VANTARION

Richtlinien, die wirken

Die zentralen Richtlinien für ein schlankes, ISO-27001-konformes ISMS

Ein Praxisleitfaden für
ISB, QM & IT-Leitung

MANAGEMENT SUMMARY

Viele ISMS-Projekte starten mit dem Ziel, „ISO-konform dokumentiert" zu sein. Was daraus häufig entsteht, ist ein umfangreicher Richtlinienbestand – jedoch kein gesteuertes Managementsystem.

ISO 27001 verlangt jedoch nicht primär Dokumente, sondern ein strukturiertes, nachvollziehbares und wirksames System zur Steuerung von Informationssicherheitsrisiken. Richtlinien sind dabei das verbindende Element zwischen Strategie, operativer Umsetzung und Auditnachweis.

Ein wirksames Policy-Set erfüllt drei Funktionen:

- ☑ **Es übersetzt Normanforderungen in verständliche Grundsätze.**
- ☑ **Es definiert Verantwortlichkeiten und Entscheidungslogiken.**
- ☑ **Es schafft überprüfbare Rahmenbedingungen für Prozesse.**

Dieses Whitepaper zeigt, wie eine vollständige, ISO-27001-konforme Policy-Struktur aufgebaut wird – mit inhaltlicher Tiefe, aber ohne unnötige Dokumentenkomplexität.

Tobias Frank,
Gründer und CEO

Als **Head of IT und Verantwortlicher für Informationssicherheit** in Handelsunternehmen und Fertigungsindustrie und habe ich in allen Facetten erlebt, wie aufwändig Informationssicherheit für CxO und Teams im Alltag ist. 20 Jahre lang.

Aus diesem persönlichen Antrieb heraus entwickelten wir VantarIS und gründeten Vantarion.

VantarIS nimmt die Bürokratie aus Normen wie NIS2 und bringt kompetente Sicherheit.

VANTARIS

Vantarion GmbH | Mergenthalerallee 73-75 | 65760 Eschborn | www.vantarion.de | info@vantarion.de

DIE ZENTRALEN RICHTLINIEN EINES ISO-KONFORMEN ISMS

Nachfolgend wird eine konsistente Richtlinienstruktur dargestellt, die sämtliche relevanten ISO-Anforderungen abdeckt.

1. Informationssicherheitsleitlinie

Die Informationssicherheitsleitlinie ist das strategische Fundament des gesamten Systems. Sie definiert, welchen Stellenwert Informationssicherheit im Unternehmen einnimmt und welche Zielrichtung verfolgt wird.

Hier werden Sicherheitsziele formuliert, die Verpflichtung der Geschäftsleitung dokumentiert und der Geltungsbereich des ISMS beschrieben. Eine wirksame Leitlinie stellt klar, dass Informationssicherheit integraler Bestandteil der Unternehmensstrategie ist und nicht isoliert in der IT-Abteilung angesiedelt wird.

Im Audit wird geprüft, ob die Leitlinie zur Organisation passt, ob sie regelmäßig überprüft wird und ob sie tatsächlich als Referenzdokument für weitere Richtlinien dient.

2. Governance- & Rollenrichtlinie

Diese Richtlinie schafft organisatorische Klarheit. Sie beschreibt die Rollen im ISMS, deren Aufgaben sowie Berichtslinien und Eskalationswege.

Neben dem Informationssicherheitsbeauftragten werden auch Fachbereichsverantwortliche, IT-Leitung, Datenschutzbeauftragter und Geschäftsführung eingebunden. Wichtig ist hier die Definition von Verantwortungsbereichen, nicht nur von Funktionsbezeichnungen. Beispiele für Verantwortungsbereiche können sein:

- ☑ **Wer darf Vorfälle bei Behörden melden?**
- ☑ **Wer darf Vorfälle dem Kunden mitteilen?**
- ☑ **Wer verantwortet die Risikoanalyse?**

Gerade bei sicherheitsrelevanten Entscheidungen oder im Vorfallmanagement ist eindeutig zu klären, wer entscheidet, wer informiert wird und wer die Umsetzung überwacht.

Eine klare Governance-Struktur reduziert Unsicherheiten und erhöht die Reaktionsfähigkeit.

3. Risikomanagement-Richtlinie

Die Risikomanagement-Richtlinie bildet das methodische Herzstück des ISMS. Sie legt fest, wie Risiken systematisch identifiziert, analysiert und behandelt werden.

Im Zentrum steht die strukturierte Betrachtung von Geschäftsprozessen, den unterstützenden Assets und möglichen Bedrohungsszenarien. Risiken werden bewertet, priorisiert und mit geeigneten Maßnahmen hinterlegt.

Vantarion GmbH | Mergenthalerallee 73-75 | 65760 Eschborn | www.vantarion.de | info@vantarion.de

Diese Richtlinie stellt sicher, dass Sicherheitsmaßnahmen nicht willkürlich oder pauschal eingeführt werden, sondern nachvollziehbar auf Risiken basieren.

Sie schafft Transparenz über Entscheidungsgrundlagen und ist ein zentrales Element jeder ISO-Prüfung.

4. Informationsklassifizierungs- & Datenschutzrichtlinie

Eine wirksame Sicherheitsarchitektur setzt voraus, dass Informationen nach Schutzbedarf unterschieden werden. Diese Richtlinie definiert Klassifizierungsstufen und beschreibt, wie Informationen entsprechend behandelt werden.

Darüber hinaus integriert sie datenschutzrechtliche Anforderungen. Personenbezogene Daten werden gesondert betrachtet, Schutzmaßnahmen definiert und organisatorische sowie technische Mindestanforderungen festgelegt.

