

# IS-200 - ISMS Richtlinie - Draft

- Über die Seite:
- Ziel und Zweck:
- Geltungsbereich:
- Regelungen:
- Zuständig / verantwortlich:
- Dokumente
- Arbeitsweise
- Weiterführende Information:
- Verbindlichkeit:
- Dokumentenmanagement:
- Änderungshistorie:

## Über die Seite:

Seitentyp	Vertraulichkeitsklasse	Zielgruppe	Version	Seitenstatus	Seiteneigner	Prüfer
Richtlinie	intern	alle Mitarbeiter	V 1.0	Entwurf	ISB	@Name

## Ziel und Zweck:

Als Ergänzung und Konkretisierung der Informationssicherheitsleitlinie werden in dieser Richtlinie grundlegende Arbeitsweisen des ISMS spezifiziert.

## Geltungsbereich:

Der Geltungsbereich dieser Richtlinie erstreckt sich über den gesamten Geltungsbereich der VdS 10000 und ist für alle Mitarbeiter des Unternehmens bindend.

## Regelungen:

### Grundsätze des ISMS

Das ISMS arbeitet nach den folgenden Grundsätzen:

- Das ISMS orientiert sich an den VdS-Richtlinien 10000 in der jeweils aktuellen Fassung und setzt – soweit nicht anders vermerkt – deren Anforderungen um. Es wird von der VdS Schadenverhütung GmbH in den vorgesehenen Abständen (re)zertifiziert.
- Es berücksichtigt die für die Organisation relevanten gesetzlichen Vorgaben in Sachen Informationssicherheit, insbesondere die folgenden:
  - Datenschutz-Grundverordnung der Europäischen Union (EU-DSGVO)
  - Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD)
  - Handelsgesetzbuch (HGB)
  - GmbH-Gesetz (GmbHG)
  - Aktiengesetz (AktG)
  - Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG)
  - Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG)
  - ...
- Sämtliche Sicherheitsmaßnahmen werden so gewählt und koordiniert, dass ein angemessenes Sicherheitsniveau mit möglichst geringem Aufwand erreicht wird.

## Zuständig / verantwortlich:

Das ISMS wird insbesondere (aber nicht nur) durch den Informationssicherheitsbeauftragten (ISB) und das Informationssicherheitsteam (IST) getragen.

### Informationssicherheitsbeauftragte (ISB)

Der ISB ist der Prozesseigentümer des ISMS:

- Der ISB steuert das ISMS und wirkt so darauf hin, dass die in der Leitlinie zur Informationssicherheit (IS-Leitlinie) definierten Ziele der Informationssicherheit erreicht werden.
- Er koordiniert und prüft dazu unter anderem die technischen und organisatorischen Maßnahmen für die Informationssicherheit.
- Darüber hinaus sorgt er für das kontinuierliche Verbessern der Informationssicherheit. Dies umfasst insbesondere das Anpassen der Informationssicherheit an neue Bedrohungen, Änderungen im technischen und organisatorischen Umfeld und an neue gesetzliche, betriebliche und vertragliche Anforderungen.
- Als zentraler Ansprechpartner für die Informationssicherheit berät er das Topmanagement sowie die Mitarbeiter in allen Belangen der Informationssicherheit.
- Er überwacht die Einhaltung der Informationssicherheitsziele sowie die Strategien für die Informationssicherheit und steuert das ISMS.
- Der ISB ist in seiner Funktion organisatorisch unabhängig und berichtet direkt an das Topmanagement (Stabsstelle).
- Er berichtet mindestens jährlich an das Informationssicherheitsteam (IST) über den aktuellen Stand der Informationssicherheit, insbesondere über Mängel, Risiken und Sicherheitsvorfälle.

