					Fügen Sie hier den Namen der eingetragenen juristischen Person ein							
Dokumentnummer: P24					Dokumenttitel: **Richtlinie für sichere 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**

1. Zweck

1.1 Diese Richtlinie legt verbindliche Sicherheitsanforderungen für Aktivitäten der Software- und Systementwicklung innerhalb der Organisation fest, einschließlich interner Projekte, ausgelagerter Entwicklung und der Integration von Code Dritter.

1.2 Ziel ist es, sicherzustellen, dass Sicherheit über den gesamten Softwareentwicklungslebenszyklus (SDLC) hinweg verankert ist und dass Schwachstellen vor der Bereitstellung in der Produktivumgebung identifiziert, reduziert und verhindert werden.

1.3 Diese Richtlinie unterstützt die Umsetzung von ISO/IEC 27001:2022, Klausel 8.1, sowie der Maßnahmen 8.25–8 aus Anhang A, indem sie die Governance für sichere Entwicklung, Verfahren zur Codevalidierung und die Überwachung von Entwicklungsleistungen Dritter standardisiert.

2. Geltungsbereich

2.1 Diese Richtlinie gilt für alle:

2.1.1 intern oder extern entwickelten Softwarelösungen, Anwendungen, Skripte, Integrationen und Automatisierungswerkzeuge

2.1.2 Entwicklungsteams, Product Owner, DevOps-Teams, Qualitätssicherung (QA), Architekten, Projektmanager und Auftragnehmer

2.1.3 SDLC-Umgebungen einschließlich Entwicklungs-, Test-, Staging- und Vorproduktionssystemen

2.1.4 Open-Source- und Drittkomponenten, die in interne Anwendungen integriert werden

2.1.5 Software, die On-Premises, in privaten, hybriden oder öffentlichen Cloud-Umgebungen bereitgestellt wird

2.2 Alle Benutzer und Stellen, die im organisatorischen Kontext an Systementwicklung, Tests oder Bereitstellung beteiligt sind, unterliegen dieser Richtlinie, einschließlich Managed Service Providern (MSPs) und Plattformanbietern.

3. Ziele

3.1 Sicherheitskontrollen sind in allen Phasen der Softwareentwicklung von der Konzeption bis zur Bereitstellung zu verankern, sodass die Risikoreduzierung proaktiv und kontinuierlich erfolgt.

3.2 Die Einführung ausnutzbarer Schwachstellen wie Injektionsfehlern, unsicherer Authentifizierung und die Gefährdung durch bekannte Schwachstellen in Drittkomponenten ist zu verhindern.

3.3 Sichere Programmierpraktiken, ausgerichtet an OWASP, SANS CWE und frameworkspezifischen Leitlinien, sind festzulegen und durchzusetzen.

3.4 Es ist sicherzustellen, dass sämtlicher Code vor der Bereitstellung einem Peer-Review, einer automatisierten Analyse und einer Sicherheitsvalidierung unterzogen wird.

3.5 Entwicklungsrisiken aus ausgelagerten Tätigkeiten, der Einbindung von Code Dritter und der Wiederverwendung von Open-Source-Software sind zu steuern.

3.6 Entwicklungs-, Test- und Staging-Umgebungen sind vor unbefugtem Zugriff zu schützen, und die Nutzung von Produktionsdaten ohne genehmigte Maskierung oder Anonymisierung ist zu verhindern.

3.7 Das Sicherheitsbewusstsein von Entwicklern, Produktmanagern und Fachkräften der Qualitätssicherung ist durch rollenbasierte Schulungen und fortlaufende Informationen über neu entstehende Bedrohungen zu stärken.

4. Rollen und Verantwortlichkeiten

4.1 Chief Information Security Officer (CISO)

4.1.1 ist Eigentümer dieser Richtlinie und stellt sicher, dass die Anforderungen an sichere Entwicklung organisationsweit durchgesetzt werden.

4.1.2 genehmigt Standards für sicheres Programmieren und Vereinbarungen zur Entwicklung durch Dritte.

4.1.3 validiert Entscheidungen zur Risikobehandlung für ungelöste oder zurückgestellte Schwachstellen.

4.2 Leiter Anwendungssicherheit / DevSecOps-Manager

4.2.1 entwickelt, pflegt und fördert Leitlinien für sicheres Programmieren.

4.2.2 integriert statische und dynamische Sicherheitstests in CI/CD-Pipelines.

4.2.3 führt Sicherheitsprüfungen des Codes durch und legt verbindliche Maßnahmen zur Mängelbeseitigung fest.

[... 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 jährlich oder bei Bedarf häufiger zu überprüfen, insbesondere als Reaktion auf:

9.1.1 wesentliche Änderungen in Entwicklungsmethoden oder DevOps-Werkzeugen

9.1.2 erhebliche Sicherheitsvorfälle infolge von Anwendungsschwachstellen

9.1.3 Änderungen regulatorischer Anforderungen an sichere Software (z. B. DSGVO, DORA)

9.1.4 neue Industriestandards oder Bedrohungsinformationen (z. B. OWASP Top 10, SLSA, MITRE CWE)

9.2 Die Überprüfung der Richtlinie ist durch den Leiter Anwendungssicherheit in Abstimmung mit dem CISO, Softwarearchitekten, der QA-Leitung und der Rechtsabteilung (bei Auswirkungen von Drittcode) zu leiten.

9.3 Alle Überarbeitungen müssen im Register zur ISMS-Dokumentenlenkung erfasst, versionskontrolliert und den betroffenen Teams über Release Notes oder Pflichtschulungen mitgeteilt werden.

9.4 Frühere Versionen sind zur rechtlichen und auditbezogenen Nachvollziehbarkeit im Archiv-Repository aufzubewahren.

10. Zugehörige Richtlinien und Verknüpfungen

10.1 P1 – Informationssicherheitsrichtlinie. Sie legt den strategischen Auftrag fest, Sicherheit in alle Informationssysteme einzubetten, wobei sichere Entwicklung eine grundlegende operative Kontrolle darstellt.

10.2 P4 – Richtlinie zur Zugriffskontrolle. Sie definiert die Kontrollmaßnahmen zur Beschränkung des Zugriffs auf Entwicklungsumgebungen, Repositories, Build-Werkzeuge und CI/CD-Pipelines.

10.3 P5 – Änderungsmanagement-Richtlinie. Sie stellt sicher, dass Codeänderungen, Releases und Bereitstellungen einer ordnungsgemäßen Genehmigung, Rollback-Planung und Verifikation nach der Bereitstellung unterliegen.

10.4 P12 – Richtlinie zum Asset-Management. Sie unterstützt die Inventarisierung von Entwicklungsumgebungen, Quellcode-Repositories und Build-Systemen als verwaltete Assets, die klassifiziert und geschützt werden müssen.

10.5 P22 – Richtlinie zur Protokollierung und Überwachung. Sie gilt für Entwicklungspipelines und stellt sicher, dass Build-Prozesse, Code-Überführungen und Bereitstellungsereignisse protokolliert, überwacht und auf Sicherheitsanomalien analysiert werden.

10.6 P30 – Incident-Response-Richtlinie (P30). Sie stellt den Rahmen für die Analyse und Reaktion auf Sicherheitsmängel bereit, die nach der Bereitstellung oder während Anwendungssicherheitstests festgestellt werden.

11. Referenzstandards und Rahmenwerke

11.1 ISO/IEC 27001

11.1.1 Klausel 8.1 – Betriebliche Planung und Steuerung: fordert die Integration sicherer Entwicklungsprozesse und Kontrollen in den Betrieb.

11.2 ISO/IEC 27002:2022 – Maßnahmen 8.25–8

11.2.1 Anhang A Maßnahme 8.25 – Sicherer Entwicklungslebenszyklus: fordert die formale Einbindung von Sicherheit in Softwaredesign und -entwicklung.

11.2.2 Anhang A Maßnahme 8.26 – Anforderungen an die Anwendungssicherheit: fordert die Definition sicherer Programmierung und von Sicherheitsabnahmekriterien.

11.2.3 Anhang A Maßnahme 8.27 – Sichere Systemarchitektur und Engineering-Grundsätze: verlangt die Anwendung von Sicherheitsdesignprinzipien und die Minderung bekannter Schwachstellen.

11.3 NIST SP 800-53 Rev. 5

11.3.1 SA-3 bis SA-15: legt strukturierte Praktiken für die Entwicklung sicherer Anwendungen fest, einschließlich Anforderungen an Design, Codeintegrität und Tests.

11.3.2 SI-10 – Validierung von Informationseingaben: adressiert Schutzmaßnahmen für sicheres Programmieren.

11.3.3 SR-3 – Schutz der Lieferkette: fordert die Prüfung von Software Dritter, Komponenten und Entwicklungsdienstleistern.

11.4 EU-DSGVO (2016/679)

11.4.1 Artikel 25 – Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen: schreibt vor, Sicherheit und Datenschutz in die Systementwicklung einzubetten.

11.4.2 Artikel 32 – Sicherheit der Verarbeitung: unterstützt technische Maßnahmen wie Eingabevalidierung, Zugriffskontrollen und sichere Bereitstellung.

11.5 EU NIS2-Richtlinie (2022/2555)

11.5.1 Artikel 21(2)(e–f): fordert Softwareentwicklungspraktiken, die Schwachstellenmanagement, Codesicherheit und Vorfallmeldung umfassen.

11.6 EU DORA (2022/2554)

11.6.1 Artikel 9 – Management von IKT-Risiken: verlangt sichere Entwicklungspraktiken für Finanzunternehmen, einschließlich Kontrollen der Softwarequalität und Mängelbeseitigung.

11.6.2 Artikel 10 – Aufrechterhaltung des Geschäftsbetriebs und Tests: fördert strenge Tests und Validierung von IKT-Systemen, einschließlich Anwendungen.

11.7 COBIT 2019

11.7.1 BAI03 – Manage Solutions Identification and Build: regelt Design, Entwicklung und Sicherheitsintegration in neue Lösungen.

11.7.2 BAI07 – Manage Change Acceptance and Transitioning: stellt sichere Bereitstellung und Bewertung nach der Bereitstellung sicher.

11.7.3 DSS05 – Sicherheitsdienste verwalten: wendet Sicherheitsvalidierung auf Software- und Servicebereitstellung an.