					Fügen Sie hier den Namen der eingetragenen juristischen Person ein							
Dokumentnummer: P26					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 regulatorischen Anforderungen

Standard/Verordnung	Klausel/Artikel	Kommentar
ISO/IEC 27001:2022	Klausel 8	Betriebliche Planung und Steuerung: Erfordert formale Kontrollen für Dienstleistungen von Drittparteien mit Auswirkungen auf das ISMS
ISO/IEC 27002:2022	Maßnahmen 5.19–5.22	Richtlinien und Verfahren für Lieferantenbeziehungen; Management von Lieferantenrisiken; Management der Leistungserbringung durch Lieferanten; Überwachung und Überprüfung von Lieferanten
NIST SP 800-53 Rev. 5	SA-9, SA-10, CA-3, PS-7	Externe Systemservices; Konfigurationsmanagement für Entwickler; Systemverbindungen; Personalsicherheit bei Drittparteien
DSGVO	Artikel 28, 32, 33	Pflichten von Auftragsverarbeitern, Sicherheit der Verarbeitung, Meldung von Verletzungen des Schutzes personenbezogener Daten
EU NIS2	Artikel 21(2)(e–f)	Risikobasiertes Lieferantenmanagement und Sicherheitsaufsicht
EU DORA	Artikel 28, 30	IKT-Drittparteienrisiko, Aufsicht über kritische IKT-Drittanbieter
COBIT 2019	BAI05, DSS02, MEA03	Organisatorische Veränderungsbefähigung steuern; Serviceanfragen und Vorfälle verwalten; Einhaltung überwachen, evaluieren und beurteilen

1. Zweck

1.1 Diese Richtlinie definiert die Anforderungen an die Informationssicherheit für die Begründung, Steuerung und Aufrechterhaltung sicherer Beziehungen zu Drittparteien, Lieferanten und Dienstleistern.

1.2 Sie stellt sicher, dass alle Lieferanten mit Zugriff auf Daten, Systeme oder Infrastrukturen der Organisation während des gesamten Servicelebenszyklus strengen Sicherheitskontrollen, vertraglichen Schutzmaßnahmen und einer kontinuierlichen Überwachung unterliegen.

1.3 Die Richtlinie unterstützt die Maßnahmen 5.19 bis 5.22 des Anhangs A der ISO/IEC 27001, indem Sicherheitsanforderungen in die Beschaffung, das Lieferanten-Onboarding, die Lieferanten-Due-Diligence, das Vertragsmanagement, die Serviceüberwachung und die Prozesse zur Vertragsbeendigung eingebettet werden.

2. Geltungsbereich

2.1 Diese Richtlinie gilt für:

2.1.1 alle Drittparteien, Lieferanten, Auftragnehmer, Cloud-Anbieter und Serviceorganisationen, die Informationswerte der Organisation verarbeiten oder auf diese zugreifen

2.1.2 alle internen Rollen, die an Lieferantenbewertung, Lieferanten-Onboarding, Vertragsabschluss, Risikomanagement, Überwachung oder Vertragsbeendigung beteiligt sind

2.1.3 alle Lieferantenbeziehungen, die den Zugriff auf sensible Daten, die Integration in Produktivservices oder die Unterstützung kritischer Geschäftsfunktionen umfassen

2.2 Sie umfasst sowohl direkte Lieferanten als auch deren Unterauftragnehmer, soweit anwendbar, und schließt Software, Infrastruktur, Support und Managed Services von Drittparteien ein.

3. Ziele

3.1 Sicherstellen, dass Sicherheitsrisiken im Zusammenhang mit Lieferanten über den gesamten Lebenszyklus der Geschäftsbeziehung hinweg konsistent identifiziert, bewertet und behandelt werden.

3.2 Standardisierte Sicherheitsanforderungen in alle Lieferantenverträge integrieren, einschließlich Meldepflichten bei Sicherheitsvorfällen, Auditrechten und Verantwortlichkeiten im Datenschutz.

3.3 Formale Lieferanten-Due-Diligence-Prüfungen und dokumentierte Risikobewertungen verlangen, bevor neue Lieferanten beauftragt oder Servicevereinbarungen mit hohem Risiko verlängert werden.

3.4 Mechanismen zur kontinuierlichen Überwachung der Compliance von Lieferanten einrichten, einschließlich Leistungsüberprüfungen, Audits und Eskalation von Vorfällen.

