					Fügen Sie hier den Namen der eingetragenen juristischen Person ein							
Dokumentnummer: P20S					Dokumenttitel: **Endpunktschutz - Richtlinie zum 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 relevanten Standards und Vorschriften ausgerichtet

Standard/Vorschrift	Klausel/Artikel	Kommentar
ISO/IEC 27001:2022	Klausel 8	Operative Kontrollen zum Schutz vor Schadsoftware
ISO/IEC 27002:2022	Maßnahme 8	Kontrollmaßnahmen für den Endpunktschutz
NIST SP 800-53 Rev.5	SI-3, SI-4	Schutz vor Schadcode und Reaktion auf Sicherheitsvorfälle
EU NIS2	Artikel 21(2)(d), (e)	Schutz vor Schadsoftware und Risikomanagement für wesentliche und wichtige Einrichtungen
EU DORA	Artikel 10(1), 15	Operative Resilienz und Überprüfung von Drittparteien
COBIT 2019	DSS05.02, DSS05.04	Endpunkt- und Netzwerkschutz sowie Überwachung
EU DSGVO	Artikel 32(1)(b), 33	Technische und organisatorische Maßnahmen sowie Meldung von Verletzungen des Schutzes personenbezogener Daten

1. Zweck

1.1 Diese Richtlinie legt die technischen, prozessualen und verhaltensbezogenen Mindestanforderungen zum Schutz aller Endgeräte – wie Laptops, Desktop-Computer, mobile Geräte und Wechselmedien – vor Schadcode fest, einschließlich Viren, Ransomware, Spyware, Rootkits und sonstigen Bedrohungen durch Schadsoftware.

1.2 Zweck dieser Richtlinie ist es, sicherzustellen, dass Endgeräte so ausgestattet, gewartet und genutzt werden, dass das Risiko einer Infektion mit Schadsoftware, ihrer Verbreitung und einer Kompromittierung von Systemen reduziert wird.

1.3 Die Organisation erkennt an, dass Endgeräte häufige Eintrittspunkte für Schadsoftware sind und daher gehärtet, überwacht und durch mehrere Schutzebenen abgesichert werden müssen.

1.4 Diese Richtlinie unterstützt die Zertifizierungsziele der Organisation nach ISO/IEC 27001:2022 und ist an der Datenschutz-Grundverordnung (DSGVO), der NIS2-Richtlinie, dem Digital Operational Resilience Act (DORA) sowie weiteren relevanten Rahmenwerken ausgerichtet.

2. Geltungsbereich

2.1 Diese Richtlinie gilt für:

2.1.1 alle Endgeräte der Organisation, einschließlich Desktop-Computer, Laptops, Tablets, Mobiltelefone und Point-of-Sale-Terminals,

2.1.2 privat genutzte Geräte im Rahmen von Bring Your Own Device (BYOD), die für den Zugriff auf Geschäftsanwendungen oder Daten verwendet werden,

2.1.3 Wechselmedien wie USB-Laufwerke und externe Festplatten,

2.1.4 sämtliche Betriebssysteme, Endgerätesoftware oder Kommunikationsmittel, die auf diesen Plattformen ausgeführt werden.

2.2 Sie gilt gleichermaßen für:

2.2.1 interne Mitarbeitende, Auftragnehmer, Praktikanten und Managed Service Provider,

2.2.2 Geräte, die vor Ort, remote oder im Rahmen hybrider Arbeitsmodelle verwendet werden,

2.2.3 cloudverbundene oder offline betriebene Endgeräte, auf denen geschäftliche oder personenbezogene Daten gespeichert werden.

3. Ziele

3.1 Verhinderung von Infektionen mit Schadsoftware und deren Ausbreitung über interne Systeme, Benutzergeräte und externe Verbindungen hinweg

3.2 Schnelle Erkennung und Eindämmung schadsoftwarebezogener Bedrohungen durch automatisierte Endpunktsicherheits-Technologien und definierte Eskalationswege

3.3 Sicherstellung, dass nur autorisierte, abgesicherte und überwachte Geräte für den Zugriff auf Geschäftsinformationen verwendet werden

3.4 Festlegung klarer Verantwortlichkeiten für Mitarbeitende und verbindlicher Verhaltensregeln für Benutzer zur Reduzierung des Risikos schadsoftwarebezogener Vorfälle

3.5 Aufrechterhaltung nachvollziehbarer und prüffähiger Aufzeichnungen zu Erkennungen von Schadsoftware, Reaktionsmaßnahmen und der Einhaltung dieser Richtlinie

3.6 Schutz personenbezogener und geschäftlicher Daten vor Kompromittierung durch Schadsoftware mittels mehrschichtiger Sicherheitsmaßnahmen

4. Rollen und Verantwortlichkeiten

4.1 Geschäftsführung

4.1.1 ist für diese Richtlinie verantwortlich und stellt sicher, dass ausreichende Ressourcen für den Endpunktschutz verfügbar sind,

4.1.2 genehmigt Antivirensoftware, Mobile-Device-Management-(MDM)-Werkzeuge und Regelungen für den Zugriff Dritter,

4.1.3 überprüft Berichte zu Schadsoftwarevorfällen, Auswirkungszusammenfassungen und Meldungen zu Verletzungen des Schutzes personenbezogener Daten, die Endgeräte betreffen.

4.2 IT-Support-Dienstleister / interner IT-Administrator

4.2.1 wählt Antivirensoftware, Anti-Malware-Lösungen sowie Software zur Endpoint Detection and Response (EDR) aus und stellt diese bereit,

4.2.2 stellt sicher, dass Aktualisierungen konsistent eingespielt und Protokolle aufbewahrt werden,

4.2.3 reagiert auf Warnmeldungen zu Schadsoftware, isoliert infizierte Systeme und führt Abhilfemaßnahmen durch,

4.2.4 setzt Kontrollen für die Nutzung von USB-Geräten und externen Datenträgern durch.

