					Fügen Sie hier den Namen der eingetragenen juristischen Person ein							
Dokumentnummer: P25					Dokumenttitel: **Richtlinie zu Anforderungen an die Anwendungssicherheit**							
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	—
ISO/IEC 27002:2022	Maßnahmen 8.25–8.26	—
NIST SP 800-53 Rev.5	SA-11, SA-15, SI-10	—
EU-DSGVO	Artikel 25, 32	—
EU NIS2	Artikel 21(2)(f), 23	—
EU DORA	Artikel 9, 11	—
COBIT 2019	BAI03, BAI09, DSS05	—

1. Zweck

1.1 Diese Richtlinie legt verbindliche Anforderungen an die Anwendungssicherheit für Software fest, die von der Organisation entwickelt, beschafft, integriert oder bereitgestellt wird. Sie stellt sicher, dass alle Anwendungen nach Grundsätzen sicherer Entwicklung, unter Einhaltung regulatorischer Verpflichtungen und im Einklang mit der Risikobereitschaft der Organisation entworfen, umgesetzt und betrieben werden.

1.2 Diese Richtlinie schreibt die Berücksichtigung von Sicherheitsanforderungen über den gesamten Anwendungslebenszyklus hinweg vor und umfasst Benutzerauthentifizierung, Datenverarbeitung, den Schutz von Schnittstellen sowie die sichere Interaktion mit APIs und Diensten.

1.3 Mit Einführung dieser Richtlinie verfolgt die Organisation das Ziel, die Entstehung von Softwareschwachstellen zu verhindern, schützenswerte Daten zu schützen sowie Nachvollziehbarkeit und Resilienz gegenüber Ausnutzung und Missbrauch sicherzustellen.

2. Geltungsbereich

2.1 Diese Richtlinie gilt für:

2.1.1 intern entwickelte oder extern bezogene Anwendungen, einschließlich SaaS und kundenspezifisch entwickelter Werkzeuge

2.1.2 Anwendungen, die kritische Geschäftsprozesse unterstützen, Kundenzugänge bereitstellen oder regulierte Daten verarbeiten

2.1.3 Entwicklungs-, DevOps-, Qualitätssicherungs-, Produkt- und Sicherheitsteams

2.1.4 Drittentwickler, Softwareanbieter und Integrationspartner mit Zugriff auf Anwendungen oder APIs der Organisation

2.2 Sie gilt für alle Umgebungen – Entwicklung, Test, Staging, Produktion und Disaster Recovery – unabhängig davon, ob diese On-Premises, in privaten Rechenzentren oder in öffentlichen Cloud-Umgebungen betrieben werden.

3. Ziele

3.1 Festlegung funktionaler und nichtfunktionaler Sicherheitsanforderungen als Mindeststandard, der von allen Anwendungen unabhängig von Entwicklungsmethode oder Technologie-Stack einzuhalten ist.

3.2 Sicherstellung der Integration von Schutzmaßnahmen auf Anwendungsebene, einschließlich Eingabevalidierung, Ausgabekodierung, Fehlerbehandlung und Sitzungssicherheit.

3.3 Verbindliche sichere Umsetzung von Mechanismen für Authentifizierung, Autorisierung und Zugriffskontrolle im Einklang mit den organisatorischen Richtlinien für Identitäts- und Zugriffsmanagement.

3.4 Verbindliche sichere Interaktion mit APIs, Webschnittstellen und Drittkomponenten unter Verwendung genehmigter Protokolle und Sicherheitskontrollen.

3.5 Ermöglichung der frühzeitigen Erkennung und Minderung von Schwachstellen durch statische und dynamische Analysen, Code-Reviews und Bedrohungsmodellierung.

3.6 Schutz schützenswerter Daten unter Einhaltung regulatorischer Anforderungen durch Durchsetzung von Verschlüsselung, Klassifizierung und Aufbewahrungsanforderungen.

3.7 Sicherstellung der fortlaufenden Validierung des Informationssicherheitsrisikoprofils von Anwendungen nach der Bereitstellung durch Tests, Überwachung und Auditbereitschaft.

4. Rollen und Verantwortlichkeiten

4.1 Chief Information Security Officer (CISO)

4.1.1 Ist Verantwortlicher für diese Richtlinie und stellt deren Ausrichtung an der Informationssicherheitsstrategie und dem Risikoprofil der Organisation sicher.

4.1.2 Genehmigt Anforderungen an die Anwendungssicherheit und setzt verbindliche Kontrollen über Entwicklungs- und Beschaffungsfunktionen hinweg durch.

4.2 Leiter Anwendungssicherheit / DevSecOps-Manager

4.2.1 Definiert Baseline-Konfigurationen für Sicherheitskontrollen und Testmethoden für Anwendungskomponenten.

4.2.2 Überwacht die sichere Integration von Werkzeugen wie SAST, DAST, IAST und SCA in die Softwarebereitstellungspipeline.

4.2.3 Pflegt die Checkliste für Anforderungen an die Anwendungssicherheit sowie die Validierungskriterien.

[... 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 jährlich oder anlassbezogen häufiger überprüft werden als Reaktion auf:

9.1.1 Bekanntmachungen kritischer Schwachstellen, die gängige Frameworks oder Abhängigkeiten betreffen

9.1.2 Aktualisierungen regulatorischer Verpflichtungen zur Anwendungssicherheit, z. B. NIS2 oder DORA

9.1.3 wesentliche Änderungen der Softwareentwicklungspraktiken, Werkzeuge oder Cloud-Architektur der Organisation

9.1.4 Feststellungen aus internen Audits oder externen Penetrationstests

9.2 Die Überprüfung ist durch den Leiter Anwendungssicherheit in Abstimmung mit dem CISO, DevOps Engineering, der Rechtsabteilung, dem Einkauf und den Leitern der Qualitätssicherung zu führen.

9.3 Alle Überarbeitungen müssen versionskontrolliert im Register zur ISMS-Dokumentenlenkung geführt und an alle betroffenen Entwicklungs- und Produktteams verteilt werden.

9.4 Ersetzte Versionen müssen für mindestens drei Jahre archiviert werden, um Nachvollziehbarkeit, Auditierbarkeit und die Unterstützung von Untersuchungen zu Sicherheitsvorfällen sicherzustellen.

10. Verwandte Richtlinien und Verknüpfungen

10.1 P1 – Informationssicherheitsrichtlinie. Legt die Grundlage für den Schutz von Systemen und Daten fest, in deren Rahmen Kontrollen auf Anwendungsebene erforderlich sind, um unbefugten Zugriff, Datenabfluss und Ausnutzung zu verhindern.

10.2 P4 – Richtlinie zur Zugriffskontrolle. Definiert die Standards für Identitäts- und Sitzungsmanagement, die von allen Anwendungen durchgesetzt werden müssen, einschließlich starker Authentifizierung, Prinzip der minimalen Rechtevergabe und Anforderungen an die Zugriffsüberprüfung.

10.3 P5 – Änderungsmanagement-Richtlinie. Regelt die Überführung von Anwendungscode und Konfigurationen in Produktivumgebungen und stellt sicher, dass nicht autorisierte oder nicht getestete Änderungen blockiert werden.

10.4 P17 – Richtlinie zu Datenschutz und Privatsphäre. Verlangt von Anwendungen die Umsetzung von Datenschutz durch Technikgestaltung und die Sicherstellung eines rechtmäßigen Umgangs, der Verschlüsselung und der Aufbewahrung personenbezogener und schützenswerter Daten in allen Umgebungen.

10.5 P24 – Richtlinie zur sicheren Entwicklung. Stellt das übergreifende Rahmenwerk für die Verankerung von Sicherheit im Systementwicklungslebenszyklus bereit; diese Richtlinie definiert die konkreten Anforderungen und technischen Maßnahmen, die auf Anwendungsebene umzusetzen sind.

10.6 P30 – Incident-Response-Richtlinie (P30). Schreibt einen strukturierten Umgang mit Informationssicherheitsvorfällen im Zusammenhang mit Anwendungen vor, einschließlich Schwachstellen, die nach der Bereitstellung oder während von Penetrationstests identifiziert werden, und beschreibt Verfahren für Eskalation, Eindämmung und Wiederherstellung.

11. Referenzstandards und Rahmenwerke

11.1 ISO/IEC 27001:2022

11.1.1 Klausel 8.1 – Betriebliche Planung und Steuerung: Verlangt, dass Anwendungssicherheit in Prozesse und Systeme integriert wird, um Vertraulichkeit, Integrität und Verfügbarkeit (CIA) sicherzustellen.

11.2 ISO/IEC 27002:2022

11.2.1 Maßnahmen 8.25–8.26: Beschreiben die Erwartungen an die Sicherheit auf Anwendungsebene, einschließlich sicherer Programmierpraktiken, Bedrohungsmodellierung, Architekturkontrollen und Validierung von Drittsoftware.

11.2.2 Anhang A, Maßnahme 8.25 – Sicherer Entwicklungslebenszyklus: Schreibt die Integration von Sicherheit über den gesamten Anwendungslebenszyklus hinweg vor.

11.2.3 Anhang A, Maßnahme 8.26 – Anforderungen an die Anwendungssicherheit: Schreibt die Definition und Durchsetzung technischer Maßnahmen zum Schutz von Anwendungen vor Missbrauch und Kompromittierung vor.

11.3 NIST SP 800-53 Rev.5

11.3.1 SA-11 – Sicherheitstests und -bewertung durch Entwickler: Schreibt statische, dynamische und Penetrationstests während der Entwicklung vor.

11.3.2 SA-15 – Entwicklungsprozess, Standards und Werkzeuge: Legt formale Standards für die sichere Anwendungsentwicklung fest.

11.3.3 SI-10 – Validierung von Informationseingaben: Verlangt Kontrollmechanismen zur Verhinderung von Injektions- und Parsing-Angriffen.

11.4 EU-DSGVO (2016/679)

11.4.1 Artikel 25 – Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen: Verlangt die Integration von Datenschutz und Privatsphäre in Anwendungslogik und Workflows.

11.4.2 Artikel 32 – Sicherheit der Verarbeitung: Schreibt geeignete technische Maßnahmen vor, wie Eingabevalidierung, Verschlüsselung und sichere Zugriffskontrollen.

11.5 EU NIS2-Richtlinie (2022/2555)

11.5.1 Artikel 21(2)(f): Verlangt den Umgang mit Schwachstellen und sichere Praktiken für den Anwendungslebenszyklus bei wesentlichen und wichtigen Einrichtungen.

11.5.2 Artikel 23 – Meldung von Sicherheitsvorfällen: Erfordert Protokollierungs- und Überwachungsfähigkeiten auf Anwendungsebene, um erhebliche Vorfälle zu erkennen und zu melden.

11.6 EU DORA (2022/2554)

11.6.1 Artikel 9 – Management von IKT-Risiken: Verpflichtet Finanzunternehmen sicherzustellen, dass Anwendungen sicher, getestet und resilient gegenüber Cyberbedrohungen sind.

11.6.2 Artikel 11 – Prüfung von IKT-Werkzeugen: Fördert regelmäßige Penetrationstests und Red-Team-Übungen für kritische Anwendungen und Dienste.

11.7 COBIT 2019

11.7.1 BAI03 – Manage Solutions Identification and Build: Legt Anforderungen an Design und Kontrollen während der Anwendungsentwicklung fest.

11.7.2 BAI09 – Manage Applications: Betont die sichere Wartung, Überwachung und Weiterentwicklung von Produktivsystemen.

11.7.3 DSS05 – Sicherheitsdienste verwalten: Verknüpft den Schutz von Anwendungen mit den übergeordneten Sicherheitsabläufen und Kontrollen der Organisation.