| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Fügen Sie hier den Namen der eingetragenen juristischen Person ein | | | | | | | |
| