					Fügen Sie hier den Namen der eingetragenen juristischen Person ein							
Dokumentnummer: P02					Dokumenttitel: **Richtlinie zu Governance-Rollen und Verantwortlichkeiten**							
Version: 1.0		Datum des Inkrafttretens: 01.01.2025			Dokumentenverantwortlicher:							
X	Richtlinie		Standard		Verfahren		Formular		Register		Sonstiges	

Änderungshistorie				
Änderungsnummer	**Änderungsdatum**	**Änderungen**	**Geprüft von**	**Prozessverantwortlicher**

Genehmigungen			
Name	**Position**	**Datum**	**Unterschrift**

An Normen und Vorschriften ausgerichtet

Standard/Vorschrift	Klausel/Artikel	Kommentar
ISO/IEC 27001:2022	Klausel 5.3; Anhang A Maßnahme 5	
ISO/IEC 27002:2022	Maßnahme 5	
NIST SP 800-53 Rev. 5	PL-1 bis PL-4, PM-1 bis PM-13	
EU-DSGVO	Artikel 5(1)(f), 24, 37	
EU-NIS2	Artikel 21(2)(a)	
EU-DORA	Artikel 5	
COBIT 2019	EDM01, EDM02, APO01, APO12, MEA	

1. Zweck

1.1 Diese Richtlinie definiert das Governance-Modell, die organisatorischen Rollen und die Verantwortlichkeiten, die für den Betrieb eines wirksamen Informationssicherheitsmanagementsystems (ISMS) erforderlich sind.

1.2 Sie legt klare Rechenschaftsstrukturen, Entscheidungsbefugnisse und Eskalationswege fest, um sicherzustellen, dass Informationssicherheit auf allen Ebenen der Organisation verankert ist und mit den strategischen Geschäftszielen im Einklang steht.

1.3 Diese Richtlinie setzt die Anforderungen aus ISO/IEC 27001:2022, Klausel 5.3 und Maßnahme A.5.2, um und stellt sicher, dass Verantwortlichkeiten für sicherheitsbezogene Tätigkeiten eindeutig zugewiesen, dokumentiert, kommuniziert und regelmäßig überprüft werden.

1.4 Diese Richtlinie schafft zudem die Grundlage für eine integrierte Governance mit anderen Disziplinen wie Risikomanagement, Compliance, IT-Betrieb und Rechtsabteilung.

2. Geltungsbereich

2.1 Diese Richtlinie gilt für alle Personen und Funktionen, die an Governance, Betrieb und Aufsicht der Informationssicherheit innerhalb des ISMS-Geltungsbereichs beteiligt sind. Dies umfasst:

2.1.1 Geschäftsleitung, obere Führungsebene und Mitglieder des Leitungsorgans

2.1.2 ISMS-Manager, CISO und Kontrollverantwortliche

2.1.3 Prozessverantwortliche und Asset-Verantwortliche

2.1.4 Auftragnehmer und Drittanbieter mit übertragenen Sicherheitsverantwortlichkeiten

2.2 Sie gilt sowohl für interne als auch für extern bezogene Funktionen (z. B. ausgelagertes SOC, Administratoren von Cloud-Plattformen), bei denen Governance-Rollen formell zugewiesen oder vertraglich festgelegt sind.

2.3 Die Richtlinie gilt außerdem für Organisationseinheiten, Abteilungen und Projektteams, die sicherheitsrelevante Assets, Systeme oder Services verwalten oder beeinflussen.

3. Ziele

3.1 Sicherzustellen, dass Rollen und Verantwortlichkeiten der Informationssicherheit formell definiert, zugewiesen, kommuniziert und dokumentiert sind.

3.2 Ein Governance-Modell aufrechtzuerhalten, das Funktionstrennung durchsetzt, Interessenkonflikte vermeidet und die Eskalation ungelöster Sicherheitsprobleme ermöglicht.

3.3 Sicherzustellen, dass Rechenschaftspflicht und Befugnisse für Sicherheitsentscheidungen entsprechend Geschäftsauswirkung und Organisationsstruktur verteilt sind.

3.4 Einen Rahmen für die Steuerung von Verantwortungsübertragungen, Rollenänderungen und der Überprüfung zugewiesener Verantwortlichkeiten zu schaffen.

3.5 Interessenträgern – einschließlich Aufsichtsbehörden, Auditoren und Kunden – die Sicherheit zu geben, dass die Informationssicherheit wirksam und in Übereinstimmung mit anwendbaren Normen gesteuert wird.

4. Rollen und Verantwortlichkeiten

4.1 Geschäftsleitung (oberste Leitung)

4.1.1 Stellt die strategische Aufsicht sicher, weist Ressourcen zu und gewährleistet die Ausrichtung zwischen ISMS-Zielen und Geschäftszielen.

