					Fügen Sie hier den Namen der eingetragenen juristischen Person ein							
Dokumentnummer: P26S					Dokumenttitel: **Richtlinie zur Sicherheit von Lieferanten und Drittparteien**							
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 Vorschriften

Standard/Regelwerk	Klausel/Artikel	Kommentar
ISO/IEC 27001:2022	Klausel 8	Operative Kontrollen für Beziehungen zu Drittparteien und Lieferanten
ISO/IEC 27002:2022	Maßnahmen 5.19–5.22	Sicherheitskontrollen für Lieferanten, vertragliche Sicherheitsklauseln, Änderungsmanagement, Überwachung und Überprüfung
NIST SP 800-53 Rev.5	SA-9, SA-10, CA-3, PS-7	Beschaffung, Konfigurationsmanagement, Zusammenschaltungsvereinbarungen und Kontrollen für externes Personal
EU-DSGVO	Artikel 28, 32	Auftragsverarbeitungsverträge, Sicherheitsanforderungen an Auftragsverarbeiter
EU NIS2	Artikel 21(2)(a)(b)(i), 23(1)	Risikomanagement in der Lieferkette, Aufsicht über Dienstleistungen Dritter
EU DORA	Artikel 5(1)(2), 28(1)(2)	Management von IKT-Risiken für Drittanbieter von Dienstleistungen
COBIT 2019	APO10, APO12, DSS05	Lieferantenmanagement und Integration von Risiken

1. Zweck

1.1 Diese Richtlinie legt die verbindlichen Sicherheitsanforderungen für die Beauftragung, Steuerung und Beendigung von Beziehungen mit Drittparteien und Lieferanten fest, die auf Daten, Systeme oder Dienstleistungen der Organisation zugreifen oder diese beeinflussen.

1.2 Sie stellt sicher, dass externe Dienstleister – einschließlich IT-Support-Dienstleister, Betreiber von Cloud-Diensten, Softwareentwickler und Auftragnehmer für Geschäftsprozesse – Unternehmenswerte sicher und in Übereinstimmung mit geltenden Gesetzen und Standards handhaben.

1.3 Diese Richtlinie reduziert Risiken wie Datenabfluss, unbefugte Systemänderungen, regulatorische Sanktionen oder Unterbrechungen des Geschäftsbetriebs, die durch unsichere oder unzureichend gesteuerte Vereinbarungen mit Drittparteien entstehen.

2. Geltungsbereich

2.1 Diese Richtlinie gilt für alle Drittparteien, die:

2.1.1 Software, Infrastruktur, Hosting- oder Cloud-Dienste bereitstellen

2.1.2 auf interne Systeme, Geräte oder Anwendungen zugreifen oder diese verwalten

2.1.3 Unternehmensdaten, Dokumente oder Sicherungen verarbeiten

2.1.4 Geschäftsprozesse, Personalwesen, Finanzen oder Kundenservice unterstützen

2.2 Sie gilt außerdem für:

2.2.1 internes Personal, das an der Auswahl, Beauftragung oder Überwachung von Lieferanten beteiligt ist

2.2.2 sämtliches Personal, das das Onboarding von Lieferanten, Verträge, Zugriffe oder Überprüfungen verwaltet

2.2.3 jedes System oder jeden Prozess, der von Komponenten oder Dienstleistungen Dritter abhängt

3. Ziele

3.1 Sicherstellen, dass alle Lieferanten klar definierte Sicherheitserwartungen erfüllen.

3.2 Sicherstellen, dass Lieferantenverträge durchsetzbare Verpflichtungen zu Informationssicherheit, Datenschutz und Reaktion auf Sicherheitsvorfälle enthalten.

3.3 Lieferantenrisiken bewerten und dokumentieren, bevor Vereinbarungen unterzeichnet oder Zugriffe gewährt werden.

3.4 Regelmäßige Überprüfungen für Lieferanten mit hohem Risiko oder kritische Lieferanten durchführen, um die Einhaltung zu bestätigen.

3.5 Einen formalen Prozess für Ausnahmen, Vorfallmanagement und Vertragsaktualisierungen festlegen.

3.6 Die Einhaltung von Verpflichtungen aus ISO/IEC 27001:2022, DSGVO, NIS2 und DORA im Zusammenhang mit der Steuerung von Lieferanten unterstützen.

4. Rollen und Verantwortlichkeiten

4.1 General Manager (GM)

4.1.1 Trägt die Gesamtverantwortung für die Auswahl von Lieferanten und die Einhaltung der Sicherheitsanforderungen

4.1.2 Genehmigt Verträge, Ausnahmen und Eskalationen im Zusammenhang mit Lieferanten

4.1.3 Überwacht die Reaktion auf Sicherheitsvorfälle und die Entscheidungsfindung, wenn Lieferanten ihren Verpflichtungen nicht nachkommen

4.2 IT-Dienstleister oder interner Ansprechpartner für Informationssicherheit

4.2.1 Bewertet den von Lieferanten angeforderten technischen Zugriff

4.2.2 Setzt Regeln zur Zugriffskontrolle um, prüft Protokolle und verifiziert den sicheren Umgang mit Daten

4.2.3 Prüft Nachweise zu Sicherheitskontrollen, Zertifizierungen oder Auditergebnissen, soweit anwendbar

[... 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 Diese Richtlinie muss mindestens jährlich durch den General Manager unter Beteiligung des IT-Dienstleisters oder Lieferantenverantwortlichen überprüft werden.

9.2 Die Richtlinie muss außerdem überprüft werden:

9.2.1 nach jeder wesentlichen Änderung gesetzlicher, regulatorischer oder vertraglicher Verpflichtungen

9.2.2 nach einem lieferantenbezogenen Informationssicherheitsvorfall oder einer Auditfeststellung

9.2.3 bei Einführung neuer Lieferantenkategorien, z. B. kritischer SaaS-Plattformen

9.3 Alle Aktualisierungen müssen:

9.3.1 mit Versionshistorie und Begründung dokumentiert werden

9.3.2 vom General Manager genehmigt werden

9.3.3 relevanten internen Mitarbeitenden und Lieferantenverantwortlichen mitgeteilt werden

9.3.4 gemäß der P14S – Richtlinie zur Datenaufbewahrung und Entsorgung zusammen mit früheren Versionen aufbewahrt werden

10. Verwandte Richtlinien und Verknüpfungen

10.1 Die Wirksamkeit dieser Richtlinie hängt von der Abstimmung mit den folgenden SME-Richtlinien zur Informationssicherheit ab:

10.1.1 P2S – Richtlinie zu Governance-Rollen und Verantwortlichkeiten: Legt die Rechenschaftspflicht für die Überwachung von Lieferanten und die Durchsetzung vertraglicher Verpflichtungen fest.

10.1.2 P4S – Richtlinie zur Zugriffskontrolle: Legt die Regeln für Zugriffsbeschränkungen fest, die anzuwenden sind, wenn Lieferanten Systemzugriff erhalten.

10.1.3 P17S – Richtlinie zu Datenschutz und Privatsphäre: Stellt sicher, dass Lieferanten, die personenbezogene Daten verarbeiten, Datenschutzgrundsätze und rechtliche Anforderungen einhalten.

10.1.4 P14S – Richtlinie zur Datenaufbewahrung und Entsorgung: Gilt für alle Daten oder Aufzeichnungen, die mit Lieferanten geteilt oder von ihnen gespeichert werden, und regelt die sichere Entsorgung nach Vertragsbeendigung.

10.1.5 P30S – Richtlinie zur Reaktion auf Sicherheitsvorfälle: Definiert das Vorgehen, wenn ein Lieferant einen Informationssicherheitsvorfall verursacht oder daran beteiligt ist, einschließlich Eskalationsverfahren und Verfahren zum Umgang mit Nachweisen.

10.2 Diese Richtlinien wirken zusammen, um sicherzustellen, dass Lieferantenrisiken über den gesamten Vertragslebenszyklus hinweg gesteuert werden.

11. Referenzstandards und Rahmenwerke

11.1 ISO/IEC 27001

11.1.1 Klausel 8.1 – Verlangt die Umsetzung operativer Kontrollen, einschließlich derjenigen, die für Beziehungen zu Drittparteien und Lieferanten gelten.

11.2 ISO/IEC 27002

11.2.1 Maßnahme 5.19 – Stellt sicher, dass Sicherheitsmaßnahmen für Lieferanten an den Anforderungen der Organisation ausgerichtet sind.

11.2.2 Maßnahme 5.20 – Verlangt formale Vereinbarungen, die Sicherheitsklauseln, Verantwortlichkeiten und Pflichten bei Sicherheitsverletzungen abdecken.

11.2.3 Maßnahme 5.21 – Steuert Änderungen an Lieferantendienstleistungen, die sich auf das Risikoprofil der Informationssicherheit auswirken können.

11.2.4 Maßnahme 5.22 – Verlangt die Überwachung und Überprüfung von Lieferantendienstleistungen und deren Einhaltung.

11.3 NIST SP 800-53 Rev.5

11.3.1 SA-9 – Regelt die Beschaffung externer Systeme und Dienstleistungen und verlangt Risikobewertungen sowie klar definierte Erwartungen.

11.3.2 SA-10 – Steuert Konfigurations- und Änderungsverfahren bei von Drittparteien verwalteten Systemen.

11.3.3 CA-3 – Verlangt Zusammenschaltungsvereinbarungen für Systeme mit externen Stellen.

11.3.4 PS-7 – Legt Prüfungen und Rechenschaftspflicht für externes Personal fest.

11.4 EU-DSGVO (2016/679)

11.4.1 Artikel 28 – Verlangt Auftragsverarbeitungsverträge mit Lieferanten, die als Auftragsverarbeiter tätig sind.

11.4.2 Artikel 32 – Schreibt angemessene technische und organisatorische Sicherheitsmaßnahmen für alle Auftragsverarbeiter vor.

11.5 EU NIS2-Richtlinie (2022/2555)

11.5.1 Artikel 21(2)(a), (b), (i) – Schreibt das Management von Risiken in der IKT-Lieferkette und Kontrollen für Drittparteien vor.

11.5.2 Artikel 23(1) – Verlangt eine dokumentierte Aufsicht über Dienstleistungen Dritter für wesentliche und wichtige Einrichtungen.

11.6 EU DORA (2022/2554)

11.6.1 Artikel 5(1) – Verlangt ein Rahmenwerk für das Management von IKT-Risiken, das alle kritischen Drittanbieter abdeckt.

11.6.2 Artikel 5(2) – Legt vertragliche und operative Kontrollen für Abhängigkeiten von IKT-Dienstleistungen fest.

11.6.3 Artikel 28(1), (2) – Etabliert Aufsichtsregeln für IKT-Drittparteienrisiken im Finanzsektor.

11.7 COBIT 2019

11.7.1 APO10 – „Manage Suppliers“ beschreibt Kontrollen für die Beschaffung und Erwartungen an das Beziehungsmanagement.

11.7.2 APO12 – „Manage Risk“ integriert Lieferantenrisiken in die organisatorische Risikosteuerung.

11.7.3 DSS05 – „Manage Security Services“ gilt für durch Drittparteien erbrachte und ausgelagerte Sicherheitsdienstleistungen.