					Fügen Sie hier den Namen der eingetragenen juristischen Person ein							
Dokumentnummer: P28					Dokumenttitel: **Richtlinie für ausgelagerte Entwicklung**							
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/Regulation	Clause/Article	Comment
ISO/IEC 27001:2022	Clause 8.1	N/A
ISO/IEC 27002:2022	Controls 5.19-5.22, 8	N/A
NIST SP 800-53 Rev.5	SA-4, SA-9, SA-10	N/A
EU GDPR	Articles 28, 32	N/A
EU NIS2	Articles 21(2)(a), (h), 23	N/A
EU DORA	Articles 28(1), (2)	N/A
COBIT 2019	APO10, BAI03, DSS	N/A

1. Zweck

1.1 Diese Richtlinie legt verbindliche Kontrollen für die Auslagerung der Software- oder Systementwicklung an externe Lieferanten, Auftragnehmer oder Agenturen fest und stellt sicher, dass sichere Praktiken über den gesamten Systementwicklungslebenszyklus hinweg verankert sind.

1.2 Sie dient der Vermeidung von Sicherheitslücken, Datenverlust, Offenlegung geistigen Eigentums und Verstößen gegen Compliance-Verpflichtungen infolge ausgelagerter Entwicklungsleistungen.

1.3 Die Richtlinie schreibt Vorgaben zur Lieferantensteuerung, Standards für sicheres Programmieren, Benutzerzugriffsverwaltung, Überwachungspflichten und das Offboarding bei Vertragsende vor, um die Vertraulichkeit, Integrität und Verfügbarkeit entwickelter Software zu gewährleisten.

2. Geltungsbereich

2.1 Diese Richtlinie gilt für alle Organisationseinheiten, die externe Stellen mit der Software- oder Systementwicklung beauftragen, einschließlich:

2.1.1 Webanwendungen, mobiler Apps, eingebetteter Systeme, APIs, Skripte, Automatisierungs-Workflows oder Plattformmodule

2.1.2 kundenspezifischer Entwicklung für interne Plattformen, kundenseitige Systeme oder kommerzielle Produkte

2.1.3 Beauftragungen von Drittentwicklern, Freelancern, Agenturen oder Offshore-Teams

2.2 Die Richtlinie gilt außerdem für jede externe Stelle, die während der Entwicklung auf Quellcode, Testumgebungen oder CI/CD-Pipelines zugreift.

2.3 Die Anforderungen sind unabhängig von Vertragsart, Entwicklungsmethodik oder geografischem Standort des ausgelagerten Anbieters verbindlich.

3. Ziele

3.1 Sicherstellung sicherer Praktiken im Systementwicklungslebenszyklus (SDLC) über alle ausgelagerten Beauftragungen hinweg, von der Planung bis zur Validierung nach der Bereitstellung.

3.2 Sicherstellung, dass alle Verträge mit externen Entwicklern verbindliche Klauseln zu Datenschutz, sicherem Programmieren und zum Verbleib geistigen Eigentums enthalten.

3.3 Festlegung von Anforderungen an Zugriffskontrolle, Überwachung und Audits für Drittentwickler, die mit internen Systemen interagieren.

3.4 Schutz der Organisation vor Risiken in der Lieferkette, Rechtsverstößen und Reputationsschäden im Zusammenhang mit extern entwickelter Software.

3.5 Aufrechterhaltung der fortlaufenden Einhaltung von Sicherheitsrahmenwerken, einschließlich ISO/IEC 27001, NIST, DSGVO, NIS2, DORA und COBIT 2019.

4. Rollen und Verantwortlichkeiten

4.1 Geschäftsleitung

4.1.1 Genehmigt ausgelagerte Entwicklungsprojekte mit hohem Risiko und genehmigt Richtlinienausnahmen, sofern diese begründet sind.

4.1.2 Stellt sicher, dass Auslagerungsentscheidungen mit den strategischen Zielen und der Risikobereitschaft des Unternehmens im Einklang stehen.