4.1.2 Genehmigt wesentliche ISMS-Dokumentation, einschließlich der Informationssicherheitsrichtlinie, Risikobehandlungspläne und Entscheidungen zu Audit-Folgemaßnahmen.

4.1.3 Nimmt an ISMS-Managementbewertungen teil und eskaliert Entscheidungen, die einer Genehmigung durch das Leitungsorgan bedürfen.

4.1.4 Fördert eine Sicherheitskultur und unterstützt die organisationsweite Einhaltung der Grundsätze der Sicherheitsgovernance.

4.2 Informationssicherheitslenkungsausschuss (ISSC)

4.2.1 Fungiert als funktionsübergreifendes Governance-Gremium für die Aufsicht über das ISMS.

4.2.2 Überprüft Risikoprofil, Kontrollwirksamkeit, Auditfeststellungen und strategische Sicherheitsinitiativen.

4.2.3 Stellt die Koordination zwischen Abteilungen sicher (z. B. IT, Recht, HR, Risiko, Compliance, Betrieb).

4.2.4 Genehmigt Eskalationsschwellen, Budgetzuweisungen und Richtlinienänderungen, die eine Beteiligung der Geschäftsleitung erfordern.

[... Abschnitte 4.3–8 sind in dieser Vorschau nicht enthalten. Erwerben Sie das vollständige Dokument, um auf den gesamten Inhalt zuzugreifen. ...]

9. Anforderungen an Überprüfung und Aktualisierung

9.1 Überprüfungsplan

9.1.1 Diese Richtlinie ist mindestens jährlich oder bei Eintritt eines der folgenden Ereignisse zu überprüfen:

9.1.1.1 Änderungen der Organisationsstruktur oder des Führungsteams

9.1.1.2 Erweiterung oder Neudefinition des ISMS-Geltungsbereichs

9.1.1.3 regulatorische Änderungen mit Auswirkungen auf Rollenzuweisung oder Aufsicht

9.1.1.4 wesentliche Auditfeststellungen oder Vorfälle im Zusammenhang mit Governance-Versagen

9.2 Überprüfungs- und Genehmigungsprozess

9.2.1 Der ISMS-Manager leitet und führt den Überprüfungsprozess durch, einschließlich der Einholung von Beiträgen der Interessenträger und Rückmeldungen aus Audits.

9.2.2 Vorgeschlagene Aktualisierungen sind durch den ISSC zu überprüfen und formell durch die Geschäftsleitung zu genehmigen.

9.2.3 Jede Version muss im ISMS-Dokumentenregister nachverfolgt werden und folgende Metadaten enthalten:

9.2.3.1 Richtlinienkennung und Titel

9.2.3.2 Versionsnummer und Zusammenfassung der Änderungen

9.2.3.3 Datum des Inkrafttretens und nächstes Überprüfungsdatum

9.2.3.4 Richtlinienverantwortlicher und Genehmigender

9.2.3.5 Dokumentenklassifizierungsstufe

9.2.3.6 Aufbewahrungs- und Archivierungshistorie

10. Zugehörige Richtlinien und Verknüpfungen

10.1 Diese Richtlinie ist in Verbindung mit den folgenden Richtlinien auszulegen:

10.1.1 P1 – Informationssicherheitsrichtlinie: Legt das übergreifende Sicherheitsprogramm fest und beschreibt die Verantwortlichkeiten der Leitung für Richtlinienfreigabe und strategische Aufsicht.

10.1.2 P5 – Änderungsmanagement-Richtlinie: Stellt sicher, dass Änderungen an Governance-Strukturen, Rollen oder Verantwortlichkeiten einer dokumentierten Genehmigung und Risikoprüfung unterliegen.

10.1.3 P6 – Risikomanagement-Richtlinie: Identifiziert und behandelt Governance-Risiken, die aus Rollenkonflikten, nicht zugewiesenen Aufgaben oder fehlender Eskalation entstehen.

10.1.4 P7 – Richtlinie für Onboarding und Austritt: Regelt Prozesse zur Zuweisung und zum Entzug von Kontrollen bei Änderungen im Beschäftigungslebenszyklus.

10.1.5 P33 – Richtlinie zur Audit- und Compliance-Überwachung: Unterstützt die unabhängige Überprüfung der Governance-Wirksamkeit und stellt die Umsetzung von Korrekturmaßnahmen bei Nichteinhaltung sicher.

10.2 Diese Richtlinien unterstützen gemeinsam ein einheitliches und durchsetzbares ISMS-Governance-Rahmenwerk.

11. Referenznormen und Rahmenwerke

11.1 Diese Richtlinie ist an weltweit anerkannten Normen und Rahmenwerken für Informationssicherheitsgovernance und Rechenschaftspflicht von Rollen ausgerichtet. Sie stellt die Rückverfolgbarkeit zu regulatorischen und Zertifizierungsanforderungen sicher und unterstützt eine belastbare ISMS-Struktur.

