
 - Roles, Responsibilities, and Authorities2
 - Resource Management2
 - Competence and Awareness.....2
 - Documented Information3
 - Monitoring, Measurement, Analysis, and Evaluation.....3
 - Internal Audit3
- 4. Continuous improvement**.....3
- 5. Accountability & regular review**.....3
- 6. Communication**.....3

Scope of this document: ASC Technologies AG, Seibelstrasse 2-4, 63768 Hoesbach, Germany, as well as such affiliated companies pursuant to § 15 of the German Companies Act (AktG) that are covered by the current scope of the relating ISO certification.

© ASC Technologies AG, 2025 All rights reserved.

Classification: Public	Information Security and Privacy Policy Rev. 00		Page 1 of 3
	Responsibility: M. Müller (COO)	Release date:	23.09.2025
		Next review:	31.12.2026

Valid without signature! Not controlled when printed - always check the Partner Portal for valid revisions!

1. Vision

As a worldwide leading provider of omnichannel recording, quality management and AI based analytics, ASC Technologies AG (“ASC”, “We”) provides state-of-the-art solutions for digital communications governance and is committed to protecting its information assets and ensuring the resilience of its critical business operations to reliably and continually safeguard its clients, employees, and business interests. We aim to remain a trusted partner by embedding effective information security, privacy, and business continuity practices into all aspects of our services. ASC recognizes that effective information security, privacy and robust business continuity are fundamental to providing reliable services and maintaining the trust of clients and stakeholders.

2. Mission

This policy establishes the framework for our integrated Information Security and Privacy Management System (“ISPMS”) and Business Continuity Management System (“BCMS”) which must be adhered to and complied with in all business activities of ASC. The scope of these integrated parts of ASC’s Multi-Management System (“MMS”) to which this policy applies covers relevant personnel, processes, technology, and physical locations involved in the delivery and support of ASC services. The Executive Board is fully committed to establishing, implementing, maintaining, and continually improving the ISPMS based on ISO 27001:2022 and the BCMS based on ISO 22301:2019.

3. Principles

Policy Objectives

This policy establishes the framework for:

- Protecting confidentiality, integrity, and availability of information.
- Ensuring the privacy of personal and sensitive data.
- Ensuring the availability of critical business processes and the ability to recover from disruptive incidents.
- Complying with applicable legal, regulatory, and contractual requirements related to information security and business continuity.
- Setting and reviewing objectives for information security, privacy and business continuity performance.

Risk Management

ASC adopts a systematic approach to information security, privacy, and business continuity risk management. Risks and opportunities are identified, analyzed, evaluated, and treated in accordance with the Risk Management Policy. This includes considering risks specific to the cloud environment and dependencies on third parties. Risks are treated to levels acceptable to the organization, and the risk acceptance criteria are defined and approved by senior management.

Roles, Responsibilities, and Authorities

Roles, responsibilities, and authorities for information security, privacy, and business continuity are defined and communicated throughout the organization. The ASC Executive Board ensures their proper internal and external communication.

Resource Management

ASC will provide adequate resources (human, financial, technological, and infrastructure) necessary to establish, implement, maintain, and continually improve the ISPMS and BCMS, including implementing necessary controls and business continuity measures.

Competence and Awareness

ASC is committed to ensuring that all personnel whose work affects information security and privacy, or business continuity are competent based on appropriate education, training, and experience. Awareness programs are in place to ensure that personnel are aware of this policy, their responsibilities, and the importance of information security, privacy, and business continuity.

Documented Information

The ISPMS and BCMS are supported by documented information necessary to ensure they are implemented, operated, and maintained effectively. This documented information is controlled in accordance with established procedures.

Monitoring, Measurement, Analysis, and Evaluation

The performance and effectiveness of the ISPMS and BCMS, including controls and business continuity arrangements, are monitored, measured, analyzed, and evaluated at planned intervals.

Internal Audit

Internal audits are conducted at planned intervals to determine whether the ISPMS and BCMS conform to the requirements of ISO 27001:2022, ISO 22301:2019, ASC's own requirements, and whether they are effectively implemented and maintained.

4. Continuous improvement

ASC is committed to the continual improvement of its ISPMS and BCMS. Nonconformities are addressed through corrective actions, and opportunities for improvement are identified and acted upon to enhance information security and privacy posture and business continuity capabilities.

5. Accountability & regular review

ASC Executive Board fully commits to this policy and is accountable for the effectiveness of the ISPMS and BCMS. All employees and relevant third parties are responsible for adhering to the requirements of this policy and supporting procedures.

This policy will be reviewed by the Executive Board at least annually or whenever significant changes occur to ensure its continued relevance and effectiveness. The Executive Board reviews the ISPMS and BCMS at planned intervals to ensure their continuing suitability, adequacy, and effectiveness. This review considers feedback on performance, audit results, changes, and opportunities for improvement.

6. Communication

Processes are established for effective internal and external communication relevant to the ISPMS and BCMS, including communicating this policy, changes, incidents, and business continuity status.

This Policy is publicly available to internal and external interested parties ("stakeholders").

Requests may be addressed to: iso@asc.de.