					Fügen Sie hier den Namen der eingetragenen juristischen Person ein							
Dokumentnummer: P20					Dokumenttitel: **Richtlinie für Endpunktschutz / Schutz vor Schadsoftware**							
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 Standards und Vorschriften ausgerichtet

Standard/Regulation	Clause/Article	Comment
ISO/IEC 27001:2022	Clause 8	Endpunktschutz und Kontrollen zum Schutz vor Schadsoftware sind erforderlich, um die Ziele des Informationssicherheitsmanagementsystems (ISMS) zu erfüllen
ISO/IEC 27002:2022	Controls 8.7, 8	Stellt technische Kontrollen und Leitlinien für Anti-Malware, Endpunktschutz und das Vorfallmanagement bereit
NIST SP 800-53 Rev.5	SI-3, SI-4, CM-6	Definiert Anforderungen an den Schutz vor Schadcode, zentrales Monitoring und Baseline-Konfigurationen
EU GDPR	Article 32	Verlangt angemessene technische Maßnahmen zum Schutz personenbezogener Daten, einschließlich Schutz vor Schadsoftware
EU NIS2	Article 21(2)(d)	Verlangt die Umsetzung von Maßnahmen zur Erkennung von Bedrohungen und präventiven Maßnahmen auf Endpunktebene
EU DORA	Article 9	Verlangt IKT-Risikomanagement für Schadsoftware und die Abwehr endpunktbasierter Bedrohungen
COBIT 2019	DSS05.01, DSS01.04, MEA	Verlangt Schutz, Monitoring und Bewertung von Endpunktschutzkontrollen

1. Zweck

1.1 Diese Richtlinie definiert die verbindlichen Kontrollen und betrieblichen Anforderungen zum Schutz organisatorischer Endpunkte – einschließlich Desktop-Systemen, Laptops, mobilen Geräten und Servern – vor Schadsoftware und damit verbundenen Bedrohungen.

1.2 Sie legt Mindeststandards für Endpunktschutz, Erkennung von Schadsoftware, Eindämmungsmaßnahmen und verhaltensbasierte Überwachung fest, um sicherzustellen, dass Systeme sowohl gegenüber weit verbreiteten als auch gegenüber fortgeschrittenen Schadsoftware-Varianten resilient bleiben.

1.3 Die Richtlinie unterstützt unmittelbar die Einhaltung von ISO/IEC 27001:2022, Clause 8.1, und Annex A Maßnahme 8.7 und ist an regionalen Cybersicherheitsanforderungen gemäß GDPR, NIS2 und DORA ausgerichtet.

2. Geltungsbereich

2.1 Diese Richtlinie gilt für alle Endpunkte, einschließlich:

2.1.1 organisationsinterne oder organisationsverwaltete Desktop-Systeme, Laptops, mobile Geräte und virtuelle Instanzen

2.1.2 privat genutzte Geräte, die im Rahmen von Bring Your Own Device (BYOD) autorisiert sind (vorbehaltlich der Installation von MDM oder Endpunkt-Agenten)

2.1.3 Server und Infrastruktur-Assets, einschließlich cloudbasierter virtueller Maschinen und Edge-Geräte

2.1.4 Betriebssysteme, Treiber, lokale Dienste, Endpunkt-Agenten und Sicherheitskontrollen, die auf jedem Knoten installiert sind

2.2 Sämtliches Personal mit administrativer, technischer oder operativer Verantwortung für Endpunkte fällt unter diese Richtlinie, einschließlich:

2.2.1 interne Mitarbeitende und Auftragnehmer

2.2.2 Managed Service Provider (MSPs), ausgelagerter Desktop-Support und IT-Administratoren von Drittparteien

2.2.3 Benutzer, die zur Nutzung tragbarer Systeme, VPN-fähiger Laptops oder mobiler Zugriffe auf organisatorische Netzwerke autorisiert sind

2.3 Die von dieser Richtlinie abgedeckte Bedrohungslage umfasst unter anderem:

2.3.1 Viren, Würmer, Trojaner, Ransomware, Spyware, Rootkits, Adware, Keylogger und Botnetze

2.3.2 dateilose Schadsoftware, Zero-Day-Payloads, Schadsoftware zur Rechteausweitung und Browser-Exploit-Kits

2.3.3 Schadcode, der über Wechselmedien, Phishing-Vektoren, Drive-by-Downloads oder USB-basierte Angriffe eingebracht wird

3. Ziele

3.1 Schutz der Integrität, Verfügbarkeit und Vertraulichkeit von Endpunktsystemen und der von ihnen verarbeiteten Daten durch wirksame Prävention, Erkennung und Reaktion im Zusammenhang mit Schadsoftware.

3.2 Verhinderung der Ausführung oder Verbreitung von Schadcode in organisatorischen Netzwerken durch die Durchsetzung technischer Schutzmaßnahmen, Härtung auf Basis von Baseline-Konfigurationen und Echtzeit-Telemetrie.

3.3 Integration des Endpunktschutzes in weitere ISMS-Kontrollen, einschließlich Schwachstellenmanagement, Zugriffskontrolle, Protokollierung und Überwachung sowie Incident Response.

3.4 Sicherstellung einer kontinuierlichen Transparenz über alle Endpunkte durch zentral verwaltete Schutzplattformen, einschließlich Antiviren-/Anti-Malware-Agenten, EDR (Endpoint Detection and Response) und SIEM-Telemetrie.

3.5 Erfüllung gesetzlicher, regulatorischer und normativer Anforderungen an die Endpunktsicherheit (z. B. GDPR Article 32, NIS2 Article 21, DORA Article 9).

3.6 Festlegung klarer Verantwortlichkeiten, Durchsetzung von SLAs für Patch- und Alarmbearbeitung sowie Sicherstellung der Auditfähigkeit durch Dokumentation und Berichterstattung.

4. Rollen und Verantwortlichkeiten

4.1 Chief Information Security Officer (CISO)

4.1.1 Ist Eigentümer dieser Richtlinie und stellt deren Ausrichtung auf das ISMS und die übergreifende Sicherheitsstrategie sicher.

4.1.2 Überprüft vierteljährlich Kennzahlen zum Endpunktschutz, Trends bei Sicherheitsvorfällen und die Wirksamkeit der eingesetzten Werkzeuge.

4.1.3 Genehmigt Ausnahmen und Risikoakzeptanzen in Bezug auf die Abdeckung des Endpunktschutzes.

4.2 Verantwortlicher für Endpunktsicherheit / SOC-Manager

4.2.1 Verwaltet Endpunktschutzsysteme (z. B. AV, EDR, MDM).

4.2.2 Überwacht die Durchsetzung dieser Richtlinie, die Feinabstimmung der Bedrohungserkennung und die Response-Playbooks.

4.2.3 Pflegt Abdeckungsstatistiken, Protokolle zu Schadsoftwarevorfällen und Baseline-Konfigurationen für Alarmierungen.

[... 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 dann überprüft werden, wenn:

9.1.1 wesentliche Schadsoftware-Kampagnen oder Sicherheitsvorfälle an Endpunkten auftreten

9.1.2 neue Bedrohungsarten (z. B. dateilose Schadsoftware, Ransomware-Varianten) aktualisierte Erkennungs- oder Reaktionsstrategien erfordern

9.1.3 sich Endpunktschutzplattformen oder Agentenarchitekturen wesentlich ändern

9.1.4 gesetzliche oder regulatorische Anforderungen, die Endpunktkontrollen betreffen, aktualisiert werden

9.2 Die Überprüfung ist durch den Verantwortlichen für Endpunktsicherheit einzuleiten und mit den Funktionen CISO, Recht, Risiko und Audit zu koordinieren.

9.3 Genehmigte Überarbeitungen müssen im ISMS-Dokumentenregister dokumentiert, mit einer neuen Versionskennung versehen und allen betroffenen Parteien mitgeteilt werden.

9.4 Ersetzte Versionen müssen archiviert, im Zugriff beschränkt und gemäß den ISMS-Aufbewahrungsfristen zur Wahrung der Integrität des Prüfpfads aufbewahrt werden.

10. Zugehörige Richtlinien und Verknüpfungen

10.1 P1 - Informationssicherheitsrichtlinie. Sie legt grundlegende Prinzipien zum Schutz von Systemen, Daten und Netzwerken fest. Diese Richtlinie setzt diese Prinzipien auf Endpunktebene durch technische und prozessuale Kontrollen zum Schutz vor Schadsoftware um.

