					Fügen Sie hier den Namen der eingetragenen juristischen Person ein							
Dokumentnummer: P22					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**

1. Zweck

1.1 Zweck dieser Richtlinie ist es, klare und durchsetzbare Anforderungen für die Erstellung, den Schutz, die Überprüfung und die Auswertung von Protokollen festzulegen, die wesentliche System- und Sicherheitsereignisse in der gesamten IT-Umgebung der Organisation erfassen.

1.2 Protokollierung und Überwachung sind wesentlich für die Erkennung von Anomalien, die Reaktion auf Bedrohungen, forensische Untersuchungen, Auditfähigkeit und die Einhaltung rechtlicher Anforderungen. Diese Richtlinie stellt sicher, dass alle systemgenerierten Ereignisse ordnungsgemäß aufgezeichnet, aufbewahrt und mit zeitsynchroner Genauigkeit korreliert werden.

1.3 Diese Richtlinie unterstützt maßgeblich ISO/IEC 27001 Abschnitt 8.1 sowie Anhang A, Maßnahmen 8.15 (Protokollierung), 8.16 (Überwachung) und 8.17 (Uhrensynchronisation), und ist unmittelbar regulatorischen Verpflichtungen aus DSGVO, NIS2, DORA und COBIT 2019 zugeordnet.

2. Geltungsbereich

2.1 Diese Richtlinie gilt für alle Systeme, Dienste und Umgebungen, die Daten speichern, verarbeiten oder übertragen und in den Geltungsbereich des Informationssicherheitsmanagementsystems (ISMS) fallen, einschließlich:

2.1.1 On-Premises-Infrastrukturen, Cloud-basierter Dienste (z. B. IaaS, PaaS, SaaS) und hybrider Umgebungen

2.1.2 Betriebssysteme, Datenbanken, Anwendungen und Netzwerkkomponenten

2.1.3 Sicherheitssysteme wie SIEM-Systeme, Firewalls, EDR-Plattformen, VPN-Konzentratoren und Identitätsprovider

2.2 Die folgenden Anspruchsgruppen fallen in den Geltungsbereich:

2.2.1 interne Benutzer mit System- oder Administrationsberechtigungen

2.2.2 Mitarbeitende aus Infrastruktur und IT-Betrieb

2.2.3 Security Operations Center (SOC) und Teams zur Bedrohungserkennung

2.2.4 Softwareentwickler und Anwendungsverantwortliche

2.2.5 externe Dienstleister, die Systeme mit Protokollerzeugung verwalten

3. Ziele

3.1 Sicherzustellen, dass alle kritischen Systeme Sicherheitsereignisprotokolle und Aufzeichnungen über Systemaktivitäten erzeugen, die gemäß regulatorischen, rechtlichen und vertraglichen Anforderungen aufbewahrt werden.

3.2 Die Mindestarten von Ereignissen und die Mindestinhalte von Protokollen festzulegen, die erforderlich sind, um unbefugte Aktivitäten zu erkennen, Benutzeraktionen nachzuvollziehen und forensische Untersuchungen zu unterstützen.

3.3 Schutzmaßnahmen durchzusetzen, um Manipulationen an Protokollen, unbefugtes Löschen oder unkontrollierten Zugriff auf Protokolldaten zu verhindern.

3.4 Zentrale Systeme zur Protokollierung und Alarmierung (z. B. SIEM) einzurichten, um verdächtige Aktivitäten nahezu in Echtzeit zu aggregieren, zu korrelieren und zu eskalieren.

3.5 Sicherzustellen, dass Systemuhren synchronisiert sind, um eine präzise systemübergreifende Korrelation und Vorfallanalyse zu ermöglichen.

3.6 Kontinuierliche Verbesserung und Compliance zu ermöglichen, indem die Protokollüberwachung in Audit-, Risiko- und Incident-Management-Prozesse integriert wird.

4. Rollen und Verantwortlichkeiten

4.1 Chief Information Security Officer (CISO)

4.1.1 Ist verantwortlich für diese Richtlinie und stellt sicher, dass sie am Risikoprofil der Organisation, an Audit-Anforderungen und an den Verpflichtungen aus dem ISMS ausgerichtet ist.

4.1.2 Genehmigt den Protokollierungsumfang für regulierte oder risikobehaftete Systeme und überwacht die Compliance-Berichterstattung.

4.2 Leiter des Security Operations Center (SOC)

4.2.1 Betreibt und pflegt zentrale Plattformen für das Log-Management (z. B. SIEM).

4.2.2 Definiert Regeln für die Log-Aggregation, Alarmschwellen und Eskalationspfade für die Triage von Sicherheitsvorfällen.

4.2.3 Prüft tägliche Berichte und stellt sicher, dass Anomalien analysiert, dokumentiert und bei Bedarf eskaliert 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 Diese Richtlinie muss jährlich oder anlassbezogen früher überprüft werden als Reaktion auf:

9.1.1 wesentliche Änderungen der Systemarchitektur oder der Protokollierungsinfrastruktur (z. B. SIEM-Migration)

9.1.2 Änderungen regulatorischer Anforderungen an die Protokollierung (z. B. Vorgaben aus NIS2 oder DORA)

9.1.3 Feststellungen aus Audits oder Nachbetrachtungen von Vorfällen

9.1.4 neue Bedrohungen, die eine verstärkte Überwachung erfordern (z. B. Insider-Bedrohungen, Kompromittierung der Lieferkette)

9.2 Der Überprüfungsprozess ist vom Leiter des Security Operations Center (SOC) in Abstimmung mit dem CISO, dem Risikomanagement, der Compliance-Funktion und den IT-Infrastrukturteams zu leiten.

