Information Security Management System (ISMS) Policy

1. Purpose

The purpose of this information security policy is to ensure the confidentiality, integrity, and availability of information as well as the security of the information systems of POS Solutions GmbH. It serves as the basis for all measures of the Information Security Management System (ISMS) in accordance with ISO/IEC 27001.

2. Scope

This ISMS policy applies to the entire POS Solutions GmbH company.

The policy applies to all employees, managers, service providers, consultants, and other third parties who have access to information and IT systems of POS Solutions GmbH.

The policy covers the POS Solutions GmbH location in Braunau am Inn and all systems and processes related to the processing of information.

3. Principles and objectives of information security

As a provider of online identification, electronic signatures, and other trust services, POS Solutions GmbH is committed to the following information security objectives:

Confidentiality of customer data, i.e.

Protection of personal data, identification data, signature and onboarding information from unauthorized access through appropriate measures such as encryption, access controls, secure authentication, etc.

Integrity of digital services and transactions, i.e.

ensuring (e.g. through hash procedures, log monitoring, tamper protection, etc.) that electronic signatures, identification processes, and data flows remain unchanged and correct.

Availability of platform and trust services, i.e.

ensuring that critical services (such as online onboarding, signature services, etc.) are available in accordance with the agreed service level and that outages are avoided as far as possible.

Compliance with applicable legal bases and regulations, i.e.

Compliance with applicable legal requirements (e.g., EU-wide signature directives, identification and money laundering legislation, etc.) and data protection requirements.

Continuous improvement and technology provision, i.e.

Establishing and maintaining security and trust services that are technologically up to date, anticipate potential threats (e.g., through cryptographic procedures, cloud/on-premises variants), and thus strengthen investment and service security for customers.

4. Responsibilities

The management bears overall responsibility for information security.

The ISMS officer is responsible for planning, implementing, and maintaining the ISMS.

Every employee is obliged to comply with the guidelines and report incidents.

5. Risk management

Information security risks are systematically identified, assessed, and addressed. The measures taken depend on the identified risk and the organization's risk appetite.

6. Security measures

Technical, organizational, and physical measures are taken to ensure the security of information. These include, among others:

- Access controls
- Network security
- Encryption
- Training and awareness

- Emergency and recovery plans

7. Training and awareness

All employees receive regular training on information security and are made aware of security-related issues.

8. Monitoring and improvement

The ISMS is regularly reviewed and adjusted through internal audits, management reviews, and continuous improvement processes.

9. Violations

Violations of this policy may result in disciplinary action and may be prosecuted under criminal or civil law.

10. Effective date

This policy shall take effect on September 29, 2025, and shall be reviewed at least once a year and adjusted as necessary.