## **Informationssicherheitsteam (IST)**

Das IST ist das zentrale Steuerungsgremium des Unternehmens für die Informationssicherheit. Es tagt monatlich sowie bei Bedarf. Es nimmt die folgenden Aufgaben wahr:

- Unterstützung der unternehmensweiten Koordinierung und Lenkung der Maßnahmen zur Informationssicherheit
- Unterstützung der Erstellung von Richtlinien und Verfahren zur Informationssicherheit
- Austausch zu sicherheitsrelevanten Themen, insbesondere:
  - neue oder geänderte Bedrohungen und Schwachstellen
  - Änderungen an Geschäftsprozessen oder der Organisationsstruktur
  - geplante oder durchgeführte Änderungen der IT-Infrastruktur

Das IST setzt sich aus den folgenden Positionen zusammen:

- ein Vertreter des Topmanagements
- der Informationssicherheitsbeauftragte (ISB)
- der Datenschutzmanager (DSM) sowie der Datenschutzbeauftragte (DSB)
- die IT-Verantwortlichen
- ein Vertreter des Betriebsrats

Bei Bedarf können weitere interne oder externe Gäste hinzugezogen werden.

-- ALTERNATIVE --

## **Informationssicherheitsbeauftragter (ISB)**

### **Aufgaben**

- Steuerung & kontinuierliche Verbesserung des ISMS
- Kennzahlen ermitteln, Management-Review vorbereiten
- Richtlinien pflegen, Sicherheitsmaßnahmen überwachen
- Primärer Ansprechpartner für Informationssicherheit
- Koordination interner/Externer Audits

### **Befugnisse**

- Weisungs- & Vetorecht bei IS-Belangen
- Zutritt zu allen IT-Bereichen
- Mitsprache bei Projekten/Beschaffungen

### **Besetzung**

- ISB: <Name>    Stellvertreter: <Name>

### **Kenntnisse / Fähigkeiten**

- Fundiertes Wissen VdS 10000
- Erfahrung Risikomanagement, Auditmethodik
- Kontinuierliche fachliche Weiterbildung

## **Informationssicherheitsteam (IST)**

### **Aufgaben (VdS 4.6)**

- Monatliche Steuerung des ISMS
- Freigabe/Empfehlung von Richtlinien & Maßnahmen
- Beratung bei Bedrohungen / Änderungen
- Notfallunterstützung

### **Befugnisse**

- Eskalationsrecht an GF
- Einberufung ad-hoc-Sitzungen

### **Besetzung**

Top-Management-Vertreter, ISB, DSB, IT-Verantw., weitere Experten nach Bedarf

### **Kenntnisse/Fähigkeiten**

- Fachkenntnis jeweiliger Domänen
- Entscheidungs- & Abstimmungs-kompetenz

## **IT-Verantwortlicher**

### **Aufgaben**

- Umsetzung technischer/organisatorischer IS-Maßnahmen
- Patch- & Backup-Prozesse
- Rechte- und Zugangskontrolle
- Dokumentation kritischer IT-Systeme

### **Befugnisse**

- System- und Netzwerkkonfiguration
- Sperrung kritischer Zugänge bei Verstößen

**Besetzung**

- IT-Leiter: <Name> Stellvertreter: <Name>

**Kenntnisse/Fähigkeiten**

- Netzwerk- & Systemadministration, Notfall-/Backup-Verfahren, VdS-IT-Anforderungen

**Risikoeigentümer (Prozess-/System-/Informationseigner)****Aufgaben**

- Klassifizierung & Schutzbedarf
- Mitwirkung bei Risikoanalyse & -behandlung
- Freigabe von Restrisiken oder Eskalation an GF

**Befugnisse**

- Entscheidung über akzeptable Risiken im Verantwortungsbereich

**Besetzung**

- Eigentümer: <Name> Stellvertreter: <Name>

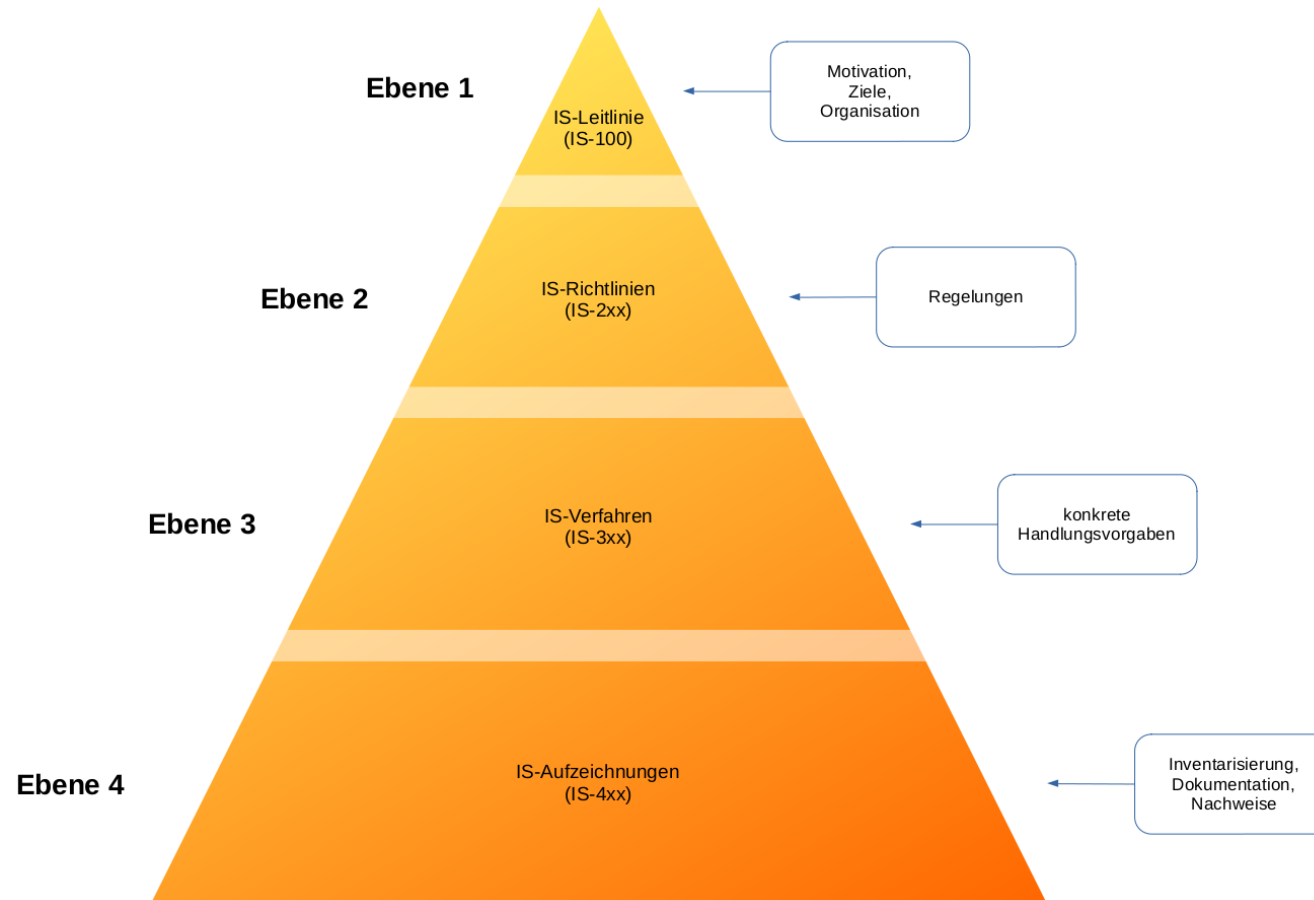
**Kenntnisse/Fähigkeiten**

- Prozess / System-Know-how
- Grundlagen Risikomanagement

---

# Dokumente

Das ISMS wird durch verschiedene Dokumente definiert und gesteuert. Diese sind in vier Ebenen unterteilt:



## Ebene 1 - IS-Leitlinie (IS-100)

Die Leitlinie zur Informationssicherheit (IS-Leitlinie) ist das zentrale Dokument für die gesamte Informationssicherheit. In ihr sind die zu erreichenden Ziele durch das vorgegeben und Verantwortlichkeiten definiert.

