					Fügen Sie hier den Namen der eingetragenen juristischen Person ein							
Dokumentnummer: P28S					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/Regelwerk	Klausel/Artikel	Kommentar
ISO/IEC 27001:2022	Klauseln 5.1, 6.1, 8	Anwendbare Kontrollen im Zusammenhang mit dem ISMS und Lieferanten
ISO/IEC 27002:2022	Maßnahmen 5.19, 5.20, 8.25–8.27	Kontrollen zu Lieferanten und zum sicheren Systementwicklungslebenszyklus
NIST SP 800-53 Rev. 5	SA-4, SA-9, SA-11, SA-15, SR-3	Anforderungen an Beschaffung, Lieferkette, sichere Entwicklung und Lieferantenvereinbarungen
DSGVO	Artikel 28	Vertragliche Anforderungen und Datenschutzanforderungen für die Verarbeitung durch Dritte
EU-NIS2	Artikel 21(2)(a), (h)	Kontrollen zur Sicherheit der Lieferkette und zur sicheren Anwendungsentwicklung
EU-DORA	Artikel 10	Management von IKT-Drittparteienrisiken einschließlich ausgelagerter Entwicklung
COBIT 2019	BAI03, DSS05	Anforderungen an externe Entwicklung und externe IT-Dienstleister

1. Zweck

1.1 Diese Richtlinie stellt sicher, dass jede ausgelagerte Softwareentwicklung – unabhängig davon, ob sie durch Freiberufler, Agenturen oder Drittanbieter erfolgt – sicher durchgeführt, vertraglich geregelt und an geltenden gesetzlichen, regulatorischen und Audit-Anforderungen ausgerichtet wird.

1.2 Sie schützt die Organisation vor Risiken durch unsicheren Code, unklare Eigentumsverhältnisse, Datenoffenlegung und unzureichende Steuerung von Lieferanten, indem verbindliche Entwicklungsstandards und eine angemessene Lieferantenüberwachung auch ohne eigene IT-Abteilung durchgesetzt werden.

1.3 Diese Richtlinie unterstützt die Zertifizierung nach ISO/IEC 27001:2022, indem sie klar definierte Erwartungen an die Entwicklung, Rechenschaftspflicht und dokumentierte Kontrollen für Entwicklungsaktivitäten Dritter festlegt.

2. Geltungsbereich

2.1 Diese Richtlinie gilt für:

2.1.1 alle ausgelagerten Entwickler, einschließlich Freiberuflern und Entwicklungsagenturen,

2.1.2 sämtliche Entwicklungsarbeiten im Zusammenhang mit internen Werkzeugen, öffentlich erreichbaren Websites, Softwareanwendungen oder Geschäftsautomatisierung,

2.1.3 Mitarbeitende, die für die Auswahl, Steuerung oder Überwachung externer Entwickler verantwortlich sind,

2.1.4 jede Systemintegration, Skripterstellung oder Entwicklung durch Dritte, die mit Unternehmensdaten oder -systemen interagiert.

2.2 Sie umfasst ferner jede Partei oder Plattform mit Zugriff auf Unternehmenszugangsdaten, Datenspeicher, Quellcode-Repositories, Staging-Umgebungen oder Produktivsysteme.

3. Ziele

3.1 Sicherstellen, dass jede ausgelagerte Entwicklung die Grundsätze sicherer Programmierung einhält und Entwickler vertraglich zur Einhaltung dokumentierter Standards und von Vertraulichkeitsklauseln verpflichtet werden.

3.2 Eindeutige Eigentumsverhältnisse für alle Liefergegenstände – Code, Assets, Zugangsdaten und Dokumentation – festlegen, einschließlich der vollständigen Übertragung der Rechte auf das Unternehmen und einer nachvollziehbaren Übergabe bei Projektabschluss.

3.3 Häufige Entwicklungsrisiken verhindern, einschließlich der Wiederverwendung proprietären Codes, Angriffen auf die Lieferkette über Bibliotheken, der Nutzung nicht unterstützter Frameworks und nicht geprüfter administrativer Zugriffe.

3.4 Für jedes ausgelagerte Projekt eine Dokumentation vor Beauftragung verlangen, einschließlich Verträgen, Geheimhaltungsvereinbarung (NDA) und Mindestanforderungen an die Sicherheit.

