| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Fügen Sie hier den Namen der eingetragenen juristischen Person ein | | | | | | | |
| Dokumentnummer:<br>P02S | | | | | Dokumenttitel:<br>**Richtlinie zu Governance-Rollen und Verantwortlichkeiten** | | | | | | | |
| Version:<br>1.0 | | Datum des Inkrafttretens:<br>01.01.2025 | | | Dokumentenverantwortlicher: | | | | | | | |
| X | Richtlinie | | Standard | | Verfahren | | Formular | | Register | | Sonstiges | |

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

| **Genehmigungen** | | | |
|---|---|---|---|
| **Name** | **Position** | **Datum** | **Unterschrift** |
| | | | |
| | | | |

Anwendbare Normen und regulatorische Anforderungen

| Standard/Regulation | Clause/Article | Comment |
|---|---|---|
| ISO/IEC 27001:2022 | Abschnitt 5 | |
| ISO/IEC 27002:2022 | Maßnahmen 5.2, 5.3, 5 | |
| NIST SP 800-53 Rev.5 | PM-1, PL-1, PL-4, CA-1, AC-1 | |
| EU-DSGVO | Artikel 5(2), 32 | |

**1. Zweck**

1.1 Diese Richtlinie legt fest, wie Governance-Verantwortlichkeiten für die Informationssicherheit in der Organisation zugewiesen, delegiert und gesteuert werden, um die vollständige Einhaltung der ISO/IEC 27001:2022 sowie weiterer regulatorischer Verpflichtungen sicherzustellen.

1.2 Sie stellt Rechenschaftspflicht auf allen Ebenen sicher und unterstützt die operative Wirksamkeit, indem eindeutig festgelegt wird, wer für jede sicherheitsbezogene Funktion verantwortlich ist.

1.3 Diese Richtlinie verbessert die Auditfähigkeit und stärkt das Vertrauen von Kunden, indem sie eine formalisierte Sicherheitsgovernance nachweist, auch in Organisationen mit begrenzten technischen Ressourcen oder ausgelagerter IT.

**2. Geltungsbereich**

**2.1 Diese Richtlinie gilt für alle Personen, die Systeme oder Daten der Organisation nutzen oder verarbeiten, einschließlich:**

2.1.1 Geschäftsführung, General Manager (GM)

2.1.2 Mitarbeitende und Auftragnehmer

2.1.3 externe IT-Dienstleister oder Berater

**2.2 Sie umfasst alle Systeme, Umgebungen und Dienste, die zur Verarbeitung, Übertragung oder Speicherung von Geschäfts- oder Kundeninformationen genutzt werden, einschließlich:**

2.2.1 Büro-IT-Infrastruktur und Endgeräte für mobiles Arbeiten

2.2.2 Cloud-basierte Plattformen und E-Mail-Dienste

2.2.3 physische Unterlagen und gemeinsame Laufwerke

2.3 Der Geltungsbereich umfasst sowohl interne als auch ausgelagerte Tätigkeiten im Zusammenhang mit der Informationssicherheitsgovernance.

**3. Ziele**

3.1 Für alle sicherheitsbezogenen Aufgaben sind klare Rechenschaftspflichten festzulegen, einschließlich Richtlinienmanagement, Zugriffskontrolle, Behandlung von Sicherheitsvorfällen und Überwachung.

3.2 Eine wirksame Funktionstrennung ist sicherzustellen, um Interessenkonflikte oder Betrugsrisiken zu verringern.

3.3 Sicherheitsaufgaben und -rollen sind eindeutig zu dokumentieren und regelmäßig zu überprüfen.

3.4 Informierte Entscheidungsfindung, Eskalation und Aufsicht in Bezug auf IT- und Sicherheitsrisiken sind sicherzustellen.

3.5 Die Zertifizierung nach ISO/IEC 27001:2022 ist zu unterstützen und das Vertrauen von Kunden, Partnern und Auditoren zu stärken.

**4. Rollen und Verantwortlichkeiten**

**4.1 General Manager (GM) / Geschäftsführung**

4.1.1 Trägt die Gesamtverantwortung für die Umsetzung und Überwachung dieser Richtlinie.

4.1.2 Genehmigt alle Sicherheitsrollen, Verantwortlichkeiten und Delegationsentscheidungen.

4.1.3 Überwacht die Einhaltung und trifft die abschließenden Entscheidungen zu Richtlinienausnahmen und Eskalationen.

**4.2 Benannter Datenschutz- oder Sicherheitskoordinator**

4.2.1 Diese Rolle kann von einem Mitarbeitenden oder einem vertrauenswürdigen Berater wahrgenommen werden.

4.2.2 In Kleinstunternehmen kann diese Rolle durch den General Manager (GM) oder einen externen Dienstleister übernommen werden.

4.2.3 Unterstützt die tägliche Umsetzung von Zugriffskontrolle, Incident Response oder grundlegenden technischen Sicherheitsaufgaben.

4.2.4 Berichtet dem General Manager (GM) unmittelbar über alle Sicherheitsprobleme oder -risiken.

[ ... 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 Jährliche Überprüfung**

9.1.1 Diese Richtlinie muss alle 12 Monate durch den General Manager (GM) überprüft werden, um sicherzustellen, dass sie weiterhin den rechtlichen Verpflichtungen, operativen Anforderungen und Zertifizierungsanforderungen nach ISO/IEC 27001 entspricht.

**9.2 Anlassbezogene Überprüfungen**

**9.2.1 Überprüfungen müssen ebenfalls erfolgen, wenn:**

9.2.1.1 wesentliche organisatorische Änderungen eintreten

9.2.1.2 ein neuer Dienstleister eingebunden wird

9.2.1.3 ein schwerwiegender Sicherheitsvorfall eintritt

9.2.1.4 Vorschriften wie DSGVO, NIS2 oder DORA aktualisiert werden

**9.3 Versionskontrolle und Dokumentation**

**9.3.1 Alle Überprüfungen müssen Folgendes umfassen:**

9.3.1.1 Datum der Überprüfung

9.3.1.2 Zusammenfassung etwaiger Änderungen

9.3.1.3 Unterschrift oder dokumentierte Genehmigung durch den General Manager (GM)

9.3.1.4 archivierte Vorversionen als Referenz für Audits

**9.4 Kommunikation von Änderungen**

9.4.1 Alle Aktualisierungen dieser Richtlinie müssen dem Personal und den Dienstleistern unverzüglich per E-Mail, über interne Portale oder durch formelle Mitteilungen bekannt gegeben werden.

**10. Verwandte Richtlinien und Verknüpfungen**

**10.1 Diese Richtlinie sollte zusammen mit den folgenden SME-Richtlinien umgesetzt werden, um ihre volle Wirksamkeit zu erreichen:**

10.1.1 P4S – Zugriffskontrollrichtlinie: Legt fest, wie Zugriffe gewährt, verwaltet und entzogen werden, unmittelbar verknüpft mit zugewiesenen Rollen und Aufsicht.

10.1.2 P8S – Richtlinie zur Sensibilisierung und Schulung in der Informationssicherheit: Bekräftigt rollenspezifische Verantwortlichkeiten und Erwartungen.

10.1.3 P17S – Richtlinie zu Datenschutz und Privatsphäre: Beschreibt rechtliche Pflichten nach der DSGVO, die den in dieser Governance-Richtlinie definierten Rollen zugewiesen sind.

10.1.4 P30S – Incident-Response-Richtlinie: Erfordert festgelegte Verantwortlichkeiten für Meldung, Eskalation und Bearbeitung von Vorfällen.

10.2 Zusammen ermöglichen diese Richtlinien eine konsistente Durchsetzung, interne Rechenschaftspflicht und externe Compliance.

## 11. Referenznormen und Rahmenwerke

### 11.1 ISO/IEC 27001

11.1.1 Abschnitt 5.3 – Organisatorische Rollen, Verantwortlichkeiten und Befugnisse: Verlangt, dass Rollen klar zugewiesen und durch die oberste Leitung unterstützt werden.

### 11.2 ISO/IEC 27002

11.2.1 Maßnahmen 5.2–5.4: Fordern eine klare Dokumentation von Rollen der Informationssicherheit, Funktionstrennung und Managementaufsicht.

### 11.3 NIST SP 800-53 Rev.5

11.3.1 PM-1: Etabliert ein übergreifendes Informationssicherheitsprogramm mit festgelegten Verantwortlichkeiten.

11.3.2 PL-1 bis PL-4: Fordern Planungskontrollen, einschließlich Richtlinienerstellung und dokumentierter Rollenzuweisungen.

11.3.3 CA-1: Verlangt festgelegte Rollen für Bewertung und Autorisierung.

11.3.4 AC-1: Verknüpft rollenbasierte Zugriffskontrolle mit zugewiesenen Governance-Verantwortlichkeiten.

### 11.4 EU-DSGVO

11.4.1 Artikel 5(2) – Rechenschaftspflicht: Verlangt von Organisationen, die Einhaltung anhand von Rollen und Verantwortlichkeiten nachzuweisen.

11.4.2 Artikel 32 – Sicherheit der Verarbeitung: Betont die klare Zuweisung von Aufgaben zum Schutz personenbezogener Daten.

### 11.5 EU NIS

11.5.1 Artikel 21(2)(a): Verlangt Governance-Strukturen, die formalisierte Rollen für das Management von Cyberrisiken und Vorfällen einschließen.

### 11.6 EU DORA

11.6.1 Artikel 9 und 10: Verlangen von Finanzunternehmen, IKT- und sicherheitsbezogene Verantwortlichkeiten klar zuzuweisen und zu überwachen.

### 11.7 COBIT 2019

11.7.1 EDM03 – Sicherstellung der Risikooptimierung: Verlangt klar definierte Rollen und Eskalationswege für das Management von Sicherheitsrisiken.

11.7.2 APO13 – Sicherheitsmanagement: Weist Einzelpersonen und Rollen strategische und operative Sicherheitsaufgaben zu.

11.7.3 DSS05 – DSS05 Sicherheitsdienste verwalten: Verlangt Struktur und Nachvollziehbarkeit bei Verantwortlichkeiten für externe und interne Sicherheitsdienste.