					Fügen Sie hier den Namen der eingetragenen juristischen Person ein							
Dokumentnummer: P25S					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	Operative Kontrollen, einschließlich Anwendungssicherheit
ISO/IEC 27002:2022	Maßnahmen 8.25–8.26	Sichere Konzeption, Entwicklung, Tests und Code-Review
NIST SP 800-53 Rev. 5	SA-11, SI-10	Entwickler- und Anwendungstests, Codeanalyse, Vermeidung von Softwarefehlern
EU-DSGVO	Artikel 25	Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen
EU-NIS2	Artikel 21(2)(a), (e)	Technische Maßnahmen zur Absicherung von Anwendungen und zur Erkennung von Risiken
EU-DORA	Artikel 9(2)(c), 10(2)(c)	Anwendungssicherheit zur Gewährleistung digitaler operationaler Resilienz
COBIT 2019	BAI03	Sichere Entwicklung bzw. Beschaffung von Software steuern

1. Zweck

1.1 Diese Richtlinie legt die verbindlichen Mindestanforderungen an Kontrollen der Anwendungssicherheit fest, die für alle von der Organisation genutzten Software- und Systemlösungen gelten, unabhängig davon, ob diese intern entwickelt oder von externen Lieferanten beschafft werden.

1.2 Sie stellt sicher, dass Anwendungen so konzipiert, implementiert und betrieben werden, dass Kunden-, Mitarbeiter- und Geschäftsdaten vor unbefugtem Zugriff, Missbrauch, Veränderung oder Zerstörung geschützt sind.

1.3 Diese Richtlinie unterstützt die Organisation dabei, die Zertifizierung nach ISO/IEC 27001 zu erreichen und aufrechtzuerhalten, Verpflichtungen aus DSGVO und NIS2 zu erfüllen und operationelle Risiken im Zusammenhang mit unsicheren Softwarebereitstellungen zu reduzieren.

1.4 Sie trägt dazu bei, einen konsistenten und auditierbaren Ansatz für die Anwendungssicherheit in KMU zu schaffen, indem eine einheitliche Checkliste von Sicherheitsmerkmalen und Praktiken festgelegt wird, die an Umgebungen mit begrenzten internen technischen Ressourcen angepasst ist.

2. Geltungsbereich

2.1 Diese Richtlinie gilt für alle Anwendungen, Systeme, Werkzeuge und Plattformen, die:

2.1.1 intern entwickelt, angepasst oder für die interne Nutzung skriptbasiert erstellt werden

2.1.2 als kommerzielle Software, SaaS oder cloudbasierte Systeme beschafft werden

2.1.3 personenbezogene Daten, Geschäftsunterlagen oder sensible betriebliche Informationen verarbeiten, speichern oder übertragen

2.1.4 von Mitarbeitern, Auftragnehmern, Kunden oder Partnern über interne Netzwerke, das Internet oder mobile Plattformen genutzt werden

2.2 Diese Richtlinie gilt für:

2.2.1 Entwickler (intern oder beauftragt)

2.2.2 Softwarelieferanten und Cloud-Service-Provider

2.2.3 IT-Support-Personal oder Administratoren, die für Bereitstellung und Support verantwortlich sind

2.2.4 Anwendungsverantwortliche und Fachanwender, die an Systemfreigabe und Überwachung beteiligt sind

3. Ziele

3.1 Sicherzustellen, dass alle von der Organisation genutzten Anwendungen integrierte und nachprüfbare Sicherheitskontrollen enthalten, die gängige Softwareschwachstellen mindern.

3.2 Die Vertraulichkeit, Integrität und Verfügbarkeit (CIA) der von Anwendungen verarbeiteten Daten zu schützen, unabhängig davon, wo diese gehostet werden.

3.3 Formale Tests, Überprüfungen und Validierungen der Anwendungssicherheit zu verlangen, bevor eine neue Anwendung oder eine wesentliche Aktualisierung für den Produktivbetrieb freigegeben wird.

3.4 Einen konsistenten und sicheren Umgang mit Benutzerkennungen, Sitzungsdaten und Zugriffsrechten über alle unternehmenskritischen Systeme hinweg zu gewährleisten.

3.5 Sichere Protokollierungs-, Auditierbarkeits- und Monitoring-Funktionen in allen Anwendungen zu verlangen, um die Erkennung verdächtiger Aktivitäten und die Reaktion darauf zu unterstützen.

3.6 Rechtliche und Compliance-Risiken zu verringern, indem sichergestellt wird, dass Anwendungen die anwendbaren regulatorischen Sicherheitsanforderungen erfüllen.

4. Rollen und Verantwortlichkeiten

4.1 Geschäftsführung (GM)

4.1.1 Trägt die Gesamtverantwortung für die Anwendungssicherheit in der gesamten Organisation.

4.1.2 Genehmigt diese Richtlinie und stellt sicher, dass alle Beschaffungs- und Entwicklungsprojekte diese einhalten.

4.1.3 Stellt sicher, dass Lieferanten und Dienstleister vertraglich an die Anforderungen der Anwendungssicherheit gebunden sind.

4.1.4 Prüft und genehmigt Ausnahmen im Rahmen der Risikoakzeptanz, wenn die vollständige Einhaltung aufgrund geschäftlicher Einschränkungen nicht erreicht werden kann.

4.2 Anwendungsverantwortlicher (sofern benannt)

4.2.1 Identifiziert anwendungsspezifische Sicherheitsanforderungen bei der Systemauswahl oder Projektinitiierung.

4.2.2 Prüft, ob wesentliche Funktionen wie Anmeldeschutz, Verschlüsselung und Aktivitätsprotokollierung vorhanden sind.

4.2.3 Nimmt an Prüfungen vor der Bereitstellung teil und bestätigt, dass die Sicherheitskontrollen den geschäftlichen Anforderungen entsprechen.

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

9.1.1 Änderungen regulatorischer Anforderungen (z. B. DSGVO, NIS2, DORA) zu berücksichtigen

9.1.2 neue oder aufkommende Bedrohungen und Angriffstechniken einzubeziehen

9.1.3 Formulierungen und Anforderungen an Änderungen bei Plattformen, Lieferanten oder Entwicklungsmethoden anzupassen

9.2 Zusätzlich müssen anlassbezogene Überprüfungen durchgeführt werden, wenn:

9.2.1 neue Anwendungen eingeführt werden

9.2.2 bestehende Anwendungen wesentliche Aktualisierungen oder Integrationen durchlaufen

9.2.3 ein anwendungsbezogener Vorfall oder eine Sicherheitsverletzung eintritt

9.2.4 neue Risiken aus externen Hinweisen oder Branchenwarnungen identifiziert werden

9.3 Alle Aktualisierungen dieser Richtlinie müssen:

9.3.1 von der Geschäftsführung genehmigt werden

9.3.2 mit Versionshistorie und Änderungsgrund dokumentiert werden

9.3.3 an alle Mitarbeiter, Entwickler und Lieferanten kommuniziert werden, die an der Anwendungsverwaltung beteiligt sind

9.3.4 sicher gespeichert werden, damit sie für Audit- und Compliance-Zwecke verfügbar sind

10. Verwandte Richtlinien und Verknüpfungen

10.1 Diese Richtlinie wird unmittelbar durch die folgenden an KMU ausgerichteten Sicherheitsrichtlinien unterstützt und trägt zu deren Durchsetzung bei:

10.1.1 P2S – Richtlinie zu Governance-Rollen und Verantwortlichkeiten: Weist Verantwortung für die Genehmigung von Anwendungen, die Durchsetzung der Richtlinie und die Steuerung von Lieferanten zu.

10.1.2 P4S – Richtlinie zur Zugriffskontrolle: Stellt sicher, dass der Zugriff auf Anwendungen den Grundsätzen der minimalen Rechtevergabe und Sitzungssteuerung entspricht.

10.1.3 P8S – Richtlinie zur Sensibilisierung und Schulung für Informationssicherheit: Stellt sicher, dass Benutzer und Entwickler für die Erkennung und Meldung anwendungsbezogener Bedrohungen geschult werden.

10.1.4 P17S – Richtlinie zu Datenschutz und Privatsphäre: Legt Datenschutzmaßnahmen fest, die durch jede Anwendung durchzusetzen sind, die personenbezogene Daten verarbeitet.

10.1.5 P14S – Richtlinie zur Datenaufbewahrung und Entsorgung: Regelt, wie von Anwendungen erzeugte Protokolle, Backups und sensible Daten aufzubewahren, zu archivieren und sicher zu vernichten sind.

10.1.6 P30S – Incident-Response-Richtlinie: Beschreibt die Schritte zur Identifizierung, Meldung und Eindämmung anwendungsbezogener Sicherheitsereignisse.

10.2 Zusammen stellen diese Richtlinien sicher, dass die Anwendungssicherheit vollständig in das Informationssicherheitsmanagementsystem (ISMS) der Organisation integriert und auditbereit ist.

11. Referenzstandards und Rahmenwerke

11.1 ISO/IEC 27001

11.1.1 Klausel 8.1 – Verlangt von Organisationen die Festlegung operativer Kontrollen zur Behandlung von Informationssicherheitsrisiken, einschließlich solcher im Zusammenhang mit Anwendungen und Softwaresystemen.

11.2 ISO/IEC 27002

11.2.1 Maßnahme 8.25 – Empfiehlt die Umsetzung sicherer Praktiken für Konzeption, Entwicklung und Code-Review in allen Anwendungen, einschließlich der von Lieferanten bereitgestellten Anwendungen.

11.2.2 Maßnahme 8.26 – Empfiehlt formale Tests von Kontrollen zur Anwendungssicherheit, insbesondere in Bereichen wie Zugriffskontrolle, Eingabevalidierung und Sitzungsverarbeitung.

11.3 NIST SP 800-53 Rev. 5

11.3.1 SA-11 – Legt Anforderungen für Entwicklertests, Codeanalyse und dynamische Anwendungsscans vor der Bereitstellung fest.

11.3.2 SI-10 – Behandelt die Erkennung und Vermeidung gängiger Softwarefehler und betont das Sicherheitsbewusstsein von Entwicklern sowie technische Schutzmaßnahmen.

11.4 EU-DSGVO (2016/679)

11.4.1 Artikel 25 – „Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen“ verlangt, Datenschutz und Sicherheit in die grundlegende Konzeption von Anwendungen einzubetten, die personenbezogene Daten verarbeiten.

11.5 EU-NIS2-Richtlinie (2022/2555)

11.5.1 Artikel 21(2)(a) und (e) – Verlangt von wesentlichen und wichtigen Einrichtungen die Umsetzung technischer Maßnahmen zur Absicherung von Anwendungen und zur Erkennung softwarebezogener Risiken.

11.6 EU-DORA (2022/2554)

11.6.1 Artikel 9(2)(c), 10(2)(c) – Verlangt von KMU im Finanzsektor, Sicherheitskontrollen auf Anwendungsebene einzubetten und regelmäßige Bewertungen durchzuführen, um die digitale operationale Resilienz aufrechtzuerhalten.

11.7 COBIT 2019

11.7.1 BAI03 – „Manage Solutions Identification and Build“ gibt Leitlinien für die Entwicklung oder Beschaffung sicherer Software, die an Risiko-, Compliance- und Geschäftsanforderungen ausgerichtet ist – auch in ressourcenbegrenzten KMU-Umgebungen.