					Fügen Sie hier den Namen der eingetragenen juristischen Person ein							
Dokumentnummer: P33S					Dokumenttitel: **– Richtlinie zur Audit- und Compliance-Überwachung**							
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/Regulierung	Klausel/Artikel	Kommentar
ISO/IEC 27001:2022	Klauseln 9.2, 10	Interne Audits, kontinuierliche Verbesserung und Behandlung von Nichtkonformitäten
ISO/IEC 27002:2022	Maßnahmen 5.35, 5.37	Geplante interne Überprüfungen, unabhängige Überprüfungen ausgelagerter Prozesse
NIST SP 800-53 Rev. 5	CA-2, CA-7, AU-6	Sicherheitsbewertungen, kontinuierliche Überwachung, Prüfung/Analyse/Berichterstattung zu Audit-Protokollen
DSGVO	Artikel 24 und 32	Auditierung technischer und organisatorischer Maßnahmen, Nachweise der Compliance zur Kontrollwirksamkeit
NIS2	Artikel 21(2)(f)	Proaktive Überprüfung und nachweisgestützte Compliance
DORA	Artikel 10	Management von IKT-Risiken, Überwachung und Berichterstattung
COBIT 2019	MEA01, MEA03	Überwachung/Konformitätsbewertung, Compliance, Bereitschaft für Überprüfungen durch Dritte

1. Zweck

1.1 Diese Richtlinie legt den Ansatz der Organisation für die Durchführung interner Audits, die Prüfung von Sicherheitskontrollen und die Überwachung der Einhaltung regulatorischer Anforderungen fest. Sie stellt sicher, dass alle Kontrollen, Richtlinien, Systeme und Dienstleister regelmäßig und strukturiert überprüft werden.

1.2 Ziel ist es, Kontrollversagen zu erkennen, Nichteinhaltung zu verhindern und die gebotene Sorgfalt im Rahmen von ISO/IEC 27001, DSGVO und verwandten Rahmenwerken nachzuweisen.

1.3 Sie ermöglicht es KMU, auch ohne eigene Compliance-Funktion die operative Steuerung und Auditbereitschaft für Zertifizierungen durch einfache, wiederholbare Checklisten und risikoorientierte Feststellungen aufrechtzuerhalten.

2. Geltungsbereich

2.1 Diese Richtlinie gilt für:

2.1.1 alle internen Abteilungen und externen Dienstleister mit Verantwortlichkeiten in Bezug auf IT-Systeme, personenbezogene Daten und geschäftskritische Services

2.1.2 alle Kontrollen und Systeme innerhalb des ISMS-Geltungsbereichs des Informationssicherheitsmanagementsystems (ISMS)

2.1.3 alle internen Audits, Überprüfungen von Sicherheitskontrollen und Compliance-Prüfungen, unabhängig davon, ob diese intern oder durch einen externen Berater, Kunden oder eine Regulierungsbehörde durchgeführt werden

2.2 Diese Richtlinie gilt außerdem für die Erhebung von Nachweisen und die Berichterstattung für:

2.2.1 Zertifizierungs- und Rezertifizierungsaudits nach ISO/IEC 27001

2.2.2 Datenschutzaudits nach DSGVO oder auf Grundlage vertraglicher Anforderungen

2.2.3 durch Kunden veranlasste Sicherheitsfragebögen oder Prüfungen im Rahmen der gebotenen Sorgfalt

2.2.4 regulatorische oder unabhängige Überprüfungen nach NIS2 oder DORA, soweit anwendbar

3. Ziele

3.1 Sicherstellen, dass alle wesentlichen Kontrollen und Richtlinien regelmäßig auf Wirksamkeit und Einhaltung überprüft werden.

3.2 Audit-Trails und Aufzeichnungen zu Korrekturmaßnahmen aufrechterhalten, um Rechenschaftspflicht und Verbesserungen nachzuweisen.

3.3 Vorbereitung auf Zertifizierungen, Rezertifizierungen und Programme zur Vertrauensbildung bei Kunden (z. B. ISO 27001, Onboarding von Lieferanten).

3.4 Lücken frühzeitig identifizieren, damit Mängel zeitnah behoben werden können, bevor Probleme eskalieren oder Verpflichtungen verletzt werden.

3.5 Den General Manager (GM) und den IT-Support-Dienstleister in die Lage versetzen, Überprüfungen mit minimaler Komplexität zu koordinieren und zugleich belastbare Ergebnisse sicherzustellen.

4. Rollen und Verantwortlichkeiten

4.1 General Manager (GM)

4.1.1 überwacht das Auditprogramm

4.1.2 genehmigt interne Auditpläne und Feststellungen

4.1.3 weist Korrekturmaßnahmen zu und verfolgt diese nach

4.1.4 genehmigt die Beauftragung externer Auditoren oder Berater

4.2 IT-Support-Dienstleister / Administrator

4.2.1 stellt im Rahmen interner und externer Audits Nachweise bereit, z. B. Protokolle, Konfigurationen und Aufzeichnungen zur Zugriffskontrolle

4.2.2 unterstützt bei technischen Prüfungen, z. B. zum Backup-Status oder zur Einhaltung von Patch-Vorgaben

4.2.3 pflegt das Audit-Repository für Nachweise

[... 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 von Richtlinie und Auditplan

9.1.1 Der General Manager (GM) muss diese Richtlinie und den Auditplan mindestens einmal jährlich überprüfen.

9.1.2 Die Überprüfung muss Folgendes bewerten:

9.1.2.1 die Wirksamkeit von Audits bei der Identifizierung von Lücken

9.1.2.2 die Abschlussquote von Audits und Korrekturmaßnahmen

9.1.2.3 Änderungen an geltenden rechtlichen, regulatorischen oder zertifizierungsbezogenen Anforderungen