4.2 Chief Information Security Officer (CISO)

4.2.1 Genehmigt das Lieferanten-Onboarding aus Sicht der Informationssicherheit.

4.2.2 Definiert Anforderungen an Sicherheitskontrollen für ausgelagerte Beauftragungen und prüft Vorfallberichte.

[... 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 ist mindestens einmal jährlich oder häufiger unter den folgenden Umständen zu überprüfen:

9.1.1 Einführung neuer Modelle, Lieferanten oder Rechtsräume für Entwicklungsoutsourcing

9.1.2 Aktualisierungen regulatorischer Rahmenwerke wie DSGVO, NIS2 oder DORA

9.1.3 nach einem Sicherheitsvorfall im Zusammenhang mit ausgelagertem Code, Zugriffen oder Liefergegenständen

9.1.4 als Teil von Audit-Feststellungen oder Verbesserungen des ISMS

9.2 Der Chief Information Security Officer (CISO) ist für die Einleitung und Koordination der Richtlinienüberprüfung in Abstimmung mit den folgenden Stellen verantwortlich:

9.2.1.1 Rechtsabteilung und Einkauf (zur Ausrichtung der vertraglichen Durchsetzung)

9.2.1.2 Projekt- und Produktverantwortliche (zur operativen Umsetzbarkeit)

9.2.1.3 Informationssicherheitsteam (für Aktualisierungen zu Bedrohungen und Kontrollen)

9.2.1.4 Geschäftsleitung (zur endgültigen Genehmigung)

9.3 Alle Aktualisierungen der Richtlinie müssen:

9.3.1.1 versionskontrolliert und in einem benannten Dokumenten-Repository gespeichert werden

9.3.1.2 den an ausgelagerten Entwicklungsaktivitäten beteiligten Interessenträgern kommuniziert werden

9.3.1.3 mit etwaigen Aktualisierungen in verknüpften Richtlinien oder Verfahrensdokumentationen abgeglichen werden

9.4 Jeder Richtlinienversion ist ein Änderungsprotokoll beizufügen, um die Nachvollziehbarkeit von Änderungen und Genehmigungen sicherzustellen.

10. Verknüpfte Richtlinien und Bezüge

10.1 Diese Richtlinie unterstützt die folgenden zugehörigen Dokumente und wird durch diese unterstützt:

10.1.1 P1 - Richtlinie zur Informationssicherheit: Legt unternehmensweite Sicherheitsgrundsätze fest, die in internen und durch Dritte betriebenen Entwicklungsumgebungen gelten.

10.1.2 P5 - Änderungsmanagement-Richtlinie: Stellt sicher, dass alle bereitstellungsbezogenen Änderungen aus ausgelagerten Codebasen vor der Umsetzung geprüft und genehmigt werden.

10.1.3 P13 - Richtlinie zur Datenklassifizierung und Kennzeichnung: Legt fest, wie sensible Daten identifiziert werden, bevor sie gegenüber Entwicklungslieferanten oder in Repositories offengelegt werden.

10.1.4 P18 - Richtlinie zu kryptografischen Kontrollen: Gibt vor, wie Schlüssel, Geheimnisse und sensible Zugangsdaten während Entwicklung und Übergabe zu handhaben sind.

10.1.5 P24 - Richtlinie zur sicheren Entwicklung: Definiert Basisanforderungen für interne und externe Praktiken der Softwareentwicklung.

10.1.6 P30 - Incident-Response-Richtlinie: Regelt, wie Verstöße oder Sicherheitsprobleme im Zusammenhang mit ausgelagerter Entwicklung eskaliert, untersucht und behoben werden.

10.1.7 P33 - Richtlinie zur Audit- und Compliance-Überwachung: Legt Anforderungen für die Überprüfung ausgelagerter Entwicklungsaktivitäten während Audits oder Compliance-Prüfungen fest.

