					Fügen Sie hier den Namen der eingetragenen juristischen Person ein							
Dokumentnummer: P23S					Dokumenttitel: **Richtlinie zur Zeitsynchronisierung**							
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	Relevante Kontrollanforderungen
ISO/IEC 27002:2022	Maßnahme 8	Synchronisierter Systembetrieb
NIST SP 800-53 Rev.5	SC-45, AU-8	Vertrauenswürdiges NTP und Genauigkeit von Protokollzeitstempeln
EU-DSGVO	Artikel 5(1)(d), 32	Genauigkeit, Rechenschaftspflicht und Integrität bei personenbezogenen Daten durch synchronisierte Zeitstempel
EU NIS2	Artikel 21(2)(d)	Durch synchronisierte Protokolle unterstützte Überwachungs- und Erkennungsfähigkeiten
EU DORA	Artikel 10, 15	Operative Resilienz und genaue technische Aufzeichnungen
COBIT 2019	DSS05.02, MEA03	Mit Zeitstempeln versehene Ereignisse und nachweisgestützte Überwachung

1. Zweck

1.1 Diese Richtlinie legt verbindliche Kontrollen zur Aufrechterhaltung einer genauen, synchronisierten Zeit auf allen Systemen fest, die Unternehmensdaten speichern, übertragen oder verarbeiten.

1.2 Die Zeitsynchronisierung ist wesentlich, um die Nachvollziehbarkeit von Systemprotokollen sicherzustellen, Informationssicherheitsvorfälle korrekt zu korrelieren und Nachweise für forensische Analysen oder rechtliche Prüfungen belastbar zu machen.

1.3 Die Organisation setzt die automatisierte Zeitsynchronisierung als grundlegende Anforderung für Auditintegrität, Incident Response und die Einhaltung regulatorischer Anforderungen nach ISO 27001, DSGVO, DORA und NIS2 um.

1.4 Diese Richtlinie stellt sicher, dass alle Systeme vertrauenswürdige Zeitquellen verwenden, manuelle Änderungen an Zeiteinstellungen verhindert werden und Abweichungen der Systemzeit rechtzeitig korrigiert werden.

2. Geltungsbereich

2.1 Diese Richtlinie gilt für:

2.1.1 alle unternehmenseigenen Systeme und Geräte, einschließlich Servern, Desktop-Systemen, Laptops, mobilen Geräten, Firewalls, Routern und virtuellen Maschinen

2.1.2 Remote- und Cloud-basierte Infrastrukturen, die im Betrieb genutzt werden, z. B. AWS, Microsoft 365 und SaaS-Plattformen

2.1.3 Systeme, die Ereignisprotokolle, Authentifizierungsaufzeichnungen oder Audit-Trails erzeugen oder speichern

2.1.4 alle Mitarbeitenden, Auftragnehmer, Lieferanten oder IT-Support-Dienstleister, die für die Konfiguration oder Wartung dieser Systeme verantwortlich sind

2.2 Die Richtlinie gilt auch für Bring-Your-Own-Device-(BYOD-)Endgeräte, die für den Zugriff auf Geschäftssysteme verwendet werden, sofern diese Endgeräte auditrelevante Daten speichern oder erzeugen.

3. Ziele

3.1 Sicherstellung, dass alle kritischen Systeme die Zeit automatisch mithilfe vertrauenswürdiger Network-Time-Protocol-(NTP-)Server oder gleichwertiger Mechanismen des Cloud-Anbieters synchronisieren

3.2 Verhinderung von Zeitabweichungen, die die Zuverlässigkeit oder Korrelation von Systemprotokollen bei Audits oder Sicherheitsuntersuchungen beeinträchtigen könnten

3.3 Ermöglichung der rechtzeitigen Erkennung und Korrektur von Zeitabweichungen außerhalb zulässiger Schwellenwerte

3.4 Aufrechterhaltung einer konsistenten Zeitstempelvergabe über alle Umgebungen hinweg, einschließlich On-Premises-, Cloud- und Remote-Umgebungen

3.5 Erfüllung technischer und rechtlicher Anforderungen an Integrität, Nachvollziehbarkeit und Nichtabstreitbarkeit von Aufzeichnungen und Ereignissen

4. Rollen und Verantwortlichkeiten

4.1 Geschäftsführung

4.1.1 genehmigt diese Richtlinie und stellt die organisationsweite Einhaltung sicher

4.1.2 überwacht regelmäßige Überprüfungen der Zeitgenauigkeit auf Systemebene sowie bestehender Umsetzungslücken

4.1.3 genehmigt Ausnahmen von der automatisierten Zeitsynchronisierung, sofern diese begründet und dokumentiert sind

4.2 IT-Support-Dienstleister / interne IT-Funktion

4.2.1 konfiguriert die Zeitsynchronisierung für alle unternehmenseigenen oder verwalteten Systeme

4.2.2 prüft, ob die tägliche oder planmäßige Synchronisierung ordnungsgemäß funktioniert

4.2.3 untersucht und behebt Ereignisse mit Zeitabweichungen, Synchronisierungsfehlern oder Problemen beim NTP-Zugriff

4.2.4 dokumentiert den Status der Zeitsynchronisierung im Rahmen monatlicher Systemzustandsprüfungen

[... 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 Planmäßige Überprüfung

9.1.1 Diese Richtlinie muss jährlich durch die Geschäftsführung, den IT-Support-Dienstleister und den Datenschutzkoordinator überprüft werden.

