					Fügen Sie hier den Namen der eingetragenen juristischen Person ein							
Dokumentnummer: P19S					Dokumenttitel: **Richtlinie zum Schwachstellen- und Patch-Management**							
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**

An Normen und Vorschriften ausgerichtet

Standard/Vorschrift	Klausel/Artikel	Kommentar
ISO/IEC 27001:2022	Klausel 8	
ISO/IEC 27002:2022	Maßnahmen 8.8, 8.9	
NIST SP 800-53 Rev.5	RA-5, SI-2, CM-2	
EU NIS2	Artikel 21(2)(d), 21(2)(e)	
EU DORA	Artikel 8(1), 10(2)	
COBIT 2019	DSS05.02, APO12	
EU DSGVO	Artikel 32(1)(b)	

1. Zweck

1.1 Diese Richtlinie legt fest, wie die Organisation Schwachstellen in Systemen, Anwendungen und Infrastrukturen identifiziert, bewertet und behandelt.

1.2 Zweck dieser Richtlinie ist die Reduzierung von Cybersicherheitsrisiken durch die verbindliche zeitnahe Einspielung von Patches und risikobasierte Verfahren zur Schwachstellenbehebung, die für kleine und mittlere Unternehmen (KMU) geeignet sind.

1.3 Diese Richtlinie unterstützt die Einhaltung der Anforderungen für eine Zertifizierung nach ISO/IEC 27001:2022 und trägt zur Erfüllung regulatorischer Verpflichtungen nach DSGVO, NIS2 und DORA bei, indem sie das proaktive Management technischer Schwachstellen verbindlich vorgibt.

1.4 Die Organisation erkennt an, dass ungepatchte Systeme eine erhebliche Bedrohung für die Informationssicherheit darstellen und systematisch sowie unverzüglich behandelt werden müssen.

2. Geltungsbereich

2.1 Diese Richtlinie gilt für:

2.1.1 alle von der Organisation genutzten Server, Arbeitsplatzsysteme, Laptops, mobilen Endgeräte, Netzwerkkomponenten und cloudbasierten Plattformen

2.1.2 alle in den Geschäftsprozessen eingesetzten Betriebssysteme, Drittanbietersoftware, Plugins und Anwendungen

2.1.3 internes IT-Personal oder externe Dienstleister, die für Systemwartung, Aktualisierungen oder Überwachung verantwortlich sind

2.1.4 jeglichen kundenspezifisch entwickelten Code oder eingebettete Software, die von der Organisation oder in ihrem Auftrag gepflegt wird

2.2 Die Richtlinie umfasst sowohl Infrastrukturen, die direkt von der Organisation verwaltet werden, als auch Systeme, die von vertraglich gebundenen Lieferanten oder Hosting-Anbietern administriert werden.

3. Ziele

3.1 Bekannte Schwachstellen in allen IT-Assets sind zeitnah und konsistent zu identifizieren und zu bewerten.

3.2 Patches und Softwareaktualisierungen sind auf Grundlage von Schweregrad und Risiko für den Geschäftsbetrieb der Organisation oder für personenbezogene Daten einzuspielen.

3.3 Die Ausnutzung technischer Schwachstellen, die zu Serviceausfällen, Datenschutzverletzungen oder regulatorischer Nichteinhaltung führen könnte, ist zu verhindern.

3.4 Zur Sicherstellung der Auditbereitschaft sind genaue Aufzeichnungen über eingespielte Patches, offene Sachverhalte und Ausnahmen zu führen.

3.5 Es sind Werkzeuge und Prozesse einzusetzen, die der Größe und betrieblichen Komplexität der Organisation entsprechen, ohne die Wirksamkeit zu beeinträchtigen.

3.6 Die Einhaltung gesetzlicher und regulatorischer Anforderungen, einschließlich DSGVO Artikel 32 und ISO Anhang A Maßnahme 8, ist zu unterstützen.

4. Rollen und Verantwortlichkeiten

4.1 Geschäftsführung

4.1.1 Trägt die Gesamtverantwortung dafür, dass Aktivitäten zum Patch-Management und Schwachstellenmanagement verbindlich umgesetzt werden.

4.1.2 Genehmigt Risikoausnahmen, wenn Patches nicht eingespielt werden können, und überprüft die zugehörigen Minderungsmaßnahmen.

4.1.3 Prüft Berichte zum Patch-Status und stellt sicher, dass ausreichende Ressourcen zur Erfüllung der Patch-Anforderungen verfügbar sind.

4.2 IT-Support-Dienstleister / interner IT-Administrator

4.2.1 Überwacht Systeme auf Schwachstellen und verfügbare Patches anhand von Herstellerwarnmeldungen, Bedrohungsinformationen und Benachrichtigungen des Betriebssystems.

4.2.2 Spielt Aktualisierungen für Betriebssysteme, Firmware und Anwendungen innerhalb der festgelegten Fristen ein.

4.2.3 Führt ein formales Patch-Protokoll und dokumentiert ungelöste oder zurückgestellte Aktualisierungen.

4.2.4 Führt Tests durch und plant kritische Aktualisierungen so ein, dass betriebliche Beeinträchtigungen minimiert werden.

[... 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 die Geschäftsführung unter Einbeziehung des IT-Support-Dienstleisters und des Datenschutzkoordinators überprüft werden.

9.2 Auslöser für Überprüfungen

9.2.1 Zwischenzeitliche Überprüfungen müssen erfolgen, wenn:

9.2.1.1 eine wesentliche Schwachstelle oder ein Exploit Systeme im Geltungsbereich betrifft

9.2.1.2 signifikante Änderungen an Systemen oder Software eintreten

9.2.1.3 ein Audit Lücken in den Patch-Management-Prozessen feststellt

9.2.1.4 ein patchbezogener Vorfall oder eine Sicherheitsverletzung erfasst wird

9.3 Versionskontrolle der Richtlinie

9.3.1 Alle Aktualisierungen müssen in einem Versionsprotokoll mit Zusammenfassung der Änderungen dokumentiert werden.

9.3.2 Änderungen müssen den betroffenen Mitarbeitenden mitgeteilt werden.

9.3.3 Veraltete Versionen müssen mit eingeschränktem Zugriff archiviert werden.

10. Verwandte Richtlinien und Verknüpfungen

10.1 Diese Richtlinie unterstützt mehrere andere SME-Richtlinien und ist von ihnen abhängig:

10.1.1 P12S – Richtlinie zum Asset-Management: Identifiziert Systemverantwortung und Klassifizierung und stellt sicher, dass alle patchpflichtigen Assets erfasst und inventarisiert sind.

10.1.2 P14S – Richtlinie zur Datenaufbewahrung und Entsorgung: Stellt sicher, dass zur Außerbetriebnahme vorgesehene Systeme sicher aktualisiert oder gelöscht werden, wodurch die Exposition gegenüber Schwachstellen reduziert wird.

10.1.3 P17S – Richtlinie zu Datenschutz und Privatsphäre: Priorisiert die Behebung von Schwachstellen in Systemen, die personenbezogene Daten verarbeiten, um Datenschutzgesetze einzuhalten.

10.1.4 P22S – Richtlinie zur Protokollierung und Überwachung: Unterstützt die Erkennung ungepatchter Systeme oder verdächtiger Verhaltensweisen, die auf die Ausnutzung einer Schwachstelle hindeuten können.

10.1.5 P30S – Incident-Response-Richtlinie: Definiert Verfahren zur Reaktion auf Schwachstellen, die zu Informationssicherheitsvorfällen führen, einschließlich Eskalations- und Meldeschritten.

11. Referenznormen und Rahmenwerke

11.1 ISO/IEC 27001

11.1.1 Klausel 8.1 – Verlangt die Umsetzung von Maßnahmen zur Behandlung betrieblicher Risiken, einschließlich des Schwachstellenmanagements.

11.2 ISO/IEC 27002

11.2.1 Maßnahme 8.8 – Legt Prozesse für das Scannen und Beheben bekannter Schwachstellen in Systemen fest.

11.2.2 Maßnahme 8.9 – Betont sichere Konfiguration, Patch-Validierung und Änderungssteuerung, um neue Expositionen während Aktualisierungen zu vermeiden.

11.3 NIST SP 800-53 Rev.5

11.3.1 RA-5 – Verlangt die Identifizierung von Schwachstellen und deren Behebung innerhalb festgelegter Fristen.

11.3.2 SI-2 – Schreibt die zeitnahe Einspielung von Patches und Aktualisierungen auf Grundlage des Schweregrads vor.

11.3.3 CM-2 – Regelt Baseline-Konfigurationen von Systemen und die Dokumentation von Aktualisierungen, um konsistente Schutzmaßnahmen sicherzustellen.

11.4 EU DSGVO

11.4.1 Artikel 32(1)(b) – Verlangt von Organisationen die Umsetzung geeigneter technischer Maßnahmen, einschließlich des Patch-Managements, um die Sicherheit der Verarbeitung zu gewährleisten.

11.5 EU NIS2-Richtlinie

11.5.1 Artikel 21(2)(d) – Verlangt die Behandlung von Schwachstellen durch systematische Scans und Behebungsmaßnahmen.

11.5.2 Artikel 21(2)(e) – Verpflichtet zu sicherer Konfiguration und Patch-Management zur Sicherstellung der IKT-Resilienz.

11.6 EU DORA

11.6.1 Artikel 8(1) – Verlangt die Erkennung und Minderung von IKT-Risiken, einschließlich technischer Schwachstellen.

11.6.2 Artikel 10(2) – Verlangt von Finanzunternehmen die Behebung von Schwachstellen, die IKT-Systeme und den IKT-Betrieb betreffen.

11.7 COBIT 2019

11.7.1 DSS05.02 – Verlangt die Behandlung bekannter technischer Schwachstellen zur Aufrechterhaltung eines sicheren Betriebs.

11.7.2 APO12.01 – Richtet das Risikomanagement auf die proaktive Überwachung und Korrektur von Systemschwachstellen aus.