					Fügen Sie hier den Namen der eingetragenen juristischen Person ein							
Dokumentnummer: P01					Dokumenttitel: **Informationssicherheitsrichtlinie**							
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**

1. Zweck

1.1 Diese Richtlinie definiert die übergeordnete Verpflichtung der Organisation zur Informationssicherheit durch die Einführung und Aufrechterhaltung eines formalen Informationssicherheits-Managementsystems (ISMS).

1.2 Sie legt die strategische Ausrichtung und die grundlegenden Anforderungen zum Schutz der Vertraulichkeit, Integrität, Verfügbarkeit und Resilienz aller Informationswerte in physischen, digitalen und Cloud-Umgebungen fest.

1.3 Die Richtlinie erfüllt die Anforderungen der ISO/IEC 27001:2022, insbesondere der Klauseln 5.1 und 5.2, indem sie die Führungsabsicht, die Verpflichtung der obersten Leitung und die Ausrichtung der Sicherheitsaktivitäten an den Organisationszielen festlegt.

1.4 Sie dient als maßgebliche Referenz für alle untergeordneten Richtlinien, Standards und Verfahren innerhalb des ISMS und ist wesentlich für die Etablierung einer risikobasierten, compliance-orientierten und auf kontinuierliche Verbesserung ausgerichteten Sicherheitsorganisation.

2. Geltungsbereich

2.1 Diese Richtlinie gilt für alle Personen, Informationswerte und Prozesse, die innerhalb des ISMS-Geltungsbereichs definiert sind, einschließlich:

2.1.1 aller Geschäftsbereiche, Abteilungen, Tochtergesellschaften und Niederlassungen

2.1.2 Mitarbeiter, Auftragnehmer, Zeitarbeitskräfte, Berater und externe Dienstleister

2.1.3 aller Daten, Informationssysteme, Anwendungen, Infrastrukturen und Kommunikationskanäle

2.1.4 aller physischen, Cloud-basierten, Remote- und hybriden Umgebungen, in denen Unternehmensdaten verarbeitet oder abgerufen werden

2.2 Die Richtlinie ist für alle Stellen verbindlich, die organisatorische Informationen verarbeiten, und gilt für alle Phasen des Informationslebenszyklus – von der Erstellung und Übertragung bis zur Speicherung und Entsorgung.

2.3 Jegliche Ausschlüsse oder Einschränkungen dieses Geltungsbereichs sind in der ISMS-Geltungsbereichserklärung zu dokumentieren und mit formaler Genehmigung der Geschäftsleitung zu begründen.

3. Ziele

3.1 Einführung und Aufrechterhaltung eines ISMS, das mit der ISO/IEC 27001:2022 im Einklang steht und risikobasierte Entscheidungen im gesamten Unternehmen unterstützt.

3.2 Sicherstellung, dass die Sicherheitsprinzipien Vertraulichkeit, Integrität und Verfügbarkeit in alle organisatorischen Aktivitäten, Systeme und Partnerschaften eingebettet sind.

3.3 Sicherstellung der Einhaltung regulatorischer und vertraglicher Anforderungen durch die Festlegung messbarer, richtliniengesteuerter Sicherheitsziele und deren Integration in die Geschäftsabläufe.

3.4 Minimierung der Eintrittswahrscheinlichkeit und der Auswirkungen von Informationssicherheitsvorfällen durch wirksame präventive, detektive und korrektive Kontrollen.

3.5 Förderung der kontinuierlichen Verbesserung des Reifegrads der Informationssicherheit anhand definierter Leistungsindikatoren, Auditergebnisse und Managementbewertungen.

3.6 Förderung einer Kultur der Rechenschaftspflicht, Sensibilisierung und Resilienz, in der Sicherheitsverantwortlichkeiten von sämtlichem Personal verstanden und umgesetzt werden.

4. Rollen und Verantwortlichkeiten

4.1 Geschäftsleitung

4.1.1 genehmigt und unterstützt die Informationssicherheitsrichtlinie und das ISMS-Rahmenwerk.

4.1.2 stellt die Ausrichtung zwischen Sicherheitszielen und Geschäftsstrategie sicher.

4.1.3 geht mit gutem Beispiel voran und fördert eine starke Kultur der Informationssicherheit.