[... 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 Anforderung an die jährliche Überprüfung

9.1.1 Diese Richtlinie muss mindestens einmal jährlich formell durch die Geschäftsführung in Abstimmung mit dem IT-Support-Dienstleister und dem Datenschutzkoordinator überprüft werden.

9.2 Anlassbezogene Aktualisierungen

9.2.1 Aktualisierungen der Richtlinie müssen außerdem erfolgen, wenn:

9.2.1.1 eine wesentliche neue Bedrohung durch Schadsoftware oder ein Ausbruch die Endgeräte der Organisation betrifft,

9.2.1.2 Antiviren- oder EDR-Werkzeuge geändert, aktualisiert oder ersetzt werden,

9.2.1.3 ein Schadsoftwarevorfall Schwächen im Geltungsbereich oder in der Durchsetzung dieser Richtlinie aufdeckt,

9.2.1.4 rechtliche oder regulatorische Anforderungen (z. B. DSGVO, DORA, NIS2) aktualisiert werden.

9.3 Versionskontrolle und Kommunikation

9.3.1 Alle Änderungen an der Richtlinie müssen mit Versionsnummer, Datum und Zusammenfassung der Änderungen dokumentiert werden.

9.3.2 Mitarbeitende müssen über Aktualisierungen informiert werden, insbesondere wenn diese operative oder verhaltensbezogene Anforderungen ändern.

9.3.3 Frühere Versionen müssen mindestens 3 Jahre im Richtlinienarchiv aufbewahrt werden, um Audits zu unterstützen.

10. Zugehörige Richtlinien und Verknüpfungen

10.1 Diese Richtlinie ist in Verbindung mit den folgenden SME-Richtlinien umzusetzen:

10.1.1 P9S – Richtlinie für Remote-Arbeit: Stellt sicher, dass Anforderungen an den Endpunktschutz auf Geräten durchgesetzt werden, die außerhalb des Standorts oder in hybriden Arbeitsmodellen genutzt werden.

10.1.2 P12S – Richtlinie zum Asset-Management: Unterstützt die Nachverfolgung und Kontrolle aller Endgeräte und stellt sicher, dass nur autorisierte und geschützte Geräte verwendet werden.

10.1.3 P17S – Richtlinie zu Datenschutz und Privatsphäre: Verankert die Verhinderung von Schadsoftware als zentrale Datenschutzkontrolle zum Schutz personenbezogener und sensibler Daten vor Kompromittierung.

10.1.4 P22S – Richtlinie zur Protokollierung und Überwachung: Legt Anforderungen für die Protokollierung von Schadsoftwareereignissen und die Aufrechterhaltung der Sichtbarkeit von Warnmeldungen für eine frühzeitige Reaktion fest.

10.1.5 P30S – Incident-Response-Richtlinie: Definiert Eskalations-, Eindämmungs- und externe Benachrichtigungsschritte, wenn Schadsoftware zu einer Datenkompromittierung oder operativen Beeinträchtigung führt.

11. Referenzstandards und Rahmenwerke

11.1 ISO/IEC 27001

11.1.1 Klausel 8.1 – verlangt die Umsetzung operativer Kontrollen zur Reduzierung von Risiken wie Angriffen durch Schadsoftware.

11.2 ISO/IEC 27002

11.2.1 Maßnahme 8.7 – beschreibt Maßnahmen zum Schutz vor Schadsoftware einschließlich Antivirensoftware, Echtzeit-Scans, Aktualisierungen und Benutzerschulung.

11.3 NIST SP 800-53 Rev.5

11.3.1 SI-3 – verlangt die Implementierung von Schutzmechanismen gegen Schadcode auf Endgeräten.

11.3.2 SI-4 – verlangt Überwachung, Erkennung, Analyse und Reaktionsmaßnahmen für Bedrohungen und Warnmeldungen auf Endgeräteebene.

11.4 EU DSGVO

11.4.1 Artikel 32(1)(b) – verlangt technische und organisatorische Maßnahmen (wie Antivirensoftware) zum Schutz personenbezogener Daten.

11.4.2 Artikel 33 – verpflichtet zur Meldung von Verletzungen des Schutzes personenbezogener Daten, wenn Schadsoftware die Integrität, Vertraulichkeit oder Verfügbarkeit von Daten beeinträchtigt.

11.5 EU NIS2-Richtlinie

11.5.1 Artikel 21(2)(d) – verlangt Maßnahmen zur Verhinderung und Reaktion auf Bedrohungen durch Schadsoftware in wesentlichen und wichtigen Einrichtungen.

11.5.2 Artikel 21(2)(e) – verlangt mehrschichtige Strategien für das Cybersicherheitsrisikomanagement einschließlich des Schutzes von Endgeräten vor Schadsoftware.

11.6 EU DORA

11.6.1 Artikel 10(1) – verlangt, dass IKT-Systeme im Rahmen der operativen Resilienz vor Schadsoftware und anderen Bedrohungen geschützt werden.

11.6.2 Artikel 15 – verpflichtet Finanzorganisationen, den Schutz vor Schadsoftware bei Drittparteien-Dienstleistern zu überprüfen.

11.7 COBIT 2019

11.7.1 DSS05.02 – betont Schutzmaßnahmen zur Abwehr von Bedrohungen durch Schadsoftware auf Endgeräten und in Netzwerken.

11.7.2 DSS05.04 – unterstützt die Überwachung und Alarmierung bei schadsoftwarebezogenen Sicherheitsereignissen als Teil des laufenden Betriebs.