📘 Regelwerk zur ISO/IEC 27001

Version: 1.0
Stand: 15. Mai 2025
Unternehmen: [Dein Unternehmensname]
Geltungsbereich: Alle Unternehmensbereiche, IT-Systeme und Prozesse, die mit der Verarbeitung von Informationen zu tun haben.

---

1. Ziel des Regelwerks

Das Ziel dieses Regelwerks ist es, Vertraulichkeit, Integrität und Verfügbarkeit von Informationen im Unternehmen sicherzustellen – gemäß den Anforderungen der ISO/IEC 27001:2022.

---

2. Geltungsbereich des ISMS

Das ISMS umfasst:

- Interne IT-Systeme, Netzwerke und Endgeräte
- Cloud-Dienste und externe IT-Dienstleister
- Verarbeitungsprozesse personenbezogener und geschäftskritischer Daten
- Mitarbeiter, Partner und Dienstleister mit Zugriff auf Unternehmensdaten

---

3. Informationssicherheitsziele

- Schutz sensibler Daten vor unbefugtem Zugriff (Vertraulichkeit)
- Schutz vor Manipulation und ungewollter Veränderung (Integrität)
- Sicherstellung der Verfügbarkeit von Informationen und IT-Systemen (Verfügbarkeit)
- Einhaltung gesetzlicher, vertraglicher und regulatorischer Anforderungen

---

4. Organisation der Informationssicherheit

4.1 Rollen & Verantwortlichkeiten

- **Informationssicherheitsbeauftragter (ISB):** Verantwortlich für Aufbau, Pflege und Überwachung des ISMS.
- **Geschäftsführung:** Trägt die Gesamtverantwortung.
- **Fachabteilungen:** Umsetzung der Sicherheitsvorgaben in ihren Bereichen.
- **Alle Mitarbeitenden:** Verpflichtet zur Einhaltung der Sicherheitsregeln.

4.2 Governance & Kontrolle

- Einrichtung eines **ISMS-Teams**
- Regelmäßige Management Reviews
- Interne Audits mindestens einmal jährlich

---

5. Risikomanagement

5.1 Risikoidentifikation

- Regelmäßige Risikoanalysen aller Systeme und Prozesse

5.2 Risikobewertung

- Eintrittswahrscheinlichkeit + Auswirkung → Risikoklasse

5.3 Risikobehandlung

- Akzeptieren, Reduzieren, Übertragen oder Vermeiden

---

6. Sicherheitsrichtlinien

6.1 Acceptable Use Policy

- Verbot privater Nutzung unternehmenskritischer Systeme
- Keine Weitergabe von Passwörtern
- Keine Installation nicht autorisierter Software

6.2 Passwortregeln

- Min. 12 Zeichen, Groß-/Kleinschreibung, Zahl + Sonderzeichen
- Passwortwechsel alle 180 Tage (wo technisch notwendig)

6.3 Zugriffskontrolle

- Zugriff nur nach dem Prinzip „Need to Know“
- Rechtevergabe durch zentralen Freigabeprozess
- Sofortige Sperrung bei Mitarbeiteraustritt

---

7. Physische und Umweltbezogene Sicherheit

- Zutrittskontrollen zu Serverräumen
- Alarmanlagen und Brandschutzmaßnahmen
- Besucherprotokollierung

---

8. Betriebssicherheit

- Regelmäßige Backups, Tests der Wiederherstellung
- Monitoring sicherheitsrelevanter Ereignisse
- Patching- und Updateprozesse für Systeme

---

9. Kommunikationssicherheit

- Verschlüsselung vertraulicher Daten (TLS, VPN, E-Mail-Verschlüsselung)
- DLP (Data Loss Prevention) bei sensiblen Daten

---

10. Lieferantenbeziehungen

- Prüfung von IT-Dienstleistern vor Vertragsabschluss
- Abschluss von AV-Verträgen (Art. 28 DSGVO)
- Kontrolle der Einhaltung vereinbarter Sicherheitsmaßnahmen

---

11. Vorfallmanagement

- Dokumentation aller Sicherheitsvorfälle
- Meldepflicht intern innerhalb von 2 Stunden
- Bewertung und Klassifikation (Kritikalität)
- Lessons Learned und Maßnahmen

---

12. Notfallmanagement / Business Continuity

- Erstellung eines Notfallhandbuchs
- Durchführung von Notfallübungen (mind. jährlich)
- Wiederanlaufpläne für kritische Systeme

---

13. Schulungen und Sensibilisierung

- Jährliche Schulungen für alle Mitarbeiter
- Awareness-Kampagnen zu aktuellen Bedrohungen (z. B. Phishing)
- Onboarding-Sicherheitseinweisung

---

14. Kontinuierliche Verbesserung

- Regelmäßige ISMS-Reviews
- Einleitung von Korrektur- und Verbesserungsmaßnahmen
- Berücksichtigung von Feedback und Auditergebnissen

---

15. Dokumentation und Nachweisführung

- ISMS-Handbuch
- Risikoanalysen und Maßnahmenpläne
- Auditberichte, Schulungsnachweise, Vorfallsdokumentationen

---

16. Anwendbare Normen und Gesetze

- ISO/IEC 27001:2022
- DSGVO
- BDSG
- Branchenspezifische Vorgaben (z. B. KRITIS, TISAX)

---

17. Gültigkeit und Revision

- Dieses Regelwerk tritt mit sofortiger Wirkung in Kraft.
- Nächste Überprüfung: [12 Monate nach Inkrafttreten]
- Verantwortlich für Revision: ISB