9.1.2 Bei der Überprüfung sind alle Protokolle und Berichte zum Status der Einhaltung der Zeitsynchronisierung zu berücksichtigen.

9.2 Anlassbezogene Aktualisierungen

9.2.1 Diese Richtlinie muss aktualisiert werden, wenn:

9.2.1.1 ein Systemausfall zu einer erheblichen Zeitabweichung führt

9.2.1.2 ein Audit Mängel bei der Zeitsynchronisierung aufdeckt

9.2.1.3 die Organisation neue Cloud-, hybride oder Virtualisierungsumgebungen einführt

9.2.1.4 rechtliche oder regulatorische Änderungen neue Anforderungen an die Integrität der Zeitführung einführen

9.3 Versionskontrolle und Kommunikation

9.3.1 Alle Aktualisierungen müssen versioniert und datiert werden.

9.3.2 Wesentliche Änderungen müssen dem gesamten technischen Personal mitgeteilt werden.

9.3.3 Frühere Versionen müssen für 3 Jahre zur Auditunterstützung aufbewahrt werden.

10. Zugehörige Richtlinien und Verknüpfungen

10.1 Diese Richtlinie ist zusammen mit den folgenden SME-Richtlinien anzuwenden:

10.1.1 P22S – Richtlinie zur Protokollierung und Überwachung: Stellt für die Nachvollziehbarkeit und forensische Korrelation eine konsistente Zeitstempelvergabe über alle Protokolle hinweg sicher.

10.1.2 P30S – Incident-Response-Richtlinie (P30): Beruht auf genauen Zeitstempeln, um Vorfälle zu rekonstruieren, Zeitachsen festzulegen und Entscheidungen über Benachrichtigungen zu unterstützen.

10.1.3 P17S – Richtlinie zu Datenschutz und Privatsphäre: Stellt sicher, dass Zugriffsprotokolle und zeitbezogene Abläufe der Datenverarbeitung mit Bezug zu personenbezogenen Daten korrekt sind und unter der DSGVO belastbar bleiben.

10.1.4 P12S – Richtlinie zum Asset-Management: Unterstützt die Identifizierung von Systemen, die synchronisiert werden müssen, insbesondere mobilen Geräten und Remote-Geräten.

10.1.5 P26S – Richtlinie zur Lieferantensicherheit: Stellt sicher, dass Lieferanten, die für die Organisation auf Daten zugreifen oder Daten protokollieren, vertraglich zur Verwendung synchronisierter Zeitverfahren verpflichtet sind.

11. Referenzstandards und Rahmenwerke

11.1 ISO/IEC 27001:

11.1.1 Klausel 8.1 – verlangt die Umsetzung von Kontrollen, die für einen sicheren Betrieb erforderlich sind, einschließlich Protokollierung und Zeitstempelvergabe.

11.2 ISO/IEC 27002:

11.2.1 Maßnahme 8.17 – empfiehlt synchronisierte Zeit für alle Systeme, die Protokolle erzeugen oder im Verbund betrieben werden.

11.3 NIST SP 800-53 Rev.5:

11.3.1 AU-8 – verlangt die Nutzung interner oder externer Zeitquellen für die Genauigkeit von Protokollzeitstempeln.

11.3.2 SC-45 – legt die Nutzung vertrauenswürdiger NTP-Quellen und die Verhinderung manueller Zeitänderungen in kritischen Systemen fest.

11.4 EU-DSGVO:

11.4.1 Artikel 5(1)(d) – verlangt Genauigkeit und Rechenschaftspflicht bei der Verarbeitung personenbezogener Daten, unterstützt durch synchronisierte Zeitstempel.

11.4.2 Artikel 32 – verlangt Sicherheitsmaßnahmen zur Sicherstellung der Datenintegrität, einschließlich konsistenter zeitlicher Protokollierung.

11.5 EU-NIS2-Richtlinie:

11.5.1 Artikel 21(2)(d) – verlangt Überwachungs- und Erkennungsfähigkeiten, unterstützt durch synchronisierte Systemprotokolle.

11.6 EU DORA:

11.6.1 Artikel 10 – fordert operative Resilienz und verlangt nachvollziehbare, mit Zeitstempeln versehene IKT-Vorfallsprotokolle.

11.6.2 Artikel 15 – verlangt von Dienstleistern die Führung genauer technischer Aufzeichnungen, einschließlich mit Zeitstempeln versehener Audit-Trails.

11.7 COBIT 2019:

11.7.1 DSS05.02 – betont die Integrität von Zeitstempeln für die Erkennung von und Reaktion auf Ereignisse.

11.7.2 MEA03.01 – verlangt eine nachweisgestützte Leistungsüberwachung, unterstützt durch genaue zeitlich synchronisierte Daten.