					Fügen Sie hier den Namen der eingetragenen juristischen Person ein							
Dokumentnummer: P22S					Dokumenttitel: **Richtlinie zur Protokollierung und Überwachung**							
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 Maßnahmen, einschließlich Protokollierung
ISO/IEC 27002:2022	Maßnahmen 8.15, 8.16, 8.17	Ereignisprotokollierung, Schutz und Überwachung
NIST SP 800-53 Rev.5	AU-2 bis AU-12, SI-4	Inhalte von Audit-Logs/Prüfprotokollen, Überprüfung, Aufbewahrung, Anomalieerkennung, Alarmierung
DSGVO	Artikel 5(1)(f), 32, 33	Vertraulichkeit und Integrität von Daten, technische Maßnahmen und Meldung von Verletzungen des Schutzes personenbezogener Daten
NIS2-Richtlinie der EU	Artikel 21(2)(d), 23	Protokollierungsmechanismen zur Erkennung von Anomalien und Meldung von Vorfällen innerhalb von 24 Stunden
DORA der EU	Artikel 10, 15	Operative Resilienz, Überwachung und Protokollierung von Dienstleistern
COBIT 2019	DSS01.03, DSS05.02	Nachvollziehbarkeit von Aktivitäten und Schutz durch Protokollierung und Überwachung

1. Zweck

1.1 Diese Richtlinie legt verbindliche Kontrollen für die Protokollierung und Überwachung fest, um die Sicherheit, Rechenschaftspflicht und operative Integrität der IT-Systeme der Organisation sicherzustellen.

1.2 Sie definiert die Arten von Ereignissen, die zu protokollieren sind, wie Protokolle zu speichern sind, wie sie zu überprüfen sind und welche Verantwortlichkeiten Mitarbeitende und Dienstleister tragen.

1.3 Protokollierung und Überwachung unterstützen die Erkennung von Bedrohungen, die Einhaltung regulatorischer Anforderungen, die Reaktion auf Vorfälle und die forensische Analyse.

1.4 Diese Richtlinie ermöglicht es der Organisation, die Anforderungen an operative Maßnahmen nach ISO/IEC 27001 zu erfüllen, und unterstützt die fortlaufende Auditbereitschaft, das Vertrauen der Kunden sowie die Einhaltung von DSGVO, NIS2 und DORA.

2. Geltungsbereich

2.1 Diese Richtlinie gilt für alle Systeme und Benutzer innerhalb der Organisation, einschließlich:

2.1.1 Arbeitsplatzrechnern, Laptops, Servern, Firewalls, Switches, Routern und drahtlosen Zugangspunkten

2.1.2 Cloud-Diensten, die für den Geschäftsbetrieb genutzt werden (z. B. E-Mail, Dateispeicherung, Backups, Kollaborationswerkzeuge)

2.1.3 Protokollierungsfunktionen in Antivirensoftware, Anwendungen, Betriebssystemen und Netzwerkkomponenten

2.1.4 allen Mitarbeitenden und Auftragnehmern sowie Managed Service Providern (MSPs), die Systeme nutzen oder administrieren

2.1.5 allen Orten, an denen Unternehmens-IT-Systeme genutzt werden, einschließlich Remote-, Hybrid- oder Bring-Your-Own-Device-(BYOD)-Umgebungen

2.2 Die Richtlinie gilt außerdem für Protokolle, die durch Dienste Dritter erzeugt werden, sofern die Organisation über administrativen Zugriff oder Auditrechte verfügt.

3. Ziele

3.1 Sicherstellung der Protokollierung von Systemaktivitäten, einschließlich Authentifizierung, Konfigurationsänderungen, Zugriffen auf sensible Daten und Sicherheitswarnungen

3.2 Aufrechterhaltung sicherer und genauer Protokolle zur Erkennung von Richtlinienverstößen, Systemfehlern oder unbefugten Handlungen

3.3 Ermöglichung einer zeitnahen Überprüfung von Protokollen bei Vorfällen, Untersuchungen und Audits

3.4 Unterstützung der Zeitsynchronisierung zur Sicherstellung der Integrität und Korrelation von Protokolldaten

3.5 Schutz von Protokollen vor Manipulation, Verlust oder vorzeitiger Löschung

3.6 Erfüllung gesetzlicher und regulatorischer Verpflichtungen hinsichtlich Rechenschaftspflicht, Nachvollziehbarkeit und Reaktion auf Verletzungen des Schutzes personenbezogener Daten

4. Rollen und Verantwortlichkeiten

4.1 Geschäftsführung (GM)

4.1.1 Genehmigt diese Richtlinie und stellt ihre Umsetzung in allen geschäftskritischen Systemen sicher

4.1.2 Überprüft Warnmeldungen mit hohem Schweregrad und wesentliche Auditfeststellungen, die von IT- oder Datenschutzfunktionen gemeldet werden

4.1.3 Genehmigt Ausnahmen, wenn Protokollierung oder Aufbewahrung technisch nicht durchgesetzt werden können

4.2 IT-Support-Dienstleister / interne IT-Funktion

4.2.1 Implementiert und konfiguriert die Protokollierung für Betriebssysteme, Netzwerkgeräte, Antivirenlösungen und geschäftskritische Anwendungen

4.2.2 Stellt sicher, dass Protokolle aufbewahrt, gesichert und vor Veränderungen geschützt werden

4.2.3 Überprüft Protokolle planmäßig und untersucht verdächtige oder unbefugte Aktivitäten

4.2.4 Betreibt Alarmierungssysteme, die anomales Verhalten oder Indikatoren für Eindringversuche erkennen

[... 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 jährlich durch die Geschäftsführung (GM) mit Unterstützung des IT-Support-Dienstleisters und des Datenschutzkoordinators überprüft werden.