3.5 Kundendaten, Systeme und interne Prozesse schützen, indem eine wirksame Steuerung der Entwicklung, Tests vor der Übergabe und eine sichere Benutzer- und Zugriffsverwaltung durchgesetzt werden.

4. Rollen und Verantwortlichkeiten

4.1 Geschäftsführer (GM)

4.1.1 Genehmigt alle Lieferantenbeziehungen und unterzeichnet Entwicklungsvereinbarungen.

4.1.2 Stellt sicher, dass jede ausgelagerte Entwicklung dieser Richtlinie entspricht.

4.1.3 Entzieht den Zugriff auf Unternehmenssysteme nach Projektabschluss.

4.1.4 Prüft die Dokumentation und Ergebnisse nach der Lieferung.

4.2 Projektverantwortlicher (in der Regel interner Mitarbeiter oder benannter Koordinator)

4.2.1 Steuert die tägliche Koordination mit dem externen Entwickler.

4.2.2 Prüft, ob funktionale Anforderungen erfüllt sind und Liefergegenstände getestet werden.

4.2.3 Stellt die sichere Übergabe von Code und Zugangsdaten sicher.

4.2.4 Meldet entwicklungsbezogene Probleme oder Vorfälle an den GM.

[... 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 mindestens einmal jährlich durch den Geschäftsführer (GM) überprüft werden. Die Überprüfung stellt sicher, dass sie weiterhin Folgendem entspricht:

9.1.1.1 den Anforderungen der Zertifizierung nach ISO/IEC 27001,

9.1.1.2 Änderungen rechtlicher Verpflichtungen (z. B. DSGVO Artikel 28, DORA Artikel 10),

9.1.1.3 aktuellen Entwicklungspraktiken auf SME-Niveau und Risiken durch Dritte.

9.2 Anlassbezogene Überprüfungen

9.2.1 Richtlinienüberprüfungen müssen auch erfolgen, wenn:

9.2.1.1 ein neuer Lieferant oder eine neue Plattform für ausgelagerte Entwicklung aufgenommen wird,

9.2.1.2 ein erheblicher Vorfall im Zusammenhang mit ausgelagerter Entwicklung eintritt,

9.2.1.3 wesentliche Änderungen an den verwendeten Werkzeugen, Plattformen oder Umgebungen vorliegen.

9.3 Überprüfungsprozess

9.3.1 Der GM ist verantwortlich für:

9.3.1.1 die Überprüfung, dass Verträge, Geheimhaltungsvereinbarungen (NDA) und Prozesse der Zugriffskontrolle wirksam bleiben,

9.3.1.2 die Bestätigung, dass aktuelle Lieferanten und Freiberufler die Richtlinie einhalten,

9.3.1.3 die Überarbeitung von Regelungen auf Grundlage von Rückmeldungen aus früheren Projekten oder Vorfällen.

9.4 Versionskontrolle und Kommunikation

9.4.1 Alle Änderungen müssen:

9.4.1.1 mit Datum, Grund und Änderungsbeschreibung erfasst werden,

9.4.1.2 durch den GM genehmigt und in die Versionshistorie aufgenommen werden,

9.4.1.3 an sämtliches Personal oder Projektverantwortliche kommuniziert werden, die mit externen Entwicklern arbeiten,

9.4.1.4 erforderlichenfalls an alle betroffenen Lieferanten und Dritten erneut verteilt werden.

10. Verwandte Richtlinien und Verknüpfungen

10.1 Diese Richtlinie unterstützt unmittelbar die Umsetzung der folgenden auf SMEs ausgerichteten Richtlinien und ist von ihnen abhängig:

10.1.1 P2S – Richtlinie zu Governance-Verantwortlichkeiten: Legt fest, wer bei der Nutzung ausgelagerter Entwickler für Lieferantengenehmigung, Zugriffskontrolle und Risikoakzeptanz verantwortlich ist.

10.1.2 P4S – Richtlinie zur Zugriffskontrolle: Definiert die ordnungsgemäße Einrichtung, Beschränkung und Beendigung von Benutzerkonten und administrativen Zugriffsrechten, die im Rahmen ausgelagerter Entwicklung verwendet werden.

10.1.3 P8S – Richtlinie zur Sensibilisierung und Schulung für Informationssicherheit: Stellt sicher, dass interne Mitarbeitende verstehen, wie sie sicher mit externen Entwicklern zusammenarbeiten, einschließlich des Umgangs mit Zugangsdaten und Projektdateien.

10.1.4 P17S – Richtlinie zu Datenschutz und Privatsphäre: Legt Sicherheitsanforderungen und rechtliche Anforderungen für den Umgang mit personenbezogenen Daten fest, die von ausgelagerten Entwicklern unter der DSGVO verarbeitet werden können.

10.1.5 P24S – Richtlinie zur sicheren Entwicklung: Legt fest, wie interne und externe Entwicklung sichere Programmierpraktiken sowie die Prüfung von Bibliotheken und Frameworks einzuhalten hat.

10.1.6 P30S – Richtlinie für die Reaktion auf Sicherheitsvorfälle: Erforderlich, wenn ausgelagerte Entwicklung zu Informationssicherheitsvorfällen oder Schwachstellen führt, und dient der koordinierten Untersuchung und Mängelbehebung.

10.2 Diese Richtlinien müssen parallel umgesetzt werden, um sicherzustellen, dass ausgelagerte Entwicklung keine ungesteuerten Risiken schafft und keine Compliance-Verpflichtungen von SMEs verletzt.

11. Referenzstandards und Rahmenwerke

11.1 ISO/IEC 27001

11.1.1 Klausel 6.1 – Organisationen müssen Informationssicherheitsrisiken im Zusammenhang mit Lieferanten bewerten und behandeln.

11.1.2 Klausel 8.1 – Verlangt operative Planung und Steuerung, einschließlich Drittleistungen wie ausgelagerter Entwicklung.

11.2 ISO/IEC 27002

11.2.1 Maßnahme 5.19 – Empfiehlt die Bewertung der Fähigkeit von Lieferanten, Anforderungen der Informationssicherheit zu erfüllen.

11.2.2 Maßnahme 5.20 – Empfiehlt die regelmäßige Überwachung und turnusmäßige Überprüfung von Drittleistungen.

11.2.3 Maßnahmen 8.25–8.27 – Beschreiben Praktiken für einen sicheren Systementwicklungslebenszyklus, die auf ausgelagerte Entwicklung anwendbar sind.

11.3 NIST SP 800-53 Rev. 5

11.3.1 SA-4 – Verlangt, dass Beschaffungsstrategien Maßnahmen der Informationssicherheit enthalten.

11.3.2 SA-9 – Behandelt externe Systementwicklung und Risiken in der Lieferkette.

11.3.3 SA-11 – Definiert sichere Entwicklungspraktiken einschließlich Codeprüfungen und Mängelbehebung.

11.3.4 SA-15 – Empfiehlt automatisierte Werkzeuge zur Fehlererkennung und Softwarequalitätssicherung.

11.3.5 SR-3 – Verlangt, dass Lieferantenvereinbarungen Anforderungen an die Cybersicherheit enthalten.

11.4 Datenschutz-Grundverordnung der EU (DSGVO)

11.4.1 Artikel 28 – Verlangt Verträge mit Auftragsverarbeitern, um angemessene Datenschutzmaßnahmen sicherzustellen; dies gilt unmittelbar für Entwickler, die auf personenbezogene Daten zugreifen oder diese verarbeiten.

11.5 EU-NIS2-Richtlinie (2022/2555)

11.5.1 Artikel 21(2)(a), (h) – Verlangt Kontrollen zur Sicherheit der Lieferkette und Praktiken für sichere Softwareentwicklung für digitale Diensteanbieter im Anwendungsbereich, einschließlich SMEs, soweit anwendbar.

11.6 EU Digital Operational Resilience Act (DORA)

11.6.1 Artikel 10 – Verlangt das Management von IKT-Drittparteienrisiken einschließlich Entwicklungsvereinbarungen, Sicherheitsverpflichtungen und Risikokontrollen in Bezug auf Drittanbieter.

11.7 COBIT 2019

11.7.1 BAI03 – Manage Solutions Identification and Build – Stellt sicher, dass externe Entwicklung geschäftliche Anforderungen und Sicherheitserwartungen erfüllt.

11.7.2 DSS05 – Manage Security Services – Verlangt, dass externe Sicherheitsdienste und Entwicklungsanbieter unter durchgesetzten Sicherheitsregeln und Aufsicht tätig sind.