Die klare Klassifizierung bildet die Grundlage für angemessene Zugriffskontrollen, Aufbewahrungsfristen und Schutzmaßnahmen.

5. Zugriffskontroll- & Identitätsrichtlinie

Zugriffskontrolle ist eines der zentralen Elemente der ISO 27001. Diese Richtlinie beschreibt, nach welchen Prinzipien Berechtigungen vergeben, überprüft und entzogen werden.

Sie regelt Genehmigungsprozesse, die Rollenbasierung von Zugriffen und regelmäßige Überprüfungen von Benutzerrechten. Auch Multi-Faktor-Authentifizierung und administrative Sonderrechte werden hier verankert.

Eine dokumentierte Zugriffspolitik verhindert unkontrollierte Rechtevergaben und erhöht die Transparenz über kritische Berechtigungen.

6. Incident-Management-Richtlinie

Kein Unternehmen ist vor Sicherheitsvorfällen gefeit. Die Incident-Richtlinie beschreibt daher klar definierte Meldewege, Eskalationsmechanismen und Dokumentationspflichten.

Sie legt fest, wie Vorfälle bewertet, klassifiziert und bearbeitet werden. Ebenso wird geregelt, wann externe Stellen informiert werden müssen, bspw. bei meldepflichtigen Datenschutzverletzungen oder NIS2-relevanten Ereignissen.

Ein dokumentierter und geübter Incident-Prozess zeigt im Audit organisatorische Reife und Handlungsfähigkeit.

Vantarion GmbH | Mergenthalerallee 73-75 | 65760 Eschborn | www.vantarion.de | info@vantarion.de

7. Business Continuity & Backup-Richtlinie

Diese Richtlinie beschreibt die organisatorischen und technischen Grundlagen zur Sicherstellung der Geschäftskontinuität.

Sie regelt Sicherungsintervalle, Aufbewahrungszeiträume, Wiederherstellungstests und Verantwortlichkeiten. Darüber hinaus wird definiert, welche Geschäftsprozesse kritisch sind und welche Wiederanlaufzeiten akzeptabel sind.

Business Continuity ist damit keine rein technische Disziplin, sondern Teil der strategischen Unternehmenssteuerung.

8. Personalsicherheits- & Awareness-Richtlinie

ISO 27001 betont die Bedeutung des Faktors Mensch. Diese Richtlinie beschreibt Anforderungen an Mitarbeitende über den gesamten Lebenszyklus hinweg, von der Einstellung über Schulungen bis zum Austritt.

Regelmäßige Awareness-Maßnahmen sensibilisieren für Risiken wie Phishing, Social Engineering oder Datenmissbrauch. Vertraulichkeitsvereinbarungen und klare Verhaltensregeln schaffen verbindliche Rahmenbedingungen.

Ein lebendiges Schulungskonzept ist ein starkes Signal für eine aktive Sicherheitskultur.

9. Physische Sicherheitsrichtlinie

Physische Sicherheit ist ein oft unterschätzter Bestandteil der Informationssicherheit. Diese Richtlinie beschreibt Maßnahmen zur Zutrittskontrolle, zum Schutz sensibler Bereiche und zur Absicherung kritischer Infrastruktur.

Besucherregelungen, Clean-Desk-Vorgaben und Schutz vor Umwelteinflüssen werden hier geregelt. Gerade in Branchen mit erhöhtem Schutzbedarf oder bei TISAX-Prüfungen ist dieser Bereich besonders relevant.

10. Supplier-Security-Richtlinie

Externe Dienstleister und Lieferanten sind integraler Bestandteil moderner Geschäftsprozesse. Diese Richtlinie beschreibt, wie externe Parteien bewertet, klassifiziert und überwacht werden.

Sicherheitsanforderungen werden vertraglich verankert, regelmäßige Überprüfungen definiert und Vorfallmeldepflichten geregelt.

So wird sichergestellt, dass Sicherheitsstandards nicht an Unternehmensgrenzen enden.

Vantarion GmbH | Mergenthalerallee 73-75 | 65760 Eschborn | www.vantarion.de | info@vantarion.de

11. Change- & Schwachstellenmanagement

Technologische Umgebungen verändern sich permanent. Diese Richtlinie beschreibt, wie Änderungen kontrolliert eingeführt und Schwachstellen systematisch behandelt werden.

Patch-Prozesse, Freigabeprozesse und Dokumentationsanforderungen werden definiert. Ein strukturierter Change-Prozess reduziert das Risiko unbeabsichtigter Sicherheitslücken.

12. Acceptable Use & IT-Nutzungsrichtlinie

Diese Richtlinie definiert klare Regeln für den Umgang mit IT-Systemen, mobilen Geräten und Remote-Arbeit.

Sie schafft Transparenz über zulässige und unzulässige Nutzung und trägt zur Sensibilisierung aller Mitarbeitenden bei.

Eine verständlich formulierte Acceptable-Use-Policy ist häufig das sichtbarste Element des ISMS im Alltag.

FAZIT

Ein vollständiges ISMS deckt organisatorische, personelle, physische und technische Anforderungen ab. Eine strukturierte Policy-Architektur übersetzt diese Anforderungen in klare, verständliche und steuerbare Grundsätze.

Richtlinien sind dann wirksam, wenn sie:

- ☑ **vollständig sind**
- ☑ **klar zugeordnet sind**
- ☑ **regelmäßig überprüft werden**
- ☑ **im Alltag gelebt werden**

Ein schlankes ISMS bedeutet nicht weniger Sicherheit, sondern mehr Klarheit.