11. Referenzstandards und Rahmenwerke

11.1 Diese Richtlinie ist an international anerkannten Sicherheitsrahmenwerken und Vorschriften ausgerichtet, um die sichere Auslagerung der Softwareentwicklung und praktikable Verfahren des Lieferantenmanagements sicherzustellen.

11.2 ISO/IEC 27001

11.2.1 Clause 8.1 - Operative Planung und Steuerung: Schreibt Prozesskontrollen für sichere Entwicklung und die sichere Leistungserbringung durch Dritte vor.

11.3 ISO/IEC 27002:2022 - Controls 5.19 bis 5.21, 8

11.3.1 Annex A Control 5.19 - Management von Lieferantenbeziehungen: Erfordert formale Vereinbarungen mit Klauseln zu Sicherheit und Compliance.

11.3.2 Annex A Control 5.20 - Berücksichtigung der Informationssicherheit in Lieferantenvereinbarungen: Stellt sicher, dass entwicklungsspezifische Kontrollen in Verträgen verankert sind.

11.3.3 Annex A Control 5.21 - Steuerung der Leistungserbringung durch Lieferanten: Umfasst die Überwachung von Entwicklungs-Liefergegenständen und Drittrisiken.

11.3.4 Annex A Control 8.27 - Ausgelagerte Entwicklung: Schreibt definierte Sicherheitsanforderungen und Zugriffskontrollen für extern entwickelte Software vor.

11.3.5 Diese Kontrollen definieren strukturierte Anforderungen an die Auswahl, vertragliche Bindung und Überwachung ausgelagerter Entwickler, einschließlich sicherer Entwicklungspraktiken, Code-Handhabung und Validierung der Leistungserbringung.

11.4 NIST SP 800-53 Rev.5

11.4.1 SA-4 - Beschaffungsprozess: Erfordert, dass Anforderungen an sichere Entwicklung bereits zum Zeitpunkt der Beschaffung festgelegt werden.

11.4.2 SA-9 - Externe Systemdienste: Regelt, wie Drittentwickler sicher mit internen Diensten interagieren.

11.4.3 SA-10 - Konfigurationsmanagement der Entwickler: Entspricht den Verpflichtungen externer Teams hinsichtlich Versionskontrolle, Codezugriff und Änderungsnachverfolgung.

11.5 EU GDPR (2016/679)

11.5.1 Article 28 - Pflichten des Auftragsverarbeiters: Erfordert, dass Verträge mit Drittentwicklern Sicherheits-, Kontroll- und Auditanforderungen für den Umgang mit personenbezogenen Daten festlegen.

11.5.2 Article 32 - Sicherheit der Verarbeitung: Schreibt angemessene Schutzmaßnahmen vor (z. B. Verschlüsselung, Zugriffskontrolle), wenn Systeme entwickelt werden, die personenbezogene Daten verarbeiten.

11.6 EU-NIS2-Richtlinie (2022/2555)

11.6.1 Articles 21(2)(a), (h), 23: Schreiben vor, dass sichere Entwicklungspraktiken über Drittbeauftragungen und digitale Lieferketten hinweg mit Aufsicht und technischer Verifizierung angewendet werden.

11.7 EU DORA (2022/2554)

11.7.1 Articles 28(1), (2): Schreiben vor, dass Finanzunternehmen IKT-Drittparteienrisiken durch vertragliche Kontrollen und die Überwachung sicherer Entwicklung steuern, insbesondere bei kritischer ausgelagerter Entwicklung.

11.8 COBIT 2019

11.8.1 APO10 - Lieferanten verwalten: Legt strukturierte Anforderungen an Lieferantenbewertung, Verträge und Leistungsüberwachung fest.

11.8.2 BAI03 - Lösungsentwicklung verwalten: Entspricht unmittelbar sicheren SDLC-Prozessen, Codeprüfungen und der Validierung der Entwicklung.

11.8.3 DSS05 - Sicherheitsdienste verwalten: Entspricht der Überwachung und dem Schutz von Systemen, die extern oder durch Dritte entwickelt wurden.