Informationssicherheitsleitlinie

1 Zweck und Geltungsbereich

Diese Leitlinie legt die Grundsätze, Ziele und Verantwortlichkeiten für die Informationssicherheit der Pröll GmbH fest. Sie gilt für alle Mitarbeitenden, Führungskräfte, externe Dienstleister sowie sonstige Personen, die Zugriff auf Informationen, IT-Systeme oder Geschäftsprozesse der Pröll GmbH haben – unabhängig von Standort, Arbeitsform (vor Ort, mobil, Homeoffice) oder eingesetzten Geräten.

Informationssicherheit dient dem Schutz der Verfügbarkeit, Vertraulichkeit, Integrität und Authentizität von Informationen. Die Leitlinie bildet den Rahmen für das Managementsystem für Informationssicherheit (ISMS) und ist verbindlich für alle innerhalb ihres Geltungsbereichs.

2 Leitbild und Grundsätze

- Top-Management-Verantwortung: Die Geschäftsleitung übernimmt die Gesamtverantwortung für Informationssicherheit, stellt Ressourcen bereit und lebt die Sicherheitskultur vor.
- Risikobasierter Ansatz: Risiken werden systematisch identifiziert, bewertet und behandelt; Maßnahmen orientieren sich an Angemessenheit und Wirtschaftlichkeit.
- „Stand der Technik“: Maßnahmen folgen anerkannten Standards und dem aktuellen Technologiestand.
- Kontinuierliche Verbesserung: Das ISMS wird regelmäßig überwacht, geprüft und verbessert (PDCA-Zyklus).
- Security by Design & by Default: Sicherheitsanforderungen werden frühzeitig in Prozesse, Projekte, Systeme und Dienste integriert.
- Compliance: Gesetzliche, regulatorische und vertragliche Anforderungen, inkl. Datenschutz (DSGVO/BDSG), werden eingehalten.
- Awareness & Verantwortung: Jede Person trägt Verantwortung für Informationssicherheit und wird regelmäßig sensibilisiert und geschult.

3 Ziele der Informationssicherheit

- Geschäftsfähigkeit sichern: Schutz geschäftskritischer Prozesse, Produkte und Services.
- Schutz von Informationen und Geschäftsgeheimnissen: Vertrauliche, personenbezogene und betriebsrelevante Daten werden angemessen geschützt.

- Risiken reduzieren: Eintrittswahrscheinlichkeit und Auswirkung relevanter Risiken werden auf ein akzeptiertes Niveau gesenkt.
- Regelkonformität erreichen: Erfüllung gesetzlicher und vertraglicher Anforderungen sowie Anforderungen von Kunden und Partnern.
- Resilienz stärken: Vorbereitetes Handeln bei Sicherheitsvorfällen, Notfällen und Krisen.

4 Rollen und Verantwortlichkeiten

Geschäftsleitung: Genehmigt diese Leitlinie, definiert Sicherheitsziele und Risikobereitschaft (Risk Appetite), stellt Ressourcen bereit, bewertet regelmäßig die Wirksamkeit des ISMS und entscheidet über wesentliche Risiken.

Informationssicherheitsbeauftragte/r (ISB): Berät die Leitung, koordiniert das ISMS, erstellt Vorgaben, überwacht die Umsetzung, berichtet regelmäßig an die Geschäftsleitung und initiiert Sensibilisierungsmaßnahmen.

Führungskräfte: Setzen die Leitlinie in ihren Bereichen um, tragen Verantwortung für die Einhaltung und melden Abweichungen.

Mitarbeitende: Befolgen Richtlinien und Arbeitsanweisungen, melden Sicherheitsvorfälle und Verdachtsfälle unverzüglich.

Datenschutzbeauftragte/r (DSB): Stellt die Einhaltung der datenschutzrechtlichen Vorgaben sicher und arbeitet eng mit dem ISB zusammen.

Dienstleister/Lieferanten: Werden vertraglich verpflichtet, die relevanten Sicherheitsanforderungen einzuhalten und dies nachzuweisen.

5 Risikomanagement

Die Pröll GmbH etabliert und betreibt ein einheitliches Risikomanagement für Informationssicherheit. Risiken werden entlang eines definierten Prozesses identifiziert, analysiert, bewertet und durch geeignete Maßnahmen behandelt. Die Risikokriterien (u. a. Schutzziele, Bewertungsskalen, Akzeptanzkriterien) werden dokumentiert und regelmäßig überprüft. Der Risikoappetit wird von der Geschäftsleitung festgelegt.

Risikobeurteilungen finden anlassbezogen (z. B. bei Projekten, Änderungen, Vorfällen) und periodisch statt. Restrisiken, die die Akzeptanzkriterien überschreiten, sind der Geschäftsleitung zur Entscheidung vorzulegen.