9.2 Anlassbezogene Aktualisierungen

9.2.1 Die Richtlinie muss überprüft und aktualisiert werden, wenn:

9.2.2 ein Zertifizierungsaudit oder Überwachungsaudit zu einer wesentlichen Nichtkonformität führt

9.2.3 sich rechtliche oder regulatorische Rahmenbedingungen ändern, z. B. neue Leitlinien zur DSGVO oder die nationale Umsetzung von NIS2

9.2.4 geschäftliche Änderungen Systeme, Prozesse oder Lieferanten betreffen, die in den Audit-Geltungsbereich einbezogen sind

9.2.5 ein kritischer Vorfall oder eine Sicherheitsverletzung zuvor unerkannte Kontrolllücken aufdeckt

9.3 Dokumentation von Aktualisierungen

9.3.1 Alle Überarbeitungen müssen in einem Versionsprotokoll für Richtlinien nachverfolgt werden.

9.3.2 Aktualisierungen müssen an alle an Audits beteiligten Teammitglieder verteilt werden.

9.3.3 Der aktualisierten Richtlinie muss eine Zusammenfassung der Änderungen beigefügt werden, um das Verständnis sicherzustellen.

10. Zugehörige Richtlinien und Verknüpfungen

10.1 Diese Richtlinie wird durch mehrere weitere SME-Richtlinien unterstützt und ergänzt:

10.1.1 P1S – Informationssicherheitsrichtlinie: Legt die Basislinie für alle Kontrollerwartungen fest und fordert deren Durchsetzung durch Audits.

10.1.2 P2S – Richtlinie zu Governance-Rollen und Verantwortlichkeiten: Legt die Rechenschaftspflicht für Auditplanung, Durchführung und die Verantwortlichkeit für Korrekturmaßnahmen fest.

10.1.3 P6S – Risikomanagement-Richtlinie: Identifiziert in Audits aufgedeckte Kontrollschwächen und stellt sicher, dass Feststellungen im Risikoregister dokumentiert werden.

10.1.4 P17S – Richtlinie zu Datenschutz und Privatsphäre: Definiert DSGVO-Kontrollen, die auditiert werden müssen, einschließlich Datenverarbeitung, Reaktion auf Datenschutzverletzungen und Datenschutzhinweisen.

10.1.5 P22S – Richtlinie zur Protokollierung und Überwachung: Stellt die Audit-Protokolle und forensischen Daten bereit, die bei Compliance-Prüfungen und Kontrollüberprüfungen verwendet werden.

10.1.6 P30S – Incident-Response-Richtlinie: Verlangt die regelmäßige Auditierung von Vorfallsaufzeichnungen und Überprüfungen nach Ereignissen zur Verifizierung der Wirksamkeit der Reaktion.

10.1.7 P31S – Richtlinie zur Erhebung von Nachweisen und Forensik: Stellt die Verfahren zur Erhebung überprüfbarer Nachweise mit dokumentierter Chain of Custody im Rahmen von Audits bereit.

10.2 Zusammen bilden diese Richtlinien ein geschlossenes Kontrollumfeld, das interne Verifizierung, externe Vertrauensbildung und an Standards ausgerichtete Governance ermöglicht.

11. Referenzstandards und Rahmenwerke

11.1 ISO/IEC 27001:

11.1.1 Klausel 9.2 – fordert interne Audits zur Bewertung der Wirksamkeit des ISMS und der Übereinstimmung mit Anforderungen.

11.1.2 Klausel 10.1 – verlangt kontinuierliche Verbesserung auf Grundlage von Auditergebnissen und der Behandlung von Nichtkonformitäten.

11.2 ISO/IEC 27002:

11.2.1 Maßnahme 5.35 – verlangt geplante interne Überprüfungen von Kontrollen und Prozessen.

11.2.2 Maßnahme 5.37 – betont unabhängige Überprüfungen, insbesondere für ausgelagerte Prozesse.

11.3 NIST SP 800-53 Rev. 5:

11.3.1 CA-2 – Sicherheitsbewertungen: verlangt Audits implementierter Kontrollen zur Verifizierung ihrer Wirksamkeit.

11.3.2 CA-7 – Kontinuierliche Überwachung: betont die proaktive Erkennung und Überprüfung von Kontrollschwächen.

11.3.3 AU-6 – Prüfung, Analyse und Berichterstattung zu Audit-Protokollen: verlangt die regelmäßige Analyse und Bearbeitung von Audit-Protokollen und Feststellungen.

11.4 DSGVO:

11.4.1 Artikel 24 und 32 – verlangen die Umsetzung und Auditierung technischer und organisatorischer Maßnahmen, einschließlich Nachweisen zur Kontrollwirksamkeit und Verbesserung im Zeitverlauf.

11.5 NIS2-Richtlinie (EU) 2022/2555:

11.5.1 Artikel 20–21 – verlangen proaktive Kontrollüberprüfung, nachweisgestützte Compliance und Auditierbarkeit für wesentliche und wichtige Einrichtungen.

11.6 COBIT 2019:

11.6.1 MEA01 – Überwachen, Evaluieren und Beurteilen von Leistung und Konformität: verlangt die regelmäßige Bewertung der Prozess- und Kontrollleistung gegenüber Standards und Zielen.

11.6.2 MEA03 – Sicherstellen der Einhaltung externer Anforderungen: fokussiert auf interne Überwachung und Bereitschaft für Audits durch Dritte und regulatorische Überprüfungen.