Die IS-Leitlinie wird vom Topmanagement erstellt, jährlich von ihm auf Aktualität geprüft und bei Bedarf angepasst.

Dokument	Titel	Eigentümer	Umsetzung
IS-100	IS-Leitlinie	Topmanagement	QM-Software

## Ebene 2 - IS-Richtlinien (IS-2xx)

Zur Unterstützung und Konkretisierung der IS-Leitlinie werden Regelungen für die Informationssicherheit in einzelnen Dokumenten, den IS-Richtlinien, gesammelt. Sie werden durch den ISB unter Einbeziehung

des IST erstellt und vom Topmanagement in Kraft gesetzt. IS-Richtlinien werden jährlich vom ISB auf Aktualität geprüft und ggf. aktualisiert.

Dokument	Titel	Eigentümer	Umsetzung
IS-200	ISMS Richtlinie	ISB	QM-Software
IS-201	Regelungen für Nutzer		
IS-202	Protokollierung und Missbrauchskontrolle		
IS-203	Internetzugang für die private Nutzung (Sozial-PCs und WLAN für Mitarbeiter)		
IS-204	Regelungen für Auftragnehmer		
IS-205	Mobile IT-Systeme		
IS-206	Mobile Datenträger		



IS-207	IT-Outsourcing und Cloud Computing		
IS-208	Speicherorte		
IS-209	Störungen und Ausfälle		
IS-210	Sicherheitsvorfälle		
IS-211	Home Office		

### Ebene 3 - IS-Verfahren (IS-3xx)

IS-Verfahren legen Abläufe fest, die für die Aufrechterhaltung der Informationssicherheit wichtig sind. Sie sind Bestandteil des Qualitätsmanagements und unterliegen den entsprechenden Regularien.

Dokument	Titel	Eigentümer	Umsetzung
IS-300	Dokumentenmanagement: Lenkung der IS-Dokumente	Leitung QM	QM-Software
IS-301	Personalmanagement: Aufnahme der Tätigkeit	Leitung Personalmanagement	
IS-302	Personalmanagement: Beendigung oder Wechsel der Tätigkeit	Leitung Personalmanagement	
IS-303	Personalmanagement: Schulungs- und Sensibilisierungsmaßnahmen	Leitung Personalmanagement	
IS-310	IT: Inbetriebnahme und Änderung von IT-Systemen	IT-Verantwortlicher	
IS-311	IT: Ausmusterung und Wiederverwendung von IT-Systemen	IT-Verantwortlicher	
IS-312	IT: Sicherheitsupdates	IT-Verantwortlicher	
IS-313	IT: Verlust mobiler IT-Systeme	IT-Verantwortlicher	

IS-314	IT: Anlegen und Ändern von Zugängen und Zugriffsrechten und Zurücksetzen von Authentifizierungsmerkmalen	IT-Verantwortlicher
IS-315	IT: Datensicherung, -wiederherstellung und -archivierung	IT-Verantwortlicher
IS-316	IT: Umgebung	IT-Verantwortlicher
IS-320	Mitarbeiter: Verlust mobiler IT-Systeme	ISB
IS-321	Mitarbeiter: Wahl sicherer Passwörter	ISB
IS-330	Reaktion: Aktualität des Wissens	ISB
IS-331	Reaktion: Reaktion auf Störungen und Ausfälle	ISB
IS-332	Reaktion: Reaktion auf Sicherheitsvorfälle	ISB
IS-340	Risikomanagement: Risikoanalyse und -behandlung	Leitung Risikomanagement
IS-341	Risikomanagement: Identifizieren von kritischen Teilen der IT-Infrastruktur	Leitung Risikomanagement

#### Ebene 4 - IS-Aufzeichnungen (IS-4xx)

IS-Aufzeichnungen sind Dokumente, die im Zuge des Betriebs des ISMS und im Zuge des Kontinuierlichen Verbesserungsprozesses (KVP) entstehen, z. B. Nachweise über durchgeführte Tätigkeiten.

Sie können in unterschiedlichen Formen vorliegen.

