

# INFORMATIONSSICHERHEITS RICHTLINIE

## 1 Zweck und Geltungsbereich

Dieses Dokument beschreibt den Geltungsbereich des Managementsystems für Informationssicherheit (ISMS). Es definiert die Grenzen, Anwendbarkeit und den Umfang des ISMS innerhalb der Organisation.

## 2 Begriffe und Definitionen

**ISMS:** Managementsystem für Informationssicherheit

**Geltungsbereich:** Definiert die Anwendbarkeit eines Managementsystems.

**Rechtseinheit:** Eine Organisation oder Einheit mit rechtlichem Status, die Verträge abschließen, Vermögenswerte besitzen und haftbar gemacht werden kann Beispiele: Muttergesellschaften, Tochtergesellschaften, Joint Ventures.

**Prozess:** Eine Abfolge von Handlungen oder Schritten zur Umwandlung von Eingaben in ein gewünschtes Ergebnis.

**Physischer Standort:** Ein bestimmter geografischer Ort, an dem die Organisation ihre Tätigkeiten ausführt. Beispiele: Hauptsitz, Zweigstellen, Rechenzentren, Produktionsstätten.

## 3 Verknüpfte Dokumente

Die folgenden Dokumente sind mit dieser Richtlinie verknüpft:

- Informationssicherheitsleitlinie

## 4 Geltungsbereich des ISMS

Kickscale FlexCo, gegründet 2019, ist ein Softwareentwicklungsunternehmen, das sich auf Softwareentwicklung und Software as a Service / SaaS -Lösungen spezialisiert hat. Das Unternehmen mit Sitz in Österreich bedient Kunden aus verschiedenen Branchen, insbesondere im Bereich Technologie und der SaaS-Industrie. Es bietet eine KI-gestützte SaaS-Plattform, die

B2B-Vertriebsteams dabei unterstützt, Kundengespräche automatisch zu transkribieren, zu analysieren und zusammenzufassen, um effizientere Nachbearbeitung, CRM-Aktualisierungen und Coachings zu ermöglichen – mit dem Ziel, die den Verkaufsprozess Prozess zu optimieren und Erfolgsquoten zu verbessern.

Der Geltungsbereich des Managementsystems für Informationssicherheit (ISMS) dieses Unternehmens umfasst die folgenden Bereiche:

- **Organisatorischer Geltungsbereich:** Umfasst alle relevanten Rechtseinheiten, Abteilungen, Bereiche und Prozesse, die für die Verwaltung und den Schutz von Informationen innerhalb der Organisation wesentlich sind.
- **Physischer Geltungsbereich:** Umfasst alle Standorte, Einrichtungen und physischen Orte, an denen Informationen elektronisch gespeichert, verarbeitet oder übertragen werden, einschließlich der damit verbundenen physischen Sicherheitsmaßnahmen.
- **IKT-Geltungsbereich:** Beinhaltet alle Informations- und Kommunikationstechnologien (IKT), Systeme, Netzwerke und zugehörige Infrastrukturen, die die Verarbeitung, Speicherung und Übertragung von Informationen innerhalb der Organisation unterstützen.

## 4.1 Organisatorischer Geltungsbereich

### Rechtseinheiten:

Das ISMS gilt für die folgende Rechtseinheit:

- Kickscale FlexCo

### Organisationseinheiten

Das ISMS gilt für die folgenden Organisationseinheiten:

- Finanzen & Administration
- Technologie
- Vertrieb & Marketing

### Prozesse

Das ISMS gilt für die folgenden Prozesse innerhalb der Organisation:

- **Produktentwicklung:** Kernprozess zur Konzeption, Entwicklung und Aktualisierung des SaaS-Produkts. Umfasst das Entwerfen neuer Funktionen, Programmieren, Testen und Bereitstellen von Updates. Gewährleistet, dass das Produkt den Marktanforderungen entspricht und wettbewerbsfähig bleibt.

- **Vertrieb und Geschäftsentwicklung:** Wesentlich für die Umsatzgenerierung; umfasst die Identifizierung potenzieller Kunden, Kontaktaufnahme und Umwandlung von Interessenten in Kunden (z. B. Verkaufsgespräche, Produktdemos, Vertragsverhandlungen).
- **Customer Success & Support:** Unterstützung der Kunden bei der effektiven Nutzung des Produkts sowie Bearbeitung von Anfragen und Problemen. Umfasst Onboarding, Support-Leistungen, Kundens Schulungen und Feedbackprozesse.
- **Marketing & Branding:** Umfasst alle Prozesse zur Steigerung der Markenbekanntheit, Lead-Generierung und Positionierung des Unternehmens im Markt (z. B. Content-Marketing, Social Media, E-Mail-Kampagnen, SEO, Branchenveranstaltungen).
- **Finanzen & Buchhaltung:** Verwaltung der finanziellen Aspekte einschließlich Budgetierung, Buchführung, Rechnungsstellung und Berichterstattung. Gewährleistet die Einhaltung gesetzlicher Vorschriften und ein wirksames Cash-Flow-Management.
- **Human Resources & Talent Management:** Zuständig für Rekrutierung, Einarbeitung, Schulung und Entwicklung von Mitarbeitenden, Leistungsmanagement und Pflege einer positiven, regelkonformen Unternehmenskultur.
- **IT & Infrastrukturmanagement:** Verwaltung, Wartung und Absicherung der IT-Systeme, Netzwerke, Hardware und sonstigen technologischen bzw. physischen Infrastrukturen zur Unterstützung der operativen Anforderungen und Wachstumsziele.