9.3 Genehmigte Änderungen müssen im ISMS-Dokumentenlenkungsregister versionskontrolliert und an folgende Stellen kommuniziert werden:

9.3.1 alle Anspruchsgruppen mit Verantwortung für die Wartung von Protokollierungssystemen

9.3.2 Anwendungs- und Systemverantwortliche

9.3.3 externe Dienstleister mit Pflichten zur Bereitstellung von Telemetrie oder zur SIEM-Integration

9.4 Alle abgelösten Versionen müssen sicher archiviert werden; der Zugriff ist für Audit- und Rechtszwecke auf autorisierte ISMS-Verantwortliche zu beschränken.

10. Zugehörige Richtlinien und Verknüpfungen

10.1 P1 – Informationssicherheitsrichtlinie. Legt die grundlegende Verpflichtung zum Schutz von Systemen und Daten fest, in deren Rahmen Protokollierung und Überwachung als wesentliche detektive Kontrollen und unterstützende Mechanismen für die Reaktion dienen.

10.2 P4 – Richtlinie zur Zugriffskontrolle. Stellt sicher, dass privilegierte Zugriffe, Benutzeranmeldungen und Autorisierungsereignisse in Protokollen erfasst und auf Missbrauch oder anomales Verhalten überwacht werden.

10.3 P5 – Richtlinie zum Änderungsmanagement. Verlangt die Protokollierung von Systemänderungen, Patch-Bereitstellungen und Konfigurationsaktualisierungen, die Risiken oder unbefugte Änderungen verursachen können.

10.4 P21 – Netzwerksicherheitsrichtlinie. Erfordert Protokollierung auf Netzwerkebene (z. B. Firewall-Protokolle, IDS-/IPS-Warnungen, VPN-Aktivitäten) und die Integration mit dem SIEM, um Transparenz in Bezug auf Verkehrsanomalien und den Schutz von Netzgrenzen sicherzustellen.

10.5 P23 – Richtlinie zur Zeitsynchronisation. Erzwingt konsistente Systemzeiten, was für eine verlässliche Protokollierung und die Korrelation von Sicherheitsereignissen über mehrere Umgebungen hinweg wesentlich ist.

10.6 P30 – Incident-Response-Richtlinie (P30). Stützt sich auf Protokolldaten und Alarmierungsmechanismen, um Informationssicherheitsvorfälle zu identifizieren, zu untersuchen und darauf zu reagieren, und bewahrt zugleich forensische Artefakte für die Nachbereitung von Vorfällen.

11. Referenzstandards und Rahmenwerke

11.1 ISO/IEC 27001

11.1.1 Abschnitt 8.1 – Betriebliche Planung und Steuerung: Verlangt Kontrollen zur Überwachung des Betriebs und zum Schutz vor unbefugtem Zugriff und Systemmissbrauch.

11.2 ISO/IEC 27002:2022 – Maßnahmen 8.15, 8.16, 8

11.2.1 Definiert detaillierte Anforderungen an die Protokollierung, einschließlich der aufzuzeichnenden Ereignisse, des Schutzes und der Analyse von Protokollen sowie der systemübergreifenden Sicherstellung verlässlicher Zeitstempel.

11.3 NIST SP 800-53 Rev.

11.3.1 AU-2 bis AU-12: Behandelt Ereignisauswahl, Protokollierung, Schutz, Auditüberprüfung, Reaktion auf Audit-Fehler und die Aufbewahrung von Audit-Aufzeichnungen.

11.3.2 SI-4 – Systemüberwachung: Verlangt eine aktive Systemüberwachung mit Warnungen auf Basis anomaler Aktivitäten.

11.3.3 SC-45 – Synchronisierung der Systemzeit: Stärkt die Zeitgenauigkeit für die Nachvollziehbarkeit von Ereignissen und die Korrelation von Vorfällen.

11.4 EU GDPR (2016/679)

11.4.1 Artikel 32 – Sicherheit der Verarbeitung: Verlangt technische Maßnahmen wie Protokollierung und Überwachung zur Gewährleistung von Sicherheit und Rechenschaftspflicht, insbesondere beim Zugriff auf personenbezogene Daten.

11.5 EU NIS2-Richtlinie (2022/2555)

11.5.1 Artikel 21(2)(e): Verlangt Ereignisprotokollierung und Überwachungssysteme zur schnellen Erkennung von und Reaktion auf Sicherheitsvorfälle.

11.6 EU DORA (2022/2554)

11.6.1 Artikel 9 – Management von IKT-Risiken: Verlangt Mechanismen zur Erkennung anomaler Aktivitäten, zur Protokollierung von Vorfällen und zur Aufbewahrung forensischer Daten.

11.6.2 Artikel 11 – Tests von Business-Continuity-Plänen (BCP/DRP): Betont die Kontinuität der Überwachung und die Validierung der Verfügbarkeit von Protokollen bei betrieblichen Störungen.

11.7 COBIT 2019

11.7.1 DSS01.05 – Sicherheitsprotokolle verwalten: Verlangt die Umsetzung von Protokollierungsfähigkeiten für alle kritischen Infrastrukturen.

11.7.2 DSS05.04 – Sicherheitsereignisse überwachen: Verlangt die Echtzeitüberwachung und Analyse von Protokollen zur Erkennung von und Reaktion auf Ereignisse.

11.7.3 MEA03 – Einhaltung überwachen, evaluieren und beurteilen: Verlangt die regelmäßige Überprüfung von Protokollierungspraktiken und deren Ausrichtung an Kontrollzielen.