Dokument	Titel	Eigentümer	Umsetzung
IS-400	Dokumentenverzeichnis: Verzeichnis der ISMS-Dokumente	ISB	QM-Software

IS-410	ISMS: Verantwortlichkeiten und nicht durchgeführte Funktionstrennungen	ISB	QM-Software
IS-411	ISMS: Ausnahmen von IS-Richtlinien	ISB	QM-Software
IS-420	Personalmanagement: Inhalte von und Teilnahme an Schulungs- und Sensibilisierungsmaßnahmen	Leitung Fortbildung	XLS-Liste
IS-430	Risikomanagement: Prozesse, kritische Informationen und kritische IT-Ressourcen	ISB	QM-Software
IS-431	Risikomanagement: Durchgeführte Risikoanalysen und -behandlungen	Leitung Risikomanagement	QM-Software
IS-440	IT: Inventarisierung der IT-Systeme	IT- Verantwortlicher	DokuSnap
IS-441	IT: Inbetriebnahme der IT-Systeme (Verzeichnis)	IT- Verantwortlicher	Ticketsystem
IS-442	IT: Ausmusterung der IT-Systeme (Verzeichnis)	IT- Verantwortlicher	Ticketsystem
IS-443	IT: Dokumentation der kritischen IT-Systeme	IT- Verantwortlicher	QM-Software
IS-444	IT: Netzwerkplan	IT- Verantwortlicher	VISIO-Zeichnung

IS-445	IT: Sicherheitsrelevante Einstellungen der Netzübergangspunkte	IT-Verantwortlicher	Kommentarfelder und Ticketsystem
IS-446	IT: Durchführung und Ergebnisse der Tests der Verfahren zur Datensicherung und -wiederherstellung	IT-Verantwortlicher	Ticketsystem
IS-447	IT: Wiederanlaufpläne	IT-Verantwortlicher	QM-Software, als Datei auf den entsprechenden Backup-Medien und als Papierversion im IT-Tresor
IS-448	IT: Abhängigkeiten zwischen kritischen Teilen der IT-Infrastruktur	IT-Verantwortlicher	QM-Software
IS-460	IT-Outsourcing und Cloud Computing	ISB	QM-System
IS-470	Zugänge und Zugriffsrechte: Zugänge	IT-Verantwortlicher	Ticketsystem
IS-471	Zugänge und Zugriffsrechte: Zugriffsrechte	IT-Verantwortlicher	Ticketsystem
IS-472	Zugänge und Zugriffsrechte: Zurückgesetzte Authentifizierungsmerkmale	IT-Verantwortlicher	Ticketsystem
IS-480	Vorfälle: Störungen und Ausfälle (Verzeichnis)	IT-Verantwortlicher	Ticketsystem
IS-481	Vorfälle: Sicherheitsvorfälle (Verzeichnis)	ISB	Ticketsystem

IS-490	Lenkung: Stand des ISMS	ISB	Präsentationen
IS-491	Lenkung: Protokolle IST-Sitzungen	ISB	QM-Software

## Arbeitsweise

Informationssicherheit muss sich stets den gesetzlichen, betrieblichen und vertraglichen Anforderungen sowie an neue technische Bedingungen (insbesondere an neue Bedrohungen und Schwachstellen) anpassen.

Im folgenden wird die Arbeitsweise des ISMS umrissen.

### Erkennen von neuen Anforderungen und Gefährdungen

Das Anforderungsmanagement stellt sicher, dass neue betriebliche, gesetzliche und vertragliche Anforderungen an die Informationssicherheit sowie neue Gefährdungen erkannt werden. Neue Anforderungen und Gefährdungen werden z. B. durch die folgenden Mechanismen bekannt:

- regelmäßige Informationen aus verlässlichen Quellen ( Verfahren IS-330 Reaktion: Aktualität des Wissens)
- Erkenntnisse aus der Nachbereitung von Störungen und Ausfällen ( Verfahren IS-331 Reaktion: Reaktion auf Störungen und Ausfälle)
- Erkenntnisse aus der Nachbereitung von Sicherheitsvorfällen ( Verfahren IS-332 Reaktion: Reaktion auf Sicherheitsvorfälle)
- durchgeführte Risikoanalysen und -behandlungen ( Verfahren IS-340 Risikomanagement: Risikoanalyse und -behandlung)
- das im Unternehmen verankerte Verbesserungs- und Innovationsmanagement

### Risikomanagement

Neue Anforderungen und Gefährdungen werden vom ISB gesammelt. Der ISB trägt dafür Sorge, dass diese bewertet werden. Er wird dabei bei Bedarf vom IST, den Prozesseigentümern und vom Risikomanagement unterstützt. Der ISB sorgt dafür, dass auf Basis dieser Erkenntnisse geeignete Maßnahmen zur Vermeidung, Reduzierung oder Übertragung der Risiken definiert und umgesetzt werden; wenn Risiken nicht angemessen behandelt werden können, werden sie vom Topmanagement akzeptiert und dies dokumentiert ( Verfahren IS-340 Risikomanagement: Risikoanalyse und -behandlung).

### Umsetzung von Maßnahmen

Die Umsetzungen von geplanten Maßnahmen wird vom ISB koordiniert und überwacht. Für die Umsetzung von Maßnahmen kann der ISB Verantwortliche definieren.

## **Management der Ausnahmen**

Richtlinien erlauben Ausnahmen, wenn dies aus betrieblichen, vertraglichen oder gesetzlichen Anforderungen erforderlich ist. Ausnahmen müssen vom ISB im Vorfeld genehmigt und zusammen mit der Begründung in [IS-411 ISMS: Ausnahmen von IS-Richtlinien] dokumentiert werden. Der ISB ist verantwortlich, dass dabei entstehenden Risiken eingeschätzt und ggf. entsprechende Maßnahmen (Vermeidung, Reduzierung, Überwälzen, Akzeptanz) ergriffen werden. Diese kann vom ISB selbst vorgenommen oder in Form einer strukturierten Risikoanalyse und -behandlung (Verfahren IS-340 Risikomanagement: Risikoanalyse und -behandlung) durchgeführt werden.

## **Weiterführende Information:**

- IS-400 - Dokumentenverzeichnis: ISMS-Dokumente
- IS-410 - ISMS: Verantwortlichkeiten und nicht durchgeführte Funktionstrennungen
- IS-411 - ISMS: Ausnahmen von IS-Richtlinien
- IS-490 - Lenkung: Stand des ISMS
- Glossar

## **Verbindlichkeit:**


Diese Richtlinie ist verbindlich.

- Bei Zuwiderhandlung gegen diese Richtlinie oder unsachgemäßer Nutzung der IT-Infrastruktur kann der Zugang zur IT-Infrastruktur oder zu Teilen davon zur Wahrung der notwendigen Sicherheit deaktiviert werden.
- Bei gravierenden Verstößen gegen diese Richtlinie muss der Mitarbeiter mit Konsequenzen bis hin zur Kündigung des Arbeitsverhältnisses sowie Schadenersatzansprüchen rechnen.
- Sollte eine Bestimmung dieser Richtlinie für einen einzelnen Mitarbeiter sachlich nicht zutreffen, so ist dennoch eine Lösung im Sinne dieser Richtlinie herbeizuführen.
- Ausnahmen von den obigen Regeln sind zulässig. Sie müssen im Vorfeld von <der zuständigen Stelle> genehmigt oder in entsprechenden Richtlinien geregelt sein.

## Dokumentenmanagement:

- Dieses Dokument ist ab dem Genehmigungsdatum gültig.
- Der Eigentümer des Dokuments ist der Informationssicherheitsbeauftragte.
- Dieses Dokument wird jährlich geprüft und bei Bedarf aktualisiert.

## Änderungshistorie:

Version	Published	Changed By	Comment
<b>CURRENT (v. 8)</b>	<b>Jun 02, 2025 11:59</b>	 Robin Leitner	

[Go to Page History](#)