## Leistungen

Das ISMS gilt für die folgenden vom Unternehmen erbrachten Leistungen und Produkte:

- **Kickscale SaaS-Lösung** im Bereich Vertriebseffizienz

## 4.2 Physischer Geltungsbereich

Das ISMS gilt für folgende Standorte und Einrichtungen:

- Graz (Entwicklungszentrum)  
DataHouse 01/189  
Sandgasse 36, 8010 Graz
- Klagenfurt  
Lakeside Science & Technology Park  
B08 / Eingang 01 / EG

**Vom physischen Geltungsbereich ausgeschlossen:**

Das Büro Wien, Startup House, Stella-Klein-Löw-Weg 8, 1020 Wien, ist formell vom Geltungsbereich dieser Kontrolle ausgeschlossen. Der Standort dient ausschließlich als geschäftliche Registrierungsadresse; dort werden keine Büroräumlichkeiten betrieben und es sind keine Mitarbeitenden, Vermögenswerte, Informationssysteme oder Vorbereitungstätigkeiten vorhanden. Daher entstehen aus diesem Standort Adresse keine Informationssicherheitsrisiken. Diese Ausnahme gilt einheitlich für alle relevanten Sicherheitskontrollen.

## 4.3 IKT-Geltungsbereich

Der IKT-Geltungsbereich legt fest, welche Informations- und Kommunikationstechnologien im Rahmen des ISMS enthalten sind, und beschreibt die Grenzen zwischen einbezogenen und ausgeschlossenen Komponenten.

Folgende IKT-Anlagen und Geräte sind im ISMS-Geltungsbereich enthalten:

- **Hardware:** Das Unternehmen betreibt kein eigenes Rechenzentrum und keine interne IT-Infrastruktur, sondern bezieht sämtliche IT-Dienste von Cloud-Anbietern (z. B. Google, Microsoft). Die einzigen im Besitz des Unternehmens befindlichen Geräte sind Endgeräte (Desktop-, Laptop-Computer und Telefone).
- **Software:** Entwicklungsumgebung, Betriebssysteme, Geschäfts- und Sicherheitsanwendungen, Datenbanken und Tools für Sicherheitsmanagement.
- **Cloud-Dienste:** Eingesetzte SaaS-, PaaS- und IaaS-Lösungen.
- **Kommunikationssysteme:** E-Mail-, Video-, Messaging- und sonstige Kommunikationsplattformen.
- **Daten-Speicher:** Datenbanken, Fileserver und Cloud-Speicher Umgebungen zur Speicherung, Verarbeitung und Übertragung von Informationen.
- **Drittssysteme:** Ausgelagerte oder von Dritten betriebene IKT-Dienste bzw. Infrastrukturen, die Auswirkungen auf die Informationssicherheit haben.

### Drittanbieter-Abgrenzung:

Kickscale nutzt Cloud-Service-Provider (CSPs), hauptsächlich Google und Microsoft, zur Bereitstellung von Anwendungen und Datenspeicherung. Für diese CSPs gelten folgende Abgrenzungen:

- **Datenhoheit:** Kickscale behält das Eigentum an allen auf der Infrastruktur der CSPs gespeicherten Daten.
- **Zugriffskontrolle:** Der CSP ist für die physische Sicherung seiner Rechenzentren verantwortlich; Kickscale verwaltet die Benutzerzugriffe auf die Cloud-Umgebung.

- **Compliance-Anforderungen:** Der CSP weist durch Zertifizierungen (z. B. ISO 27001, SOC 2) die Einhaltung von Sicherheitsstandards nach; Kickscale stellt sicher, dass eigene Anwendungen und Konfigurationen diese Anforderungen erfüllen.
- **Vorfallmanagement:** Der CSP informiert Kickscale über Sicherheitsverletzungen oder Vorfälle in seiner Infrastruktur; Kickscale bearbeitet Vorfälle innerhalb der eigenen Anwendungen oder Daten.

Bezüglich **physischer Kontrollen** gilt:

- Der physische Zutritt zu den Büroräumen wird durch verschiedene Workspace-Provider verwaltet (Wien / Startup House, Graz / DataHouse, Klagenfurt / Lakeside Park). Daher liegen die Zutritts-Infrastruktur und -Prozesse (z. B. Zutrittskarten, Rezeption, CCTV, Besucherregistrierung) außerhalb der direkten Kontrolle der Organisation und sind vom ISMS ausgeschlossen. Das Unternehmen stützt sich auf vertragliche Vereinbarungen mit den Workspace-Anbietern, um ein angemessenes Sicherheitsniveau sicherzustellen.
- Die von den Workspace-Providern bereitgestellte IT-Infrastruktur (WLAN / Internetzugang) ist ebenfalls aus dem ISMS-Geltungsbereich ausgenommen.

#### **Ausschließung bez. des IKT Geltungsbereich:**

Die physische Infrastruktur der Dritt-Cloud-Anbieter bleibt unter deren Kontrolle und ist gemäß dem Shared-Responsibility-Modell vom ISMS ausgeschlossen.