					Fügen Sie hier den Namen der eingetragenen juristischen Person ein							
Dokumentnummer: P01S					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**

Ausgerichtet an Standards und regulatorischen Anforderungen

Standard/Vorschrift	Klausel/Artikel	Kommentar
ISO/IEC 27001:2022	Klauseln 5.1, 5.2, 5.3, 6.1, 6.2, 8	Legt die Verpflichtung der Leitung, Richtlinienanforderungen, die Zuweisung von Rollen, die Risikobewertung und die operative Steuerung fest
ISO/IEC 27002:2022	Maßnahmen 5.1–5	Legt die Erstellung dokumentierter Informationssicherheitsrichtlinien, die Zuweisung von Rollen, die Funktionstrennung und die Verantwortlichkeiten der Leitung fest
NIST SP 800-53 Rev.5	PM-1, PL-1, CA-1, AC-1	Anforderungen an Sicherheitsprogrammplan, Planungsrichtlinie, Bewertung/Zulassung und Zugriffskontrolle
EU-DSGVO (2016/679)	Artikel 5(2), Artikel 32	Rechenschaftspflicht und Maßnahmen zur Sicherheit der Verarbeitung, insbesondere in Bezug auf dokumentierte Rollen
NIS2-Richtlinie der EU (2022/2555)	Artikel 21(2)(a)	Verlangt Risikomanagementmaßnahmen sowie Rollen und Verantwortlichkeiten für Cyberrisiken
EU DORA (2022/2554)	Artikel 9, Artikel 10	Verlangt die Zuweisung von Rollen für das IKT-Risikomanagement und die Betriebskontinuität
COBIT 2019	EDM03, APO13, DSS05	Stellt durch klare Rollenzuweisung Risikooptimierung, Sicherheitsmanagement und das Management von Sicherheitsdiensten sicher

1. Zweck

1.1 Diese Richtlinie dokumentiert die Verpflichtung unserer Organisation zum Schutz von Kunden- und Geschäftsinformationen, indem Verantwortlichkeiten und praktikable Sicherheitsmaßnahmen klar festgelegt werden; sie ist für Organisationen ohne dediziertes IT-Team geeignet.

1.2 Sie stellt sicher, dass alle Mitarbeiter, Auftragnehmer und Dienstleister verbindliche Regeln einhalten und dadurch die vollständige Erfüllung der Anforderungen für eine ISO/IEC-27001-Zertifizierung ermöglicht wird.

1.3 Diese Richtlinie stärkt das Vertrauen unserer Kunden, indem sie klar darlegt, wie ihre Informationen durch definierte Verantwortlichkeiten, strukturierte Prozesse und klare Rechenschaftspflicht geschützt werden.

2. Geltungsbereich

2.1 Diese Richtlinie gilt für alle Personen, die auf die Daten und Systeme der Organisation zugreifen oder diese verwalten, einschließlich:

2.1.1 Geschäftsinhaber und Geschäftsführer

2.1.2 Mitarbeiter, Auftragnehmer und Praktikanten

2.1.3 Externe IT-Dienstleister oder Berater

2.2 Sie umfasst alle Arten von Informationen, Systemen und Dienstleistungen, einschließlich:

2.2.1 Geschäftsunterlagen, Kundendaten, Passwörter und E-Mails

2.2.2 IKT-Hardware wie Laptops und Telefone

2.2.3 Cloud-Dienste für Dateispeicherung, Kommunikation oder Finanzprozesse

2.2.4 Physische Dokumente, die an Bürostandorten aufbewahrt werden

2.3 Die Richtlinie gilt für alle Arbeitsumgebungen – im Büro, im Homeoffice und cloudbasiert – und umfasst alle Geräte und Softwarelösungen, die zur Verarbeitung oder Speicherung von Geschäftsinformationen genutzt werden.

3. Ziele

3.1 Klare Verantwortlichkeit zuweisen: Es ist sicherzustellen, dass jederzeit eine Person für die Informationssicherheit rechenschaftspflichtig ist. In der Regel ist dies der Geschäftsführer (GF) oder die von ihm formell benannte Person.

3.2 Kunden- und Geschäftsinformationen schützen: Es sind verlässliche und konsistente Schutzmaßnahmen umzusetzen, um Missbrauch, Verlust oder Diebstahl sensibler Daten, einschließlich Kunden- und Finanzunterlagen, zu verhindern.

3.3 ISO/IEC-27001-Zertifizierung unterstützen: Die Organisation muss in die Lage versetzt werden, die vollständige Einhaltung der Anforderungen der ISO/IEC 27001 nachzuweisen und auditbereit sowie zertifizierungsfähig zu sein, ohne eine komplexe Infrastruktur vorauszusetzen.

3.4 Sicherheit in Geschäftsabläufe integrieren: Informationssicherheit ist in die täglichen Aufgaben und Entscheidungen in der gesamten Organisation zu integrieren.

3.5 Sicherheitsbewusstsein und Sicherheitskultur fördern: Jeder Mitarbeiter ist verpflichtet, Sicherheitspraktiken zu verstehen und einzuhalten, etwa die Verwendung starker Passwörter und die Meldung verdächtiger Aktivitäten.

4. Rollen und Verantwortlichkeiten

4.1 Geschäftsführer oder Geschäftsinhaber

4.1.1 Trägt die volle Rechenschaftspflicht für die Informationssicherheit.

4.1.2 Genehmigt diese Richtlinie und hält sie aktuell.

4.1.3 Stellt sicher, dass alle wesentlichen Sicherheitsaufgaben entweder direkt wahrgenommen oder schriftlich delegiert werden.

4.1.4 Verifiziert, dass delegierte Sicherheitsaufgaben, wie die Verwaltung von Zugriffsrechten oder die Reaktion auf Sicherheitsvorfälle, wirksam ausgeführt werden.

4.1.5 Ist der standardmäßige Ansprechpartner für alle internen und externen Sicherheitsangelegenheiten, einschließlich Audits und Kundenanfragen.

4.1.6 Überwacht im Rahmen der jährlichen Überprüfung den Fortschritt in Bezug auf diese Ziele. Die Ziele sollen, soweit möglich, messbar sein (z. B. Prozentsatz geschulter Mitarbeiter, Anzahl gemeldeter Vorfälle) und auf Grundlage von Sicherheitserkenntnissen und Veränderungen der Risikolage angepasst werden.

4.2 Benannter Mitarbeiter (falls zutreffend)

4.2.1 Kann den Geschäftsführer bei der Wahrnehmung täglicher Aufgaben unterstützen, beispielsweise bei der Anlage von Benutzerkonten, dem Entzug von Zugriffsberechtigungen bei Austritten oder der Koordination mit dem IT-Support-Dienstleister.

4.2.2 Muss offiziell benannt sein und über ausreichende Befugnisse und geeignete Mittel zur Durchführung der Aufgaben verfügen.

4.2.3 Meldet alle Probleme an den Geschäftsführer zurück.

[... 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 durch den Geschäftsführer (GF) mindestens einmal jährlich überprüft werden, um die fortlaufende Einhaltung der Anforderungen der ISO/IEC-27001-Zertifizierung, regulatorischer Änderungen (z. B. DSGVO, NIS2 und DORA) sowie sich ändernder Geschäftsanforderungen sicherzustellen.

9.2 Anlassbezogene Überprüfungen

9.2.1 Zusätzliche Überprüfungen müssen erfolgen, wenn wesentliche Änderungen eintreten, beispielsweise:

9.2.1.1 Größere Sicherheitsvorfälle oder Sicherheitsverletzungen.

9.2.1.2 Einführung neuer Geschäftsprozesse oder Technologien (z. B. neue Software, Plattformen für mobiles Arbeiten oder Cloud-Dienste).

9.2.1.3 Änderungen rechtlicher oder regulatorischer Anforderungen, die den Umgang mit Informationen betreffen.

9.3 Dokumentation von Änderungen

9.3.1 Alle Überprüfungen und Änderungen dieser Richtlinie müssen formell dokumentiert werden; dabei sind Datum, Art der Änderungen und die Genehmigung durch den GF eindeutig anzugeben.