11.2 ISO/IEC 27001

11.2.1 Klausel 5.3 – Organisatorische Rollen, Verantwortlichkeiten und Befugnisse: Diese Richtlinie erfüllt die Anforderung, dass informationssicherheitsrelevante Rollen eindeutig zugewiesen, kommuniziert und dokumentiert werden.

11.2.2 Klausel 9.3 – Managementbewertung: Diese Richtlinie stellt die Aufsicht der Geschäftsleitung über ISMS-Rollen und Governance durch quartalsweise und jährliche Überprüfungen sicher.

11.2.3 Anhang A Maßnahme 5.2 – Rollen und Verantwortlichkeiten der Informationssicherheit: Definiert Rollen auf technischer, operativer und strategischer Ebene, um Funktionstrennung, Risikoverantwortung und nachvollziehbare Rechenschaftspflicht sicherzustellen.

11.3 ISO/IEC 27002:2022 – Maßnahme 5

11.3.1 Bietet Umsetzungsleitlinien für die Zuweisung von Verantwortlichkeiten der Informationssicherheit innerhalb einer Organisation. Diese Richtlinie übernimmt diese Leitlinien durch die Definition von Rollentypen, Regeln zur Verantwortungsübertragung, Eskalationsverfahren und Überprüfungsmechanismen.

11.4 NIST SP 800-53 Rev. 5

11.4.1 PL-1 bis PL-4: Betonen die Notwendigkeit formeller Planungsdokumentation, einschließlich Richtlinien, die Governance definieren und Sicherheitsverantwortlichkeiten zuweisen.

11.4.2 PM-1 (Plan für das Informationssicherheitsprogramm) und PM-2 (Leitender Informationssicherheitsbeauftragter): In dieser Richtlinie durch die Zuweisung des CISO/ISMS-Managers und formelle Governance-Rollen umgesetzt.

11.4.3 PM-5 bis PM-13: Diese Richtlinie erfüllt Anforderungen an Rollendokumentation, organisationsweite Risikorollen, Aufsicht über das Konfigurationsmanagement und Integration mit Missions- bzw. Geschäftsfunktionen.

11.5 EU-DSGVO (2016/679)

11.5.1 Artikel 5(1)(f): Verlangt, dass personenbezogene Daten gegen unbefugte oder unrechtmäßige Verarbeitung geschützt werden. Diese Richtlinie stellt sicher, dass für den Datenschutz verantwortliche Personen eindeutig benannt und überwacht werden.

11.5.2 Artikel 24: Verlangt angemessene organisatorische Maßnahmen, einschließlich Governance-Strukturen.

11.5.3 Artikel 37: Verlangt die Benennung eines Datenschutzbeauftragten (DSB), was im Governance-Rahmenwerk und im Verantwortlichkeitsverzeichnis der Organisation abzubilden ist.

11.6 EU-NIS2-Richtlinie (2022/2555)

11.6.1 Artikel 21(2)(a): Verlangt, dass Einrichtungen Richtlinien zur Risikoanalyse und Sicherheit von Informationssystemen umsetzen, einschließlich rollenspezifischer Verantwortlichkeiten. Diese Richtlinie definiert solche Rollen und ihre Governance-Mechanismen.

11.7 EU-DORA (2022/2554)

11.7.1 Artikel 5 – Governance- und internes Kontrollrahmenwerk: Verlangt die formelle Zuweisung von Verantwortlichkeiten für das IKT-Risikomanagement, Entscheidungsrollen und Berichtskanäle. Diese Richtlinie bildet die Grundlage für die Governance sicherheitsbezogener Rollen in IKT-Umgebungen.

11.8 COBIT 2019

11.8.1 EDM01 – Sichergestellte Einrichtung des Governance-Rahmenwerks: Diese Richtlinie stellt sicher, dass das ISMS über eine klar definierte Governance-Struktur verfügt, die an den Anforderungen des Unternehmens ausgerichtet ist.

11.8.2 EDM02 – Sichergestellte Leistungsrealisierung: Richtet rollenbasierte Sicherheitsaktivitäten an strategischen und operativen Zielen aus und stellt Rechenschaftspflicht sowie messbare Ergebnisse sicher.

11.8.3 APO01 – Gesteuertes Management-Rahmenwerk für I&T und APO12 – Gesteuertes Risiko: Diese Richtlinie unterstützt die strukturierte Steuerung von Rollen der Informationssicherheit innerhalb eines breiteren IT-Governance- und Risikorahmens.

11.8.4 MEA01 – Überwachen, Evaluieren und Beurteilen der Leistung: Verankert Überprüfungsmechanismen, mit denen verifiziert wird, dass Governance-Rollen wirksam, aktuell und durchgesetzt sind.