INFORMATIONSSICHERHEITS-LEITLINIE

Vertraulichkeitsstufe:	Intern
Erstellt von:	ISB
Verantwortlich:	ISB
Freigegeben durch:	<FREIGEGEBEN_VON>
Version:	1.0
Normbezug:	ISO/IEC 27001:2022 Controls 5.1, 5.4, 5.36; Clauses 4.3, 5.2

Änderungshistorie

Version	Datum	Geändert von	Änderung

1. Zweck, Geltungsbereich und Zielgruppe

Diese Informationssicherheits-Leitlinie definiert die übergeordneten Grundsätze und Verpflichtungen von <UNTERNEHMENSNAME> zum Schutz von Informationen und informationsverarbeitenden Systemen. Sie bildet das strategische Dach des Informationssicherheitsmanagementsystems (ISMS) gemäß ISO/IEC 27001:2022.

Sie gilt für alle Mitarbeitenden, Führungskräfte, Zeitarbeitskräfte, Praktikanten, externe Dienstleister sowie sonstige Dritte, die im Rahmen ihrer Tätigkeit Zugang zu Informationen oder IT-Systemen von <UNTERNEHMENSNAME> haben.

> 👉 Hinweis: Der Zweck dieses Dokuments ist es, die strategische Ausrichtung der Informationssicherheit festzulegen. Erklären Sie hier, warum Informationssicherheit für Ihr Unternehmen wichtig ist. Beispiel: „Wir verarbeiten sensible Kundendaten und müssen das Vertrauen unserer Partner schützen." Der Geltungsbereich definiert, für wen diese Leitlinie gilt – in der Regel für alle im Unternehmen und externe Dienstleister.

2. Begriffsklärungen

Folgende Begriffe werden in dieser Leitlinie verwendet:

Begriff	Definition
Informationssicherheit	Schutz von Informationen hinsichtlich Vertraulichkeit, Integrität und Verfügbarkeit durch Anwendung eines Risikomanagementprozesses.
ISMS	Informationssicherheitsmanagementsystem – systematischer Ansatz zur Steuerung und kontinuierlichen Verbesserung der Informationssicherheit.
Informationswert	Schutzbedarf einer Information, der sich aus ihrer Vertraulichkeit, Integrität und Verfügbarkeit ergibt.
ISB	Informationssicherheitsbeauftragte/r – die Person, die das ISMS operativ koordiniert.
<HIER_ERGAENZEN>	<HIER_ERGAENZEN>

> 👉 Hinweis: Ergänzen Sie hier weitere Begriffe, die in Ihrem Unternehmen spezifisch sind. Zum Beispiel: interne Systemnamen, Abkürzungen für Abteilungen, branchenspezifische Fachbegriffe. Ziel ist, dass jeder Leser das Dokument ohne Rückfragen versteht.

3. Grundsätze und Verpflichtungen

3.1 Strategische Bedeutung

Informationssicherheit ist ein integraler Bestandteil der Unternehmensstrategie von <UNTERNEHMENSNAME>. Die Geschäftsführung bekennt sich zur Umsetzung und kontinuierlichen Verbesserung des ISMS gemäß ISO/IEC 27001:2022 und stellt die hierfür notwendigen Ressourcen bereit.

<HIER_STRATEGISCHE_BEGRUENDUNG_ERGAENZEN>

> 👉 Hinweis: Hier zeigen Sie, dass Informationssicherheit „Chefsache" ist. Formulieren Sie, warum Ihr Unternehmen Sicherheit ernst nimmt – etwa: „Wir verarbeiten sensible Kundendaten", „Wir erfüllen gesetzliche Vorgaben" oder „Wir schützen unser geistiges Eigentum". ISO 27001 Clause 5.1 verlangt dieses Commitment der Geschäftsführung.

3.2 Schutzziele (CIA-Triade)

Alle Maßnahmen der Informationssicherheit orientieren sich an den drei grundlegenden Schutzzielen:

- **Vertraulichkeit (Confidentiality):** Informationen sind nur für befugte Personen zugänglich. Unbefugte erhalten keinen Zugriff auf sensible Daten.
- **Integrität (Integrity):** Informationen sind korrekt, vollständig und unverändert. Manipulationen werden verhindert oder erkannt.
- **Verfügbarkeit (Availability):** Informationen und Systeme sind für berechtigte Nutzer bei Bedarf verfügbar und funktionsfähig.

Weitere Schutzziele wie Authentizität, Nachvollziehbarkeit und Nichtabstreitbarkeit werden je nach Informationswert und Geschäftsprozess ergänzt.

> 👉 Hinweis: Die CIA-Triade ist das Fundament der Informationssicherheit. Einfach erklärt: Vertraulichkeit = „Nur die Richtigen sehen es“ (z.B. Passwörter für Buchhaltungssystem), Integrität = „Es ist nicht manipuliert“ (z.B. Rechnungsdaten), Verfügbarkeit = „Es funktioniert, wenn ich es brauche“ (z.B. E-Mail-Server). Jede Sicherheitsmaßnahme lässt sich einem oder mehreren dieser Ziele zuordnen.

3.3 Verpflichtung zur Einhaltung von Anforderungen

<UNTERNEHMENSNAME> verpflichtet sich zur Einhaltung aller anwendbaren gesetzlichen, regulatorischen und vertraglichen Anforderungen im Bereich der Informationssicherheit. Dies umfasst insbesondere:

- Datenschutz-Grundverordnung (DSGVO)
- <HIER_BRANCHENSPEZIFISCHE_GESETZE_ERGAENZEN>
- Vertragliche Verpflichtungen gegenüber Kunden und Partnern
- Anforderungen aus Zertifizierungen (z.B. ISO 27001)

Eine Übersicht der relevanten rechtlichen Anforderungen findet sich im E-1.04 Rechtskataster.

> 👉 Hinweis: Dieser Abschnitt ist wichtig für Audits nach ISO 27001 Clause 5.2, da die Norm ein explizites „Commitment to satisfy applicable requirements“ fordert. Ergänzen Sie hier branchenspezifische Gesetze wie z.B. KRITIS, NIS-2, BAIT, VAIT, KDGV oder sonstige regulatorische Vorgaben, die für Ihr Unternehmen gelten.

3.4 Kontinuierliche Verbesserung

<UNTERNEHMENSNAME> verpflichtet sich zur kontinuierlichen Verbesserung des ISMS. Dies erfolgt durch:

- Regelmäßige Überprüfung und Bewertung der Wirksamkeit von Sicherheitsmaßnahmen
- Durchführung interner Audits und Management Reviews
- Auswertung von Sicherheitsvorfällen und Ableitung von Verbesserungsmaßnahmen
- Anpassung an neue Bedrohungen, Technologien und Geschäftsanforderungen

> 👉 Hinweis: ISO 27001 Clause 5.2 verlangt ein „Commitment to continual improvement“. Gemeint ist: Das ISMS ist kein starres System, sondern wird ständig weiterentwickelt. Praktisch bedeutet das: Nach Vorfällen schauen Sie, was schiefgelaufen ist. Nach Audits setzen Sie Verbesserungen um. Mindestens jährlich prüfen Sie, ob alles noch passt.

3.5 Risikobasierter Ansatz

Die Umsetzung von Sicherheitsmaßnahmen erfolgt risikobasiert. Das bedeutet: Ressourcen werden dort eingesetzt, wo die größten Risiken für das Unternehmen bestehen. Die Risikobewertung erfolgt gemäß P-1.03 Risikomanagement-Richtlinie.

> 👉 Hinweis: „Risikobasiert“ heißt: Sie müssen nicht alles zu 100% absichern, sondern sich auf die wichtigsten Risiken konzentrieren. Beispiel: Die Finanzbuchhaltung braucht strengere Zugriffsbeschränkungen als der öffentliche Bereich der Website. Der detaillierte Risikomanagement-Prozess wird in einer eigenen Richtlinie beschrieben.

4. Informationssicherheitsziele

Die Informationssicherheitsziele von <UNTERNEHMENSNAME> leiten sich aus der Geschäftsstrategie und den identifizierten Risiken ab. Sie bilden den Rahmen für die operative Umsetzung des ISMS und werden regelmäßig überprüft und angepasst.

Die konkreten, messbaren Sicherheitsziele sind in E-1.06 ISMS-Ziele dokumentiert. Beispiele für Informationssicherheitsziele:

- Reduzierung der durchschnittlichen Reaktionszeit bei Sicherheitsvorfällen auf < <HIER_ZIELWERT_ERGAENZEN> Stunden
- Durchführung von Awareness-Schulungen für 100% der Mitarbeitenden mindestens einmal jährlich
- Einhaltung einer Verfügbarkeit von mindestens <HIER_ZIELWERT_ERGAENZEN>% für kritische IT-Systeme
- <HIER_WEITERE_ZIELE_ERGAENZEN>

> 👉 Hinweis: ISO 27001 Clause 5.2 verlangt, dass die Leitlinie entweder Sicherheitsziele enthält ODER einen Rahmen setzt, um diese festzulegen. Wir nutzen hier den Rahmen-Ansatz: Die Leitlinie gibt die Richtung vor, die konkreten Ziele mit KPIs werden in einem separaten Dokument gepflegt. So müssen Sie die Leitlinie nicht jedes Mal ändern, wenn sich ein Zielwert ändert.

5. Umsetzung durch themenspezifische Richtlinien

Die Sicherheitsmaßnahmen werden gemäß der Risikobewertung geplant, umgesetzt und dokumentiert. Dabei kommen die Controls gemäß ISO/IEC 27001:2022 Annex A zum Einsatz. Die Auswahl der anzuwendenden Controls ist im S-1.01 Statement of Applicability (SOA) begründet und dokumentiert.