3.5 Änderungen an Lieferantenservices steuern und ein sicheres Offboarding sowie die Rückgabe oder Vernichtung von Daten bei Vertragsbeendigung durchsetzen.

3.6 Sicherheitskontrollen für Drittparteien an anwendbaren regulatorischen und vertraglichen Verpflichtungen ausrichten, einschließlich DSGVO, NIS2, DORA und ISO/IEC 27001.

4. Rollen und Verantwortlichkeiten

4.1 Chief Information Security Officer (CISO)

4.1.1 Ist Eigentümer dieser Richtlinie und stellt deren Ausrichtung am gesamten ISMS, am Risikomanagement und an der Compliance-Strategie sicher.

4.1.2 Genehmigt Lieferantenklassifizierungsstufen, Ergebnisse von Sicherheitsbewertungen und Ausnahmen mit hohem Risiko.

4.1.3 Wirkt an der Eskalation schwerwiegender Lieferantenvorfälle und an Vertragsverhandlungen für kritische Services mit.

4.2 Beschaffung und Lieferantenmanagement

4.2.1 Stellt sicher, dass alle neuen und verlängerten Lieferantenverträge genehmigte Sicherheits- und Datenschutzklauseln enthalten.

4.2.2 Pflegt das zentrale Lieferantenregister und koordiniert sich mit der Rechtsabteilung und den Compliance-Verantwortlichen hinsichtlich der Dokumentation von Drittparteienrisiken.

4.2.3 Initiiert Onboarding-Prozesse und stellt die Abstimmung mit Sicherheitsbewertungen vor Vertragsabschluss sicher.

[... 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 oder früher überprüft werden, wenn eines der folgenden Ereignisse eintritt:

9.1.1 wesentliche Änderungen der Beschaffungsstrategie oder des Lieferantenökosystems

9.1.2 Aktualisierungen rechtlicher oder regulatorischer Rahmenwerke (z. B. DORA, DSGVO)

9.1.3 schwerwiegende Vorfälle bei Drittparteien, Datenschutzverletzungen oder Audit-Feststellungen mit erheblichen Mängeln

9.1.4 Feststellungen aus Risikobewertungen oder von externen Zertifizierungsstellen

9.2 Der Überprüfungsprozess liegt gemeinsam in der Verantwortung von CISO, Beschaffung, Rechtsabteilung und Risikomanagement.

9.3 Alle Überarbeitungen dieser Richtlinie müssen im Register der ISMS-Dokumentenlenkung dokumentiert, versionskontrolliert und über Kanäle der Lieferanten-Governance sowie Sensibilisierungsprogramme für Mitarbeitende an relevante Interessengruppen kommuniziert werden.

9.4 Ersetzte Versionen müssen zur Sicherstellung der Nachvollziehbarkeit und der rechtlichen Compliance mindestens drei Jahre archiviert werden.

10. Verwandte Richtlinien und Verknüpfungen

10.1 P1 – Richtlinie zur Informationssicherheit. Legt die übergreifende Verpflichtung fest, alle organisatorischen Tätigkeiten sicher auszugestalten, einschließlich der Abhängigkeit von Drittparteien, Lieferanten und externen IT-Dienstleistern.

10.2 P6 – Risikomanagement-Richtlinie. Leitet die Identifizierung, Bewertung und Minderung von Risiken im Zusammenhang mit Drittparteienbeziehungen, einschließlich übernommener oder systemischer Risiken aus Lieferantenökosystemen.

10.3 P17 – Richtlinie zu Datenschutz und Privatsphäre. Gilt für alle Lieferanten, die personenbezogene Daten verarbeiten, und verlangt angemessene vertragliche Bedingungen, Schutzmaßnahmen bei Übermittlungen und Datenschutz durch Technikgestaltung.

10.4 P4 – Richtlinie zur Zugriffskontrolle. Regelt, wie Personal von Drittparteien Zugriff auf Systeme der Organisation erhält, und setzt rollenbasierte Berechtigungen, Sitzungssteuerungen und Verfahren zum Entzug von Zugriffsrechten durch.

10.5 P22 – Richtlinie zur Protokollierung und Überwachung. Verlangt, dass Zugriffe von Lieferanten auf Systeme überwacht, protokolliert und überprüft werden, insbesondere in Umgebungen, in denen privilegierte oder datenbezogene Tätigkeiten stattfinden.