6 Klassifikation und Umgang mit Informationen

Informationen werden mindestens in die Klassen „Öffentlich“, „Intern“, „Vertraulich“ und „Streng vertraulich“ eingeteilt. Für jede Klasse gelten Handhabungsvorgaben (Erstellung, Speicherung, Verarbeitung, Übertragung, Weitergabe, Archivierung, Löschung/Vernichtung). Die Eigentümer („Information Owner“) sind für die korrekte Einstufung verantwortlich.

7 Grundanforderungen und Maßnahmenrahmen

- Organisation & Richtlinien: Etablierung und Pflege verbindlicher Richtlinien (z. B. Acceptable Use, Passwort, Mobile Arbeit, Cloud, Lieferanten).
- Identitäts- und Berechtigungsmanagement: Rollen-/Rechtekonzepte, Need-to-know, MFA, regelmäßige Rezertifizierungen.
- Asset- und Konfigurationsmanagement: Vollständiges Inventar, Baselines, Härtung, sichere Konfigurationen.
- Patch- und Schwachstellenmanagement: Regelmäßige Updates, priorisierte Behebung, Nachverfolgung und Reporting.
- Malwareabwehr & EDR: Angemessene Schutzmechanismen an Endpunkten, Servern und Gateways, zentrale Auswertung von Ereignissen.
- Netzwerksicherheit: Segmentierung, sichere Fernwartung/VPN, Firewalls, Protokollierung und Angriffserkennung.
- Kryptographie: Einsatz geeigneter, aktueller Verfahren und Schlüsselverwaltung nach festgelegten Standards.
- Sicherer Softwarelebenszyklus: Security by Design, Code-Reviews, Tests, Schwachstellenanalysen, SBOM soweit angemessen.
- Physische Sicherheit & Umgebung: Zutrittskontrollen, Schutz von Serverräumen, Notstrom/USV, Brand- und Wasserschutz.
- Dokumentation & Nachweisführung: Nachvollziehbarkeit von Entscheidungen, Maßnahmen und Prüfungen.

8 Ereignis- und Schwachstellenmanagement

Sicherheitsrelevante Ereignisse und Schwachstellen sind zentral zu erfassen, zu bewerten und zu behandeln. Ein Incident-Management-Prozess mit Meldewegen, Reaktionszeiten, Eskalationsstufen und Kommunikationsregeln ist verbindlich. Relevante Protokolle werden zweck- und risikogerecht aufgezeichnet und ausgewertet unter Beachtung rechtlicher Vorgaben.

9 Notfall- und Kontinuitätsmanagement

Zur Aufrechterhaltung kritischer Geschäftsprozesse bei Störungen betreibt die Pröll GmbH ein angemessenes Business Continuity Management (BCM). Dies umfasst Business Impact Analysen (BIA), Strategien und Notfall-/Wiederanlaufpläne, regelmäßige Übungen sowie die Nachbereitung von Ereignissen.

10 Sensibilisierung und Schulung

Alle Mitarbeitenden werden anlassbezogen und regelmäßig zu Informationssicherheit, Datenschutz und sicherem Arbeiten geschult. Spezifische Zielgruppen (z. B. Administratoren, Entwickler, Führungskräfte) erhalten vertiefte Trainings.

11 Steuerung externer Dienstleister und Cloud-Nutzung

Externe Dienstleister und Cloud-Anbieter werden vor Beauftragung bewertet und vertraglich auf Sicherheitsanforderungen verpflichtet. Es erfolgen regelmäßige Kontrollen und Nachweise (z. B. Auditberichte, Zertifikate). Datenhoheit, Speicherorte, Subdienstleister und Exit-Strategien sind vertraglich zu regeln.

12 Rechtliche, regulatorische und vertragliche Anforderungen

Die Einhaltung relevanter Gesetze, Normen und Verträge (u. a. DSGVO/BDSG, Urheber- und Arbeitsrecht, branchenspezifische Pflichten) ist sicherzustellen. Abweichungen und Verstöße sind zu melden und zu behandeln.

13 Überwachung, Bewertung und Verbesserung

Die Wirksamkeit des ISMS wird mittels Kennzahlen, internen Audits, Managementbewertungen und externen Prüfungen bewertet. Erkenntnisse fließen in Korrektur- und Verbesserungsmaßnahmen ein. Die Leitlinie wird mindestens jährlich oder anlassbezogen überprüft und bei Bedarf aktualisiert.

14 Inkrafttreten und Gültigkeit

Diese Leitlinie tritt mit Veröffentlichung in Kraft. Verstöße können arbeits-, zivil- und strafrechtliche Konsequenzen nach sich ziehen. Alle leitlinienbezogenen Dokumente (Richtlinien, Prozesse, Standards) sind Bestandteil des ISMS und verbindlich einzuhalten.