10.2 P4 - Richtlinie zur Zugriffskontrolle. Sie definiert Beschränkungen des Benutzerzugriffs, die auf Endpunktebene durchgesetzt werden, einschließlich Schutzmaßnahmen gegen Rechteausweitung und unbefugte Installationen nicht geprüfter Software.

10.3 P5 - Richtlinie zum Änderungsmanagement. Sie stellt sicher, dass Aktualisierungen von Endpunktschutzsoftware, Richtlinienregeln oder Agentenkonfigurationen Genehmigungen und kontrollierten Bereitstellungsprozessen unterliegen.

10.4 P12 - Richtlinie zum Asset Management. Sie stellt die für Endpunkttransparenz, Patch-Abdeckung und die Definition des Geltungsbereichs des Schutzes vor Schadsoftware erforderliche Grundlage für Asset-Klassifizierung und Inventarisierung bereit.

10.5 P22 - Richtlinie zur Protokollierung und Überwachung. Sie ermöglicht die Integration von Endpunktalarmen, dem Zustand von Agenten und Bedrohungsinformationen in zentrale SIEM-Systeme zur Echtzeiterkennung und forensischen Nachvollziehbarkeit.

10.6 P30 - Incident-Response-Richtlinie (P30). Sie verknüpft endpunktbasierte Schadsoftwarevorfälle mit standardisierten Workflows für Eindämmung, Beseitigung, Untersuchung und Wiederherstellung sowie mit zugewiesenen Rollen und Eskalationsschwellen.

11. Referenzstandards und Rahmenwerke

11.1 ISO/IEC 27001:

11.1.1 Clause 8.1 - Operative Planung und Steuerung: Verlangt die Umsetzung technischer Kontrollen, einschließlich Schutzmaßnahmen für Endpunkte, zur Aufrechterhaltung der ISMS-Ziele.

11.2 ISO/IEC 27002:2022 - Controls 8.7, 8:

11.2.1 Stellt detaillierte technische Leitlinien zu Anti-Malware-Maßnahmen, sicherer Softwarebereitstellung, Überwachung und Vorfallsbereitschaft für Endpunktumgebungen bereit.

11.3 NIST SP 800-53 Rev.5:

11.3.1 SI-3 - Schutz vor Schadcode: Verlangt den Einsatz von Anti-Malware-Werkzeugen mit Echtzeit-Scans, Scans bei Zugriff und Verhaltensanalyse.

11.3.2 SI-4 - Systemüberwachung: Unterstützt die Integration von Telemetrie in zentrale Erkennungsplattformen.

11.3.3 CM-6 - Konfigurationseinstellungen: Verstärkt Baseline-Kontrolleinstellungen auf Endpunkten, einschließlich der Durchsetzung von Schutz-Agenten.

11.4 EU GDPR (2016/679):

11.4.1 Article 32 - Sicherheit der Verarbeitung: Verlangt von Organisationen die Umsetzung angemessener technischer Maßnahmen zum Schutz personenbezogener Daten, einschließlich des Schutzes vor Bedrohungen durch Schadsoftware.

11.5 EU NIS2-Richtlinie (2022/2555):

11.5.1 Article 21(2)(d): Verpflichtet Einrichtungen zur Umsetzung von Maßnahmen zur Erkennung und Verhinderung von Bedrohungen, einschließlich Mechanismen zur Abwehr von Schadsoftware auf Endpunktebene.

11.6 EU DORA (2022/2554):

11.6.1 Article 9 - Anforderungen an das IKT-Risikomanagement: Verlangt von Finanzunternehmen die Einführung von Schutzmaßnahmen zur Verhinderung, Erkennung und Reaktion auf Schadsoftware und endpunktbasierte Bedrohungen.

11.7 COBIT 2019:

11.7.1 DSS05.01 - Schutz vor Schadsoftware: Verlangt die Erkennung und Minderung von Schadsoftware über alle organisatorischen Endpunkte hinweg.

11.7.2 DSS01.04 - Verfügbarkeit und Kapazität verwalten: Stellt sicher, dass der Schutz vor Schadsoftware mit Systemleistung und Aufrechterhaltung des Geschäftsbetriebs in Einklang steht.

11.7.3 MEA03 - Überwachen, Evaluieren und Beurteilen der Compliance: Verlangt regelmäßige Audits von Endpunktkontrollen und deren Schutzwirksamkeit.