					Fügen Sie hier den Namen der eingetragenen juristischen Person ein							
Dokumentnummer: P24S					Dokumenttitel: **Richtlinie zur sicheren Softwareentwicklung**							
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	Relevante Sicherheitsmaßnahmen für operative Prozesse, einschließlich sicherer Entwicklung
ISO/IEC 27002:2022	Maßnahmen 8.25–8.27	Deckt den sicheren Systementwicklungslebenszyklus, Tests und Sicherheitsverantwortlichkeiten externer Entwickler ab
NIST SP 800-53 Rev.5	SA-3 – SA-15, SI-10	Behandelt den sicheren SDLC, Zugriffskontrolle und Schwachstellenmanagement in der Entwicklung
EU-DSGVO	Artikel 25	Verlangt Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen in der Softwareentwicklung
EU NIS2	Artikel 21(2)(a), (e), (h)	Verlangt Richtlinien für sichere Entwicklung, die Überwachung der Nutzung von Open Source und dokumentierte Minderungsmaßnahmen
EU DORA	Artikel 6(7), 9(1)(c), 10(2)(c)	Sicherheitsanforderungen über den gesamten Lebenszyklus kritischer IKT-Systeme im Finanzsektor
COBIT 2019	BAI	Rahmenwerk für ein strukturiertes, nachvollziehbares und resilientes Management sicherer Entwicklung

1. Zweck

1.1 Diese Richtlinie stellt sicher, dass alle durch die Organisation oder ihre externen Partner entwickelten oder geänderten Softwareprodukte, Skripte und webbasierten Werkzeuge sicher entwickelt werden, um das Risiko von Schwachstellen, unbefugtem Datenzugriff und Betriebsstörungen zu minimieren.

1.2 Sie legt verbindliche Vorgaben für sichere Entwicklung und Programmierpraktiken fest, die von allen internen Entwicklern, Auftragnehmern und Lieferanten unabhängig von Projektgröße oder -komplexität einzuhalten sind.

1.3 Diese Richtlinie dient dem Schutz von Kundendaten, der Vermeidung von Sicherheitsvorfällen und der Sicherstellung, dass durch oder für die Organisation entwickelte oder angepasste Software Sicherheitsprüfungen besteht, rechtliche Anforderungen (z. B. DSGVO, NIS2, DORA) erfüllt und die ISO/IEC-27001-Zertifizierung unterstützt.

2. Geltungsbereich

2.1 Diese Richtlinie gilt für alle Personen und Einheiten, die im Auftrag der Organisation die folgenden Elemente entwickeln, anpassen, bereitstellen oder verwalten:

2.1.1 Websites, Anwendungen oder Automatisierungswerkzeuge

2.1.2 intern entwickelte Skripte oder Software

2.1.3 von externen Entwicklern oder Freiberuflern erstellten Code

2.1.4 Plugins, Bibliotheken und Softwarekomponenten, die in Produktivsysteme integriert werden

2.2 Sie umfasst alle Umgebungen, die für Entwicklungstätigkeiten genutzt werden, einschließlich:

2.2.1 Entwicklungs- und Testumgebungen

2.2.2 Staging- und Vorproduktionsumgebungen

2.2.3 Produktivsysteme, auf denen kundenspezifisch entwickelter Code ausgeführt wird

2.3 Die Richtlinie regelt außerdem den Umgang mit Daten während Entwicklung und Bereitstellung, insbesondere jede Nutzung von Produktionsdaten in Nicht-Produktivumgebungen.

3. Ziele

3.1 Verhinderung der Einführung von Sicherheitsmängeln oder Schwachstellen in individuell entwickelter Software oder in durch Dritte entwickelter Software.

3.2 Sicherstellung, dass sichere Programmierpraktiken und die Vermeidung von Schwachstellen in jede Phase des Softwareentwicklungslebenszyklus integriert sind.

3.3 Reduzierung von Risiken im Zusammenhang mit der Nutzung von Open-Source- oder Drittkomponenten durch verbindliche Prüfung und Nachverfolgung.

3.4 Verpflichtung zu formaler Codeprüfung und Anwendungssicherheitstests vor der Freigabe.

3.5 Kontrolle des Zugriffs auf Entwicklungsumgebungen und Sicherstellung der Trennung von Produktivsystemen.

3.6 Erfüllung verbindlicher Anforderungen aus internationalen Standards und Vorschriften (z. B. ISO/IEC 27001, DSGVO, DORA, NIS2).

4. Rollen und Verantwortlichkeiten

4.1 Geschäftsführung (GM)

4.1.1 genehmigt diese Richtlinie und trägt die Gesamtverantwortung.

4.1.2 stellt sicher, dass sämtliche Softwareentwicklungsaktivitäten, unabhängig davon, ob sie intern oder ausgelagert durchgeführt werden, dieser Richtlinie entsprechen.

4.1.3 prüft und unterzeichnet Entwicklungs- oder Dienstleistungsverträge, die Klauseln zur sicheren Entwicklung enthalten.

4.1.4 überwacht die Einhaltung durch Lieferanten durch regelmäßige Abstimmungen oder durch Anforderung von Nachweisen.

4.2 Interner Entwickler oder Anwendungsverantwortlicher

4.2.1 hält sichere Programmier- und Bereitstellungspraktiken ein.

4.2.2 wendet die Checkliste für sichere Entwicklung auf jedes Projekt an.

4.2.3 prüft die Sicherheit aller verwendeten Open-Source- oder Drittkomponenten.

4.2.4 meldet festgestellte Schwachstellen unverzüglich an die Geschäftsführung.

[... 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 durch die Geschäftsführung mindestens einmal jährlich überprüft werden, um:

9.1.1 die fortlaufende Einhaltung von ISO/IEC 27001, DSGVO, NIS2 und DORA zu verifizieren

9.1.2 aktualisierte Bedrohungen oder Änderungen bewährter Praktiken der sicheren Entwicklung abzubilden

9.1.3 die Kompatibilität mit neuen Werkzeugen, Plattformen oder Lieferantenbeziehungen sicherzustellen

9.2 Außerordentliche Überprüfungen müssen ausgelöst werden durch:

9.2.1 jeden gemeldeten Softwaresicherheitsvorfall

9.2.2 die Einführung eines neuen Entwicklungsframeworks oder einer neuen Hosting-Plattform

9.2.3 eine Änderung bei Entwicklungspartnern von Drittparteien

9.2.4 regulatorische Aktualisierungen, die Software- oder Sicherheitsverpflichtungen betreffen

9.3 Alle Änderungen an dieser Richtlinie müssen:

9.3.1 mit Datum, Änderungszusammenfassung und Genehmigung der Geschäftsführung dokumentiert werden

9.3.2 allen internen und externen an der Entwicklung beteiligten Personen klar kommuniziert werden

9.3.3 als Teil der versionskontrollierten Richtlinienverwaltung und Versionshistorie der Organisation gespeichert werden

9.4 Aktualisierte Versionen müssen leicht zugänglich gemacht werden, entweder über interne Plattformen, gedruckte Dokumentation oder für Lieferanten zugängliche Cloud-Dienste.

10. Verwandte Richtlinien und Verknüpfungen

10.1 Diese Richtlinie unterstützt die wirksame Umsetzung mehrerer weiterer SME-Richtlinien und setzt deren wirksame Umsetzung voraus:

10.1.1 P2S – Richtlinie zu Governance-Rollen und Verantwortlichkeiten: Legt die Rechenschaftspflicht für die Zuweisung und Überprüfung von Sicherheitsmaßnahmen in der Entwicklung über Projekte und Lieferanten hinweg fest.

10.1.2 P4S – Richtlinie zur Zugriffskontrolle: Definiert grundlegende Regeln zur Beschränkung des Zugriffs auf Entwicklungsumgebungen und Code-Repositories, einschließlich Funktionstrennung.

10.1.3 P8S – Richtlinie zur Sensibilisierung und Schulung für Informationssicherheit: Stellt sicher, dass interne Entwickler und Auftragnehmer sichere Programmierpraktiken und damit verbundene Sicherheitsverantwortlichkeiten verstehen.

10.1.4 P17S – Richtlinie zu Datenschutz und Privatsphäre: Erläutert, wie personenbezogene Daten während Entwicklung, Tests und Protokollierungsprozessen verarbeitet werden müssen, um die DSGVO einzuhalten.

10.1.5 P30S – Incident-Response-Richtlinie: Definiert, wie entwicklungsbezogene Informationssicherheitsvorfälle, einschließlich codebezogener Expositionen, gemeldet, bewertet und behoben werden müssen.

10.2 Diese Richtlinien wirken zusammen, um sicherzustellen, dass sichere Entwicklung auch in kleinen oder nicht technischen Organisationen umsetzbar und nachweisbar ist.

11. Referenzstandards und Rahmenwerke

11.1 ISO/IEC 27001

11.1.1 Klausel 8.1 – Verlangt die Umsetzung operativer Kontrollen, einschließlich sicherer Entwicklung, die an Geschäftszielen und Risikoprofil ausgerichtet sind.

11.2 ISO/IEC 27002

11.2.1 Maßnahme 8.25 – Empfiehlt die Integration von Sicherheit über den gesamten Softwarelebenszyklus hinweg, einschließlich Quellcodeverwaltung, Versionierung und Entwicklerzugriff.

11.2.2 Maßnahme 8.26 – Legt Methoden für Anwendungstests und die Überprüfung von Sicherheitsfunktionen vor dem Produktivgang fest.

11.2.3 Maßnahme 8.27 – Verlangt, dass externe Entwickler dieselben Entwicklungsstandards einhalten und ihre Sicherheitsverantwortlichkeiten klar festgelegt sind.

11.3 NIST SP 800-53 Rev.5

11.3.1 SA-3 bis SA-15 – Definieren sichere Entwicklungsprozesse, einschließlich Zugriffskontrolle für Entwickler, Tests, Bedrohungsmodellierung und Dokumentation.

11.3.2 SI-10 – Verlangt, dass Entwickler häufige Softwareschwächen identifizieren und mindern sowie, soweit anwendbar, automatisierte Werkzeuge einsetzen.

11.4 EU-DSGVO (2016/679)

11.4.1 Artikel 25 – „Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen“ verlangt die Integration von Sicherheits- und Datenschutzmaßnahmen während Softwaredesign und -entwicklung, insbesondere bei der Verarbeitung personenbezogener Daten.

11.5 EU NIS2-Richtlinie (2022/2555)

11.5.1 Artikel 21(2)(a), (e) und (h) – Verlangt Richtlinien für sichere Entwicklung, die Überwachung der Nutzung von Open Source und die dokumentierte Minderung anwendungsbezogener Risiken in wesentlichen und wichtigen Einrichtungen.

11.6 EU DORA (2022/2554)

11.6.1 Artikel 6(7), 9(1)(c) und 10(2)(c) – Legen Sicherheitsverpflichtungen über den Entwicklungslebenszyklus für Unternehmen des Finanzsektors, einschließlich KMU, fest, insbesondere für kritische IKT-Systeme.

11.7 COBIT 2019

11.7.1 BAI03 – „Manage Solutions Identification and Build“ unterstützt die Umsetzung strukturierter Entwicklungsmaßnahmen mit Schwerpunkt auf Sicherheit, Nachvollziehbarkeit und Resilienz, zugeschnitten auf die Rahmenbedingungen von KMU.