Konkrete Vorgaben und Prozesse sind in themenspezifischen Richtlinien festgelegt, darunter:

- Risikomanagement: P-1.03 Risikomanagement-Richtlinie
- Zugriffskontrolle: P-4.01 Identitäts-/Zugriffsrichtlinie
- Incident Management: P-5.01 Incident-Management-Richtlinie
- Personalsicherheit: P-3.01 Personalsicherheits-Richtlinie
- Weitere themenbezogene Richtlinien gemäß S-1.01 Statement of Applicability (SOA)

> 👉 Hinweis: Hier listen Sie auf, welche konkreten Richtlinien in Ihrem Unternehmen gelten. Die Leitlinie ist das „Dach“, darunter kommen spezifische Policies. Je nach Größe Ihres Unternehmens können dies 10–30 einzelne Richtlinien sein. Das SOA (Statement of Applicability) zeigt die vollständige Übersicht aller Controls und der zugehörigen Dokumente.

6. Verantwortung der Geschäftsführung

Die Geschäftsführung von <UNTERNEHMENSNAME> trägt die Gesamtverantwortung für die Informationssicherheit. Sie stellt sicher, dass:

- ausreichende Ressourcen (Budget, Personal, Zeit) für das ISMS bereitgestellt werden
- die Informationssicherheitsleitlinie mit der strategischen Ausrichtung des Unternehmens vereinbar ist
- die Anforderungen des ISMS in die Geschäftsprozesse integriert werden

Die detaillierte Beschreibung aller Rollen und Verantwortlichkeiten im ISMS – einschließlich ISB, Führungskräfte, Mitarbeitende und externe Dienstleister – ist in der P-1.02 ISMS-Organisations-Richtlinie geregelt.

> 👉 Hinweis: Dies ist das „Top Management Commitment“ aus ISO 27001 Clause 5.1. Die Geschäftsführung muss das ISMS nicht selbst betreiben, aber sie muss es aktiv unterstützen. Die konkreten Rollen (wer macht was) werden in der ISMS-Organisations-Richtlinie beschrieben – hier geht es nur um das grundsätzliche Bekenntnis.

7. Kommunikation und Verfügbarkeit der Leitlinie

Diese Informationssicherheits-Leitlinie wird allen Mitarbeitenden zur Verfügung gestellt und ist über <HIER_SPEICHERORT_ERGAENZEN> zugänglich. Neue Mitarbeitende werden im Rahmen des Onboardings über die Leitlinie informiert.

Bei Bedarf wird eine zusammengefasste Version der Leitlinie für interessierte Parteien (z.B. Kunden, Partner, Auditoren) bereitgestellt. Die Freigabe erfolgt durch <HIER_FREIGABESTELLE_ERGAENZEN>.

> 👉 Hinweis: ISO 27001 Clause 5.2 verlangt, dass die Leitlinie „kommuniziert wird“ und „verfügbar ist“. Praktisch: Stellen Sie die Leitlinie ins Intranet, erwähnen Sie sie im Onboarding, versenden Sie eine E-Mail bei Aktualisierungen. Auditoren fragen gezielt danach, ob Mitarbeitende wissen, dass es eine Leitlinie gibt und wo sie zu finden ist.

8. Referenzierte Dokumente

Diese Leitlinie steht in Zusammenhang mit folgenden Dokumenten:

- ISMS-Organisations-Richtlinie: P-1.02 ISMS-Organisations-Richtlinie
- ISMS-Ziele: E-1.06 ISMS-Ziele
- Geltungsbereich des ISMS: P-1.02 ISMS-Organisations-Richtlinie
- Statement of Applicability (SOA): S-1.01 Statement of Applicability (SOA)
- Risikomanagement-Richtlinie: P-1.03 Risikomanagement-Richtlinie
- Rechtskataster: E-1.04 Rechtskataster
- Benennung ISB: E-1.01 Benennung ISB
- Interner Auditplan: S-1.04 Auditplan
- Themenbezogene Richtlinien (vollständige Liste im SOA)

> 👉 Hinweis: Hier verknüpfen Sie die Leitlinie mit anderen Dokumenten Ihres ISMS. Diese Liste zeigt Auditoren, dass Ihr ISMS strukturiert ist und verschiedene Aspekte abdeckt. Passen Sie die Verweise an Ihre tatsächliche Dokumentenstruktur an. Tipp: Nutzen Sie einheitliche Dokumenten-IDs (z.B. P-1.02, P-1.03), damit Verweise eindeutig sind.

9. Gültigkeit und Überprüfung

Diese Leitlinie ist gültig ab <GUELTIG_AB_DATUM> und wird mindestens jährlich durch den/die ISB überprüft und bei Bedarf aktualisiert. Überprüfungen erfolgen zudem anlassbezogen bei:

- Wesentlichen Änderungen der Geschäftstätigkeit oder Unternehmensstruktur
- Neuen gesetzlichen oder regulatorischen Anforderungen
- Schwerwiegenden Sicherheitsvorfällen
- Ergebnissen aus internen oder externen Audits

Die Leitlinie und alle referenzierten Dokumente unterliegen der Dokumentenlenkung gemäß P-1.05 Dokumentenlenkungsrichtlinie.

> 👉 Hinweis: ISO 27001 verlangt regelmäßige Reviews – mindestens einmal pro Jahr. Dies können Sie im Management Review machen. Dokumentieren Sie das Datum der letzten Überprüfung in der Änderungshistorie oben. Tipp: Setzen Sie sich eine jährliche Erinnerung.