



## 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 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. Sie umfasst alle Standorte, Systeme und Prozesse, die mit der Verarbeitung von Informationen in Verbindung stehen.

### 3. Grundsätze der Informationssicherheit

Die POS Solutions GmbH verpflichtet sich zur Einhaltung der folgenden Grundsätze:

1. Vertraulichkeit: Informationen werden nur autorisierten Personen zugänglich gemacht.
2. Integrität: Informationen sind korrekt, vollständig und vor unbefugter Manipulation geschützt.
3. Verfügbarkeit: Informationen und Systeme stehen berechtigten Nutzern bei Bedarf zur Verfügung.

### 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.