9.3.2 Eine Versionshistorie der Richtlinie ist sicher aufzubewahren, um die Weiterentwicklung der Richtlinie und die Einhaltung bei Audits nachweisen zu können.

9.4 Kommunikation von Aktualisierungen

9.4.1 Änderungen dieser Richtlinie müssen unverzüglich allen Mitarbeitern, Auftragnehmern und relevanten Dritten mitgeteilt werden.

9.4.2 Aktualisierte Versionen der Richtlinie müssen für alle betroffenen Personen leicht zugänglich sein (z. B. elektronisch bereitgestellt oder physisch am Arbeitsplatz ausgehängt).

10. Verwandte Richtlinien und Verknüpfungen

10.1 Diese Richtlinie steht in engem Zusammenhang mit weiteren Richtlinien aus dem KMU-Richtliniensatz der Organisation, insbesondere:

10.1.1 P2S – Richtlinie zu Governance-Rollen und Verantwortlichkeiten: Präzisiert die Zuweisung von Sicherheitsaufgaben und Verantwortlichkeiten.

10.1.2 P4S – Zugriffskontrollrichtlinie: Definiert den sicheren Umgang mit dem Zugriff auf Unternehmensinformationen.

10.1.3 P8S – Richtlinie zur Sensibilisierung und Schulung für Informationssicherheit: Legt wesentliche Anforderungen für Schulung und Sensibilisierung des Personals fest.

10.1.4 P17S – Richtlinie zu Datenschutz und Privatsphäre: Stellt die Einhaltung der DSGVO und anderer Datenschutzgesetze sicher.

10.1.5 P30S – Richtlinie zur Reaktion auf Sicherheitsvorfälle: Beschreibt die im Fall von Sicherheitsvorfällen erforderlichen detaillierten Maßnahmen.

10.2 Diese verknüpften Richtlinien geben klare operative Vorgaben und müssen gemeinsam umgesetzt werden, um die vollständige Einhaltung der Anforderungen für eine ISO/IEC-27001-Zertifizierung zu erreichen.

11. Referenzstandards und Rahmenwerke

11.1 ISO/IEC 27001

11.1.1 Klausel 5.1 – Führung und Verpflichtung: Verlangt die Verpflichtung der obersten Leitung und deren Rechenschaftspflicht für die Wirksamkeit der Informationssicherheit in der Organisation.

11.1.2 Klausel 5.2 – Informationssicherheitsrichtlinie: Fordert klare, dokumentierte Richtlinien, die auf die Organisationsstrategie und Compliance-Anforderungen abgestimmt sind.

11.1.3 Klausel 5.3 – Organisatorische Rollen und Verantwortlichkeiten: Definiert die klare Zuweisung von Verantwortlichkeiten für Informationssicherheit innerhalb der Organisation und ist wesentlich für wirksame Governance und Auditkonformität.

11.1.4 Klausel 6.1 – Maßnahmen zum Umgang mit Risiken und Chancen: Stellt sicher, dass Risiken für die Informationssicherheit systematisch identifiziert, bewertet und behandelt werden.

11.1.5 Klausel 8.1 – Operative Planung und Steuerung: Verlangt, dass die Organisation die zur Erreichung der Ziele der Informationssicherheit erforderlichen Prozesse plant und umsetzt und damit verbundene Risiken wirksam steuert.

11.2 ISO/IEC 27002:2022 Maßnahmen 5.1–5

11.2.1 Anhang A Maßnahme 5.1 – Richtlinien für Informationssicherheit: Legt die Erstellung und Kommunikation dokumentierter Informationssicherheitsrichtlinien fest.

11.2.2 Anhang A Maßnahme 5.2 – Rollen der Informationssicherheit: Präzisiert und weist die Rollen und Verantwortlichkeiten der Informationssicherheit den relevanten Parteien formell zu.

11.2.3 Anhang A Maßnahme 5.3 – Funktionstrennung: Erzwingt eine klare Funktionstrennung, um Interessenkonflikte und Betrugsrisiken beim Umgang mit sensiblen Informationen zu verringern.