10.6 P30 – Incident-Response-Richtlinie (P30). Definiert Eskalationsverfahren und Anforderungen an die Meldung von Sicherheitsvorfällen für von Lieferanten verursachte Sicherheitsereignisse oder gemeinsame Untersuchungen unter Beteiligung von Systemen von Drittparteien.

11. Referenzstandards und Rahmenwerke

11.1 ISO/IEC 27001: Klausel 8.1 – Betriebliche Planung und Steuerung: Erfordert formale Kontrollen für Dienstleistungen von Drittparteien mit Auswirkungen auf das ISMS.

11.2 ISO/IEC 27002:2022 – Maßnahmen 5.19 bis 5.22:

11.2.1 Anhang A Maßnahme 5.19 – Richtlinien und Verfahren für Lieferantenbeziehungen: Verlangt Kontrollen zur Steuerung von Interaktionen mit Lieferanten.

11.2.2 Anhang A Maßnahme 5.20 – Management von Lieferantenrisiken: Fokussiert auf die Identifizierung, Bewertung und fortlaufende Überwachung des Informationssicherheitsrisikoprofils von Lieferanten.

11.2.3 Anhang A Maßnahme 5.21 – Management der Leistungserbringung durch Lieferanten: Erfordert die Ausrichtung von Leistung und Sicherheit an vertraglichen Erwartungen.

11.2.4 Anhang A Maßnahme 5.22 – Überwachung und Überprüfung von Lieferanten: Bekräftigt die Notwendigkeit der fortlaufenden Validierung und Neubewertung der Compliance von Drittparteien.

11.3 NIST SP 800-53 Rev. 5:

11.3.1 SA-9 – Externe Systemservices: Definiert Sicherheits- und Risikoanforderungen für Systeme, die von externen Stellen betrieben werden.

11.3.2 SA-10 – Konfigurationsmanagement für Entwickler: Gilt, wenn Drittparteien Software oder Umgebungen bereitstellen.

11.3.3 CA-3 – Systemverbindungen: Erfordert Aufsicht und Vereinbarungen über Datenflüsse zwischen Systemen verschiedener Stellen.

11.3.4 PS-7 – Personalsicherheit bei Drittparteien: Stellt sicher, dass Auftragnehmer und Personal von Lieferanten angemessen überprüft und überwacht werden.

11.4 DSGVO (2016/679):

11.4.1 Artikel 28 – Pflichten von Auftragsverarbeitern: Erfordert schriftliche Vereinbarungen mit Auftragsverarbeitern einschließlich technischer und organisatorischer Maßnahmen.

11.4.2 Artikel 32 – Sicherheit der Verarbeitung: Verlangt angemessene Schutzmaßnahmen sowohl durch Verantwortliche als auch durch Auftragsverarbeiter.

11.4.3 Artikel 33 – Meldung von Verletzungen des Schutzes personenbezogener Daten: Erfordert eine unverzügliche Meldung durch Lieferanten im Fall einer Verletzung.

11.5 EU-NIS2-Richtlinie (2022/2555):

11.5.1 Artikel 21(2)(e–f): Verlangt risikobasiertes Lieferantenmanagement und Sicherheitsaufsicht, insbesondere in digitalen Lieferketten wesentlicher und wichtiger Einrichtungen.

11.6 EU DORA (2022/2554):

11.6.1 Artikel 28 – IKT-Drittparteienrisiko: Begründet Verpflichtungen zu Risikobewertung, vertraglichen Sicherheitsbedingungen und Ausstiegsstrategien für Anbieter von Finanzdienstleistungen.

11.6.2 Artikel 30 – Aufsicht über kritische IKT-Drittanbieter: Etabliert erhöhte Anforderungen an Überwachung und Aufsicht für wesentliche Lieferanten.

11.7 COBIT 2019:

11.7.1 BAI05 – Organisatorische Veränderungsbefähigung steuern: Stellt sicher, dass Lieferantenübergänge sicher gesteuert werden.

11.7.2 DSS02 – Serviceanfragen und Vorfälle verwalten: Gilt für von Lieferanten gemeldete Probleme und die Integration in das Vorfallmanagement.

11.7.3 MEA03 – Einhaltung überwachen, evaluieren und beurteilen: Bekräftigt die Leistungsmessung und Überwachung der Compliance bei Lieferanten.