Informationssicherheits-Managementsystem (ISMS) Policy

1. Zweck

Ziel dieser Informationssicherheits-Policy ist es, die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen sowie die Sicherheit der Informationssysteme der POS Solutions GmbH sicherzustellen. Sie dient als Grundlage für alle Maßnahmen des Informationssicherheits-Managementsystems (ISMS) gemäß ISO/IEC 27001.

2. Geltungsbereich

Diese ISMS-Policy hat für das gesamte Unternehmen POS Solutions GmbH seine Gültigkeit.

Die Policy gilt für alle Mitarbeiter:innen, Führungskräfte, Dienstleister:innen, Berater:innen und sonstige Dritte, die Zugriff auf Informationen und IT-Systeme der POS Solutions GmbH haben.

Die Policy umfasst den POS Solutions GmbH Standort in Braunau am Inn und alle Systeme und Prozesse, die mit der Verarbeitung von Informationen in Verbindung stehen.

3. Grundsätze und Ziele der Informationssicherheit

Als Anbieter von Online-Identifikation, elektronischen Signaturen und weiteren Vertrauensdiensten fühlt sich die POS Solutions GmbH den folgenden Informationssicherheitszielen verpflichtet:

Vertraulichkeit der Kundendaten, d.h.

Schutz von personenbezogenen Daten, Identifikationsdaten, Signatur- und Onboarding-Informationen vor unberechtigtem Zugriff durch geeignete Maßnahmen wie z.B. Verschlüsselung, Zugriffskontrollen, sichere Authentifizierung etc..

Integrität der digitalen Dienste und Transaktionen, d.h.

Sicherstellung (z. B. durch Hash-Verfahren, Log-Monitoring, Manipulationsschutz etc.), dass elektronische Signaturen, Identifikationsprozesse und Datenflüsse unverändert und korrekt ablaufen.

Verfügbarkeit der Plattform- und Vertrauensdienste, d.h.

Gewährleistung, dass die kritischen Dienste (wie z. B. Online-Onboarding, Signatur-Service etc.) gemäß vereinbartem Servicelevel erreichbar sind und Ausfälle möglichst vermieden werden.

Konformität in Bezug auf geltende Rechtsgrundlagen und Regulatorien, d.h.

Einhaltung der anzuwendenden gesetzlichen Anforderungen (z. B. EU-weit gültige Signaturrichtlinien, Identifikations- und Geldwäschegesetzgebung etc.) sowie Datenschutzvorgaben.

Kontinuierliche Verbesserung und Technologievorsorge, d.h.

Aufbau und Pflege von Sicherheits- und Vertrauensdiensten, die technologisch aktuell sind, mögliche Bedrohungen antizipieren (z. B. durch Kryptoverfahren, Cloud/On-Prem Varianten) und so die Investitions- und Service-Sicherheit für Kunden stärken.

4. Verantwortlichkeiten

Die Geschäftsführung trägt die Gesamtverantwortung für die Informationssicherheit.

Der ISMS-Beauftragte ist für die Planung, Umsetzung und Aufrechterhaltung des ISMS verantwortlich.

Jede:r Mitarbeiter:in ist verpflichtet, die Richtlinien einzuhalten und Vorfälle zu melden.

5. Risikomanagement

Informationssicherheitsrisiken werden systematisch identifiziert, bewertet und behandelt. Die Maßnahmen richten sich nach dem ermittelten Risiko und der Risikobereitschaft der Organisation.

6. Sicherheitsmaßnahmen

Es werden technische, organisatorische und physische Maßnahmen getroffen, um die Sicherheit der Informationen zu gewährleisten. Dazu gehören u. a.:

- Zugriffskontrollen
- Netzwerksicherheit
- Verschlüsselung

- Schulungen und Sensibilisierung
- Notfall- und Wiederherstellungspläne

7. Schulung und Bewusstsein

Alle Mitarbeiter:innen erhalten regelmäßig Schulungen zur Informationssicherheit und werden für sicherheitsrelevante Themen sensibilisiert.

8. Überwachung und Verbesserung

Das ISMS wird regelmäßig durch interne Audits, Managementbewertungen und kontinuierliche Verbesserungsprozesse überprüft und angepasst.

9. Verstöße

Verstöße gegen diese Policy können disziplinarische Maßnahmen nach sich ziehen und ggf. straf- oder zivilrechtlich verfolgt werden.

10. Inkrafttreten

Diese Policy tritt am 29.09.2025 in Kraft und wird mindestens einmal jährlich überprüft und bei Bedarf angepasst.