11.2.4 Anhang A Maßnahme 5.4 – Verantwortlichkeiten der Leitung: Verlangt, dass die Leitung ihr Engagement für Informationssicherheit durch aktive Aufsicht und Ressourcenzuweisung nachweist.

11.2.5 Bekräftigt die Notwendigkeit klar dokumentierter Informationssicherheitsrichtlinien, Rollen, Verantwortlichkeiten und Governance-Strukturen und stellt dadurch eine konsistente Steuerung und Auditierbarkeit in der gesamten Organisation sicher.

11.3 NIST SP 800-53 Rev.5

11.3.1 PM-1 – Plan für das Informationssicherheitsprogramm: Verlangt dokumentierte Strategien und Richtlinien für die Governance der Informationssicherheit und schafft damit ein Rahmenwerk für konsistente Umsetzung und Steuerung.

11.3.2 PL-1 – Richtlinie für Sicherheitsplanung: Verlangt eine organisationsweite Richtlinie für die Sicherheitsplanung, um den sicheren Betrieb und die strategische Ausrichtung von Informationssicherheitsaktivitäten zu steuern.

11.3.3 CA-1 – Richtlinie für Sicherheitsbewertung und -zulassung: Verlangt klar definierte Rollen für Bewertung und Zulassung, um die fortlaufende Wirksamkeit und Einhaltung der Anforderungen an die Informationssicherheit sicherzustellen.

11.3.4 AC-1 – Zugriffskontrollrichtlinie: Verlangt, dass Organisationen Praktiken und Verantwortlichkeiten der Zugriffsverwaltung klar definieren, dokumentieren und durchsetzen.

11.4 EU-DSGVO (2016/679)

11.4.1 Artikel 5(2) – Rechenschaftspflicht: Verlangt, dass Organisationen die Einhaltung der Datenschutzgrundsätze nachweisen, einschließlich dokumentierter Rollen und Richtlinien für Datenschutzverantwortlichkeiten.

11.4.2 Artikel 32 – Sicherheit der Verarbeitung: Verlangt die Umsetzung geeigneter technischer und organisatorischer Maßnahmen, einschließlich klarer Sicherheitsverantwortlichkeiten, zum Schutz personenbezogener Daten vor Sicherheitsverletzungen und unbefugtem Zugriff.

11.5 NIS2-Richtlinie der EU (2022/2555)

11.5.1 Artikel 21(2)(a) – Risikomanagementmaßnahmen: Verlangt klare Governance-Regelungen einschließlich definierter Rollen und Verantwortlichkeiten für Informationssicherheit, die für die wirksame Steuerung von Cyberrisiken wesentlich sind.

11.6 EU DORA (2022/2554)

11.6.1 Artikel 9 – IKT-Risikomanagement: Verlangt, dass Organisationen Rollen und Verantwortlichkeiten im Zusammenhang mit dem IKT-Risikomanagement klar zuweisen, um Resilienz und die Vorbereitung auf die Betriebskontinuität zu stärken.

11.6.2 Artikel 10 – IKT-Betriebskontinuität: Verlangt klare Rechenschaftspflicht und strukturierte Rollen zur Aufrechterhaltung von IKT-Resilienz und -Kontinuität, damit Organisationen verlässlich auf Störungen reagieren können.

11.7 COBIT 2019

11.7.1 EDM03 – Risikooptimierung sicherstellen: Betont klar definierte Rechenschaftspflicht und Rollen beim Management organisatorischer Risiken und unterstützt dadurch eine starke Governance und wirksame Aufsicht über Informationssicherheitsrisiken.

11.7.2 APO13 – Sicherheitsmanagement: Verlangt, dass Organisationen Verantwortlichkeiten für das Sicherheitsmanagement klar festlegen und kommunizieren, um die Ausrichtung an Geschäftszielen und regulatorischen Anforderungen sicherzustellen.

11.7.3 DSS05 – Sicherheitsdienste verwalten: Fordert strukturierte Rollen und klare Verantwortlichkeiten beim Management von Sicherheitsdiensten, um eine konsistente Umsetzung und die Verifizierung der Einhaltung zu ermöglichen.