4.1.4 prüft und genehmigt wesentliche Änderungen des ISMS-Geltungsbereichs, der Risikobehandlung und der Governance-Struktur.

4.2 Chief Information Security Officer (CISO) / ISMS-Manager

4.2.1 verantwortet das ISMS und pflegt diese Richtlinie in Übereinstimmung mit der ISO/IEC 27001.

4.2.2 leitet Risikobewertungen, die Umsetzung von Kontrollen und Prozesse der kontinuierlichen Verbesserung.

4.2.3 stellt die funktionsübergreifende Koordination der Sicherheitsmaßnahmen sicher und überwacht untergeordnete Richtlinien.

4.2.4 berichtet der Geschäftsleitung über den Status des ISMS, Vorfälle, Auditergebnisse und Kennzahlen.

4.2.5 stellt sicher, dass Richtlinienprüfungen und -aktualisierungen gemäß Abschnitt 9 dieses Dokuments durchgeführt werden.

[... 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 Häufigkeit der Überprüfung

9.1.1 Diese Richtlinie ist mindestens jährlich oder bei einem der folgenden Auslöser zu überprüfen:

9.1.1.1 wesentliche Änderungen gesetzlicher, regulatorischer oder vertraglicher Verpflichtungen

9.1.1.2 wesentliche Änderungen des organisatorischen Risikoprofils

9.1.1.3 Ergebnisse interner oder externer Audits

9.1.1.4 schwerwiegende Vorfälle oder Kontrollausfälle

9.2 Zuständigkeit und Verfahren für die Überprüfung

9.2.1 Der CISO oder ein benannter ISMS-Manager leitet den Überprüfungsprozess.

9.2.2 Eingaben für die Überprüfung müssen Folgendes umfassen:

9.2.2.1 Ergebnisse interner Audits

9.2.2.2 Trends aus Risikobewertungen

9.2.2.3 Änderungen von Geschäftsprozessen und Technologien

9.2.2.4 Leistung im Verhältnis zu KPIs und Risikoschwellenwerten

9.2.3 Alle Aktualisierungen müssen:

9.2.3.1 versionskontrolliert und dokumentiert sein

9.2.3.2 von der Geschäftsleitung genehmigt werden

9.2.3.3 über offizielle Kommunikationskanäle an alle betroffenen Parteien verteilt werden

9.2.3.4 erforderliche Aktualisierungen untergeordneter Dokumentation und Schulungen auslösen

10. Verknüpfte Richtlinien und Bezüge

10.1 Diese grundlegende Richtlinie ist unmittelbar mit den folgenden organisatorischen Sicherheitsrichtlinien und Rahmenwerken verknüpft:

10.1.1 P2 – Richtlinie zu Governance-Rollen und Verantwortlichkeiten: Definiert die in diesem Dokument referenzierte Governance-Struktur und Befugnishierarchie.

10.1.2 P3 – Richtlinie zur zulässigen Nutzung: Regelt die verhaltensbezogene Compliance sowie den zulässigen Umgang mit Informationswerten.

10.1.3 P4 – Richtlinie zur Zugriffskontrolle: Operationalisiert zugriffsbezogene Kontrollen, die aus dieser übergeordneten Richtlinie abgeleitet sind.

10.1.4 P6 – Risikomanagement-Richtlinie: Liefert den risikobasierten Kontext für die Auswahl von Kontrollen und die Akzeptanz von Restrisiken.

10.1.5 P33 – Richtlinie für Audit und Compliance-Überwachung: Legt fest, wie interne Sicherungsmechanismen die Durchsetzung der Richtlinie validieren.

10.2 Diese Abhängigkeiten stellen eine umfassende Ausrichtung und Rückverfolgbarkeit im gesamten ISMS sicher und unterstützen eine konsistente Governance für Risiko und Compliance.

11. Referenzstandards und Rahmenwerke

11.1 Diese Informationssicherheitsrichtlinie ist formell an den folgenden Standards und Rahmenwerken ausgerichtet, um vollständige Compliance, Auditbereitschaft und regulatorische Belastbarkeit sicherzustellen:

11.2 ISO/IEC 27001

11.2.1 Klausel 5.1 – Führung und Verpflichtung: Diese Richtlinie belegt die Verpflichtung der obersten Leitung zur Informationssicherheit und definiert Verantwortlichkeiten sowie Ressourcenzuweisungen für das ISMS.

11.2.2 Klausel 5.2 – Informationssicherheitsrichtlinie: Dieses Dokument dient als formale Sicherheitsrichtlinie der Organisation und ist an den festgelegten Sicherheitszielen, der Geschäftsstrategie und den Anforderungen der ISO/IEC 27001 ausgerichtet.

11.2.3 Klausel 6.1 – Maßnahmen zum Umgang mit Risiken und Chancen: Der in dieser Richtlinie verankerte risikobasierte Ansatz stellt sicher, dass Sicherheitsressourcen verhältnismäßig zu Bedrohungen eingesetzt werden.

11.2.4 Klausel 9.2 – Internes Audit und Klausel 10 – Verbesserung: Diese Richtlinie ist in den Zyklus der kontinuierlichen Verbesserung der Organisation eingebettet und unterliegt der Validierung durch interne Audits.

11.2.5 ISO/IEC 27002:2022 – Maßnahme 5.1: Enthält Leitlinien für die Erstellung und Aufrechterhaltung von Sicherheitsrichtlinien. Diese Richtlinie entspricht den Empfehlungen der ISO/IEC 27002 hinsichtlich hierarchischer Dokumentation, Überprüfungszyklen und Durchsetzbarkeit.

11.3 NIST SP 800-53 Rev.5

11.3.1 PL-1 (Richtlinie und Verfahren zur Sicherheitsplanung): Diese Richtlinie erfüllt die Anforderung zur Entwicklung, Bekanntgabe und Überprüfung einer formalen, organisationsweiten Informationssicherheitsrichtlinie.

11.3.2 PM-1 bis PM-5: Behandelt Governance auf Programmebene einschließlich Rollen in der Informationssicherheit, Ressourcenzuweisung, Risikostrategie und Integration der Sicherheitsplanung in Unternehmensabläufe.

11.4 DSGVO (2016/679)

11.4.1 Artikel 5(2): Setzt das Prinzip der Rechenschaftspflicht um. Diese Richtlinie definiert verantwortliche Stellen und nachvollziehbare Durchsetzungsmaßnahmen.

11.4.2 Artikel 24: Verlangt die Umsetzung technischer und organisatorischer Maßnahmen, einschließlich risikoorientierter Richtlinien.

11.4.3 Artikel 32: Unterstützt die Umsetzung geeigneter Maßnahmen zur Sicherstellung der Sicherheit personenbezogener Daten über ihren gesamten Lebenszyklus.

11.5 EU NIS2-Richtlinie (2022/2555)

11.5.1 Artikel 21(2)(a): Verpflichtet Einrichtungen zur Umsetzung einer dokumentierten Sicherheitsrichtlinie für Risikomanagement und Governance. Diese Richtlinie erfüllt diese Anforderung und unterstützt eine weitergehende Cybersicherheitsbereitschaft sowie den Schutz kritischer Infrastrukturen.

11.6 EU DORA (2022/2554)

11.6.1 Artikel 5(2): Verlangt ein dokumentiertes internes Kontrollrahmenwerk für das IKT-Risikomanagement. Diese Richtlinie unterstützt die Compliance im Finanzsektor durch die Zuweisung von Rollen, Kontrollen und Aufsichtsfunktionen im Einklang mit den Governance-Erwartungen der DORA.

11.7 COBIT 2019

11.7.1 EDM01 – Festlegung des Governance-Rahmenwerks: Diese Richtlinie unterstützt die Unternehmensführung durch die Definition von ISMS-Rollen, Führungsverpflichtungen und strategischen Zielen.

11.7.2 APO01 – Management-Rahmenwerk: Unterstützt die Einführung und den Betrieb eines strukturierten ISMS.

11.7.3 APO12 – Risikomanagement: Bietet die Grundlage für die Governance des Informationssicherheitsrisikomanagements.

11.7.4 MEA01/MEA03 – Überwachen, Evaluieren und Beurteilen: Stärkt die kontinuierliche Leistungsbewertung und die Überwachung interner Kontrollen durch die Durchsetzung der Richtlinieneinhaltung.