9.2 Auslöser für Überprüfungen

9.2.1 Außerplanmäßige Überprüfungen müssen durchgeführt werden als Reaktion auf:

9.2.1.1 Feststellungen im Zusammenhang mit der Protokollierung aus internen oder externen Audits

9.2.1.2 Informationssicherheitsvorfälle, bei denen Protokolle fehlten, beschädigt waren oder nicht ausreichten

9.2.1.3 Wesentliche Änderungen an der IT-Infrastruktur (z. B. Migration auf Cloud-Plattformen für die Protokollierung)

9.2.1.4 Aktualisierungen gesetzlicher oder regulatorischer Verpflichtungen (z. B. DSGVO, NIS2, DORA)

9.3 Versionskontrolle

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

9.3.2 Frühere Versionen müssen archiviert und mindestens 3 Jahre aufbewahrt werden

9.3.3 Aktualisierte Richtlinien müssen den betroffenen Interessenträgern mitgeteilt werden, insbesondere Personen mit Zugriff auf Systemebene

10. Zugehörige Richtlinien und Verknüpfungen

10.1 Diese Richtlinie unterstützt unmittelbar die folgenden SME-Richtlinien zur Informationssicherheit und wird durch diese unterstützt:

10.1.1 P17S – Richtlinie zu Datenschutz und Privatsphäre: Stellt sicher, dass Protokolldaten mit personenbezogenen Informationen mit Integritäts-, Aufbewahrungs- und Zugriffsschutzmaßnahmen im Einklang mit den Anforderungen der DSGVO verwaltet werden.

10.1.2 P21S – Netzwerksicherheitsrichtlinie: Schafft die Grundlage für die Erfassung von Protokollen im Zusammenhang mit Firewalls, drahtlosem Zugriff, VPNs und der Überwachung der Segmentierung.

10.1.3 P24S – Richtlinie zur sicheren Entwicklung: Stellt sicher, dass Anwendungsprotokolle (z. B. für Anmeldeversuche, Fehler und Ausnahmen) in Softwaredesign und -betrieb integriert sind.

10.1.4 P30S – Incident-Response-Richtlinie (P30): Ist auf genaue und vollständige Protokolldaten angewiesen, um Informationssicherheitsereignisse zu erkennen, zu analysieren und darauf zu reagieren.

10.1.5 P23S – Richtlinie zur Zeitsynchronisierung: Stellt konsistente und nachvollziehbare Zeitstempel auf allen Systemen sicher, sodass Protokolle bei Untersuchungen korreliert werden können.

11. Referenzstandards und Rahmenwerke

11.1 ISO/IEC 27001

11.1.1 Klausel 8.1 – Verlangt die Umsetzung operativer Maßnahmen zur Minderung von Informationssicherheitsrisiken, einschließlich Protokollierung.

11.2 ISO/IEC 27002

11.2.1 Maßnahme 8.15 – Verlangt die Ereignisprotokollierung zur Unterstützung der Erkennung von Anomalien und der Rechenschaftspflicht.

11.2.2 Maßnahme 8.16 – Verlangt den Schutz von Protokollen vor Manipulation und unbefugtem Zugriff.

11.2.3 Maßnahme 8.17 – Verlangt die Überwachung von Systemen auf ungewöhnliche Aktivitäten und die Bestätigung der Wirksamkeit von Überwachungskontrollen.

11.3 NIST SP 800-53 Rev.5

11.3.1 AU-2 bis AU-12 – Decken Inhalte von Audit-Logs/Prüfprotokollen, Überprüfung, Aufbewahrung und automatisierte Alarmierung ab.

11.3.2 SI-4 – Verlangt die Erkennung von Systemanomalien und die Meldung verdächtiger Ereignisse.

11.4 DSGVO

11.4.1 Artikel 5(1)(f) – Verlangt Integrität und Vertraulichkeit personenbezogener Daten, was auch die Protokollierung von Zugriffen umfasst.

11.4.2 Artikel 32 – Schreibt technische und organisatorische Maßnahmen zur Gewährleistung der Sicherheit vor, einschließlich Protokollierung und Überwachung.

11.4.3 Artikel 33 – Verlangt die rechtzeitige Meldung von Verletzungen des Schutzes personenbezogener Daten, unterstützt durch Protokolle, die eine Ursachenanalyse ermöglichen.

11.5 NIS2-Richtlinie der EU

11.5.1 Artikel 21(2)(d) – Verlangt Protokollierungsmechanismen, die Anomalien erkennen und Untersuchungen von Vorfällen unterstützen.

11.5.2 Artikel 23 – Schreibt die Meldung von Vorfällen innerhalb von 24 Stunden vor, was von genauen und zeitnah verfügbaren Protokolldaten abhängt.

11.6 EU DORA

11.6.1 Artikel 10 – Verlangt digitale operationale Resilienz, einschließlich der Nachvollziehbarkeit IKT-bezogener Vorfälle durch Protokollierung.

11.6.2 Artikel 15 – Verpflichtet zur Überwachung von Dienstleistern, einschließlich Zugriffs- und Überprüfungsrechten in Bezug auf Protokolle.

11.7 COBIT 2019

11.7.1 DSS01.03 – Verlangt die Nachvollziehbarkeit von Systemaktivitäten durch Protokollierung und Überwachung.

11.7.2 DSS05.02 – Behandelt Protokollierung als wesentliche Maßnahme zum Schutz vor Schadsoftware und anderen unbefugten Aktivitäten.