					Fügen Sie hier den Namen der eingetragenen juristischen Person ein							
Dokumentnummer: P19					Dokumenttitel: **Richtlinie für 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**

Ausgerichtet an Standards und regulatorischen Anforderungen

Standard/Regelwerk	Klausel/Artikel	Kommentar
ISO/IEC 27001:2022	Abschnitt 8	Systematische Behandlung technischer Schwachstellen; fortlaufende Wirksamkeit von Sicherheitskontrollen.
ISO/IEC 27002:2022	Maßnahmen 8.8, 8.9, 5	Umsetzungsleitlinien für Patch-Management, Schwachstellenscans, Softwareintegrität, sichere Konfiguration und Asset-Inventare.
NIST SP 800-53 Rev. 5	RA-5, SI-2, CM-2, CM-6	Regelmäßige Scans, Mängelbehebung und Konfigurationsmanagement werden durchgesetzt.
EU-DSGVO	Artikel 32, Erwägungsgrund 49	Technische Maßnahmen für zeitnahes Patchen, Schwachstellenbehandlung und Aufrechterhaltung der Sicherheit.
EU-NIS2	Artikel 21(2)(d)	Erkennung, Reaktion und Eindämmung von Schwachstellen zur Gewährleistung eines hohen Maßes an Cyberhygiene.
EU-DORA	Artikel 8, 10(2)(f)	Rechtzeitige Behebung von IKT-Schwachstellen; kontinuierliche, bedrohungsgeleitete Bewertungen.
COBIT 2019	DSS05.02, DSS01.03, MEA	Scannen, Nachverfolgung und Eindämmung technischer Schwachstellen; Überwachung auf Ausnutzung; Prüfung der Wirksamkeit einschließlich Patch-Status.

1. Zweck

1.1 Diese Richtlinie legt die verbindlichen Anforderungen der Organisation für die Identifizierung, Klassifizierung, Behebung und Überwachung technischer Schwachstellen und Softwarefehler in allen Informationssystemen und Assets innerhalb des ISMS-Geltungsbereichs fest.

1.2 Sie stellt sicher, dass alle bekannten Schwachstellen risikobasiert und zeitnah durch koordiniertes Patch-Management, Konfigurationsanpassungen oder kompensierende Kontrollen bewertet und behandelt werden, im Einklang mit geschäftlichen Erfordernissen und Compliance-Verpflichtungen.

1.3 Diese Richtlinie unterstützt die Einhaltung von ISO/IEC 27001 Anhang A Maßnahme 8.8 sowie der Leitlinien aus ISO/IEC 27002 und adressiert regulatorische Anforderungen aus DORA Artikel 8, NIS2 Artikel 21, DSGVO Artikel 32 sowie den Domänen DSS und APO von COBIT 2019.

2. Geltungsbereich

2.1 Diese Richtlinie gilt für alle Informationssysteme, Assets und Umgebungen, die Daten speichern, verarbeiten oder übertragen und der ISMS-Governance unterliegen, einschließlich:

2.1.1 Betriebssysteme, Anwendungen, Netzwerkkomponenten, Firmware, Cloud-Plattformen, APIs und Software von Drittanbietern.

2.1.2 Systeme in Entwicklungs-, Test-, Produktions-, Backup- und Disaster-Recovery-Umgebungen.

2.1.3 Endgeräte, Server, IoT-Geräte, Virtualisierungsinfrastrukturen und Container.

2.2 Sie ist verbindlich für:

2.2.1 Internes Personal: IT-Administratoren, Systemingenieure, Anwendungsentwickler, Sicherheitsanalysten und Infrastrukturteams.

2.2.2 Externe Parteien: Auftragnehmer, Managed Service Provider (MSPs), Softwarehersteller und Systemintegratoren mit technischer Verantwortung für Assets im Geltungsbereich.

2.3 Die Richtlinie umfasst den vollständigen Lebenszyklus des Schwachstellen- und Patch-Managements, einschließlich:

2.3.1 Scans und Erkennung

2.3.2 Risikoklassifizierung und Priorisierung

2.3.3 Beschaffung, Test, Bereitstellung und Rollback von Patches

2.3.4 Behandlung von Ausnahmen und Planung kompensierender Kontrollen

2.3.5 Protokollierung, Berichterstattung und Auditierbarkeit

3. Ziele

3.1 Sicherstellen, dass alle bekannten Schwachstellen so identifiziert, bewertet und behoben werden, dass die Risikoexposition minimiert wird und die operativen Prioritäten gewahrt bleiben.

3.2 Einheitliche, unternehmensweite Prozesse für Schwachstellenscans, Schweregradklassifizierung (z. B. CVSS) und Patch-Management festlegen, einschließlich Notfallbehandlung und Rollback-Planung.

3.3 Ein sicheres Konfigurationsmanagement durch Abstimmung mit Härtungs-Baselines, Änderungsmanagement-Praktiken und Bedrohungsinformationen in Echtzeit ermöglichen.

3.4 Messbare Einhaltung regulatorischer und normativer Kontrollen im Zusammenhang mit Systemintegrität, Patch-Hygiene und zeitnaher Mängelbehebung sicherstellen.

3.5 Verantwortung und Rechenschaftspflicht über alle Rollen hinweg für den vollständigen Lebenszyklus des Schwachstellenmanagements festlegen, damit alle relevanten Stellen innerhalb definierter SLAs handeln und berichtspflichtige Kontrollkennzahlen melden.

3.6 Auditbereitschaft stärken und die Resilienz gegenüber neu entstehenden Bedrohungen verbessern, einschließlich Zero-Day-Schwachstellen, aktiven Exploit-Ketten und sicherheitsrelevanten Herstellerveröffentlichungen.

4. Rollen und Verantwortlichkeiten

4.1 Chief Information Security Officer (CISO)

4.1.1 Trägt die Gesamtverantwortung für diese Richtlinie und stellt ihre Integration in das ISMS sicher.

4.1.2 Definiert das unternehmensweite Risikoprofil und stellt die Ausrichtung an regulatorischen Anforderungen und Kontrollerwartungen sicher.

4.2 Leiter Schwachstellenmanagement / Leiter Security Operations

4.2.1 Überwacht den End-to-End-Betrieb des Schwachstellen- und Patch-Managements.

4.2.2 Koordiniert Scan-Zeitpläne, Priorisierungsmodelle und Fristen für die Behebung.

4.2.3 Pflegt das Schwachstellenregister und wirkt an der Bewertung kompensierender Kontrollen mit.

[... 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 mindestens jährlich oder anlassbezogen zu überprüfen bei:

9.1.1 Wesentlichen regulatorischen Aktualisierungen (z. B. Änderungen an DORA, NIS2)

9.1.2 Änderungen an Rahmenwerken zur Priorisierung von Schwachstellen (z. B. CVSS-Aktualisierungen)

9.1.3 Wesentlichen Änderungen der IT-Umgebung (z. B. Cloud-Migration, grundlegende EDR-Umstellung)

9.1.4 Sicherheitsvorfällen mit hoher öffentlicher Wahrnehmung oder externen Warnhinweisen, die eine Stärkung der Richtlinie erforderlich machen

9.2 Die Überprüfungen sind durch den CISO in Zusammenarbeit mit Security Operations, Risikomanagement und der Infrastrukturleitung durchzuführen.

9.3 Aktualisierungen der Richtlinie müssen:

9.3.1 Im Register zur Lenkung von ISMS-Dokumenten dokumentiert werden

9.3.2 Durch die Geschäftsleitung geprüft und genehmigt werden

9.3.3 Allen betroffenen Stellen, einschließlich Drittverarbeitern, mitgeteilt werden

9.4 Frühere Versionen sind zu Audit- und Rechenschaftszwecken sicher aufzubewahren.

10. Zugehörige Richtlinien und Verknüpfungen

10.1 P1 - Informationssicherheitsrichtlinie. Legt die übergeordnete Verpflichtung zum Schutz von Systemen und Daten fest, einschließlich des proaktiven Managements von Schwachstellen und der Sicherstellung der Softwareintegrität.

10.2 P5 - Richtlinie für Änderungsmanagement. Regelt alle Patch-Bereitstellungen und Konfigurationsanpassungen und fordert Dokumentation, Tests, Genehmigung und Rollback-Verfahren als Ergänzung zu Prozessen der Schwachstellenbehebung.

10.3 P6 - Risikomanagement-Richtlinie. Unterstützt die Klassifizierung und Behandlung nicht behobener Schwachstellen durch strukturierte Risikobewertungen, Auswirkungsanalysen und Verfahren zur Akzeptanz von Restrisiken.

10.4 P12 - Asset-Management-Richtlinie. Stellt sicher, dass Systeme korrekt inventarisiert und klassifiziert werden, sodass konsistente Schwachstellenscans, die Zuweisung von Verantwortlichkeiten und eine durchgängige Patch-Abdeckung über den gesamten Lebenszyklus hinweg möglich sind.

10.5 P22 - Richtlinie für Protokollierung und Überwachung. Definiert Anforderungen an Ereigniserkennung und die Erstellung eines Prüfpfads. Diese Richtlinie unterstützt die Transparenz in Bezug auf Patch-Aktivitäten, nicht autorisierte Änderungen und Exploit-Versuche gegen bekannte Schwachstellen.

10.6 P30 - Incident-Response-Richtlinie (P30). Legt Eskalationsprotokolle und Eindämmungsstrategien für ausgenutzte Schwachstellen, Untersuchungen von Sicherheitsvorfällen und Korrekturmaßnahmen im Einklang mit den Kontrollen dieser Richtlinie fest.

11. Referenzstandards und Rahmenwerke

11.1 ISO/IEC 27001: Abschnitt 8.1 - Operative Planung und Steuerung: Verlangt die systematische Behandlung technischer Schwachstellen, um die fortlaufende Wirksamkeit von Sicherheitskontrollen sicherzustellen.

11.2 ISO/IEC 27002:2022 - Maßnahmen 8.8, 8.9, 5: Stellt Umsetzungsleitlinien für Patch-Management, Schwachstellenscans, Softwareintegrität sowie die Integration mit sicherer Konfiguration und Asset-Inventaren bereit.

11.3 NIST SP 800-53 Rev. 5: RA-5 - Überwachung und Scannen von Schwachstellen: Verlangt regelmäßige Scans und die Nachverfolgung der Mängelbehebung. SI-2 - Mängelbehebung: Verlangt die zeitnahe Bewertung und Eindämmung von Fehlern durch verfügbare Patches oder andere Maßnahmen. CM-2 / CM-6 - Baseline-Konfigurationen und Kontrollen für das Konfigurationsmanagement: Schafft die Grundlage für sichere Systemkonfigurationen in Verbindung mit der Durchsetzung von Patches.

11.4 EU-DSGVO (2016/679): Artikel 32 - Sicherheit der Verarbeitung: Verlangt die Umsetzung geeigneter technischer Maßnahmen, wie zeitnahes Patchen und Schwachstellenbehandlung, um Vertraulichkeit und Resilienz von Systemen sicherzustellen. Erwägungsgrund 49: Ermutigt Organisationen zur Umsetzung präventiver Kontrollen gegen bekannte Bedrohungen zur Unterstützung von Sicherheit und Kontinuität.

11.5 EU-NIS2-Richtlinie (2022/2555): Artikel 21(2)(d): Verpflichtet wesentliche und wichtige Einrichtungen dazu, Systemschwachstellen zu erkennen, darauf zu reagieren und sie einzudämmen sowie ein hohes Maß an Cyberhygiene aufrechtzuerhalten.

11.6 EU-DORA (2022/2554): Artikel 8 - IKT-Risikomanagement: Verlangt die Identifizierung und rechtzeitige Behebung von Schwachstellen in Informations- und Kommunikationstechnologien, die in Finanzsystemen eingesetzt werden. Artikel 10(2)(f): Betont kontinuierliche, bedrohungsgeleitete Schwachstellenbewertungen und Patch-Management als Bestandteil der operationellen Resilienz.

11.7 COBIT 2019: DSS05.02 - Sicherheitslücken verwalten: Weist Organisationen an, bekannte technische Schwachstellen zu scannen, nachzuverfolgen und einzudämmen. DSS01.03 - Infrastruktur überwachen: Stellt sicher, dass Systeme auf Anzeichen von Ausnutzung oder Schwachstellen überwacht werden. MEA03 - Einhaltung überwachen, evaluieren und beurteilen: Verlangt regelmäßige Prüfungen der Kontrollwirksamkeit, einschließlich Patch-Status und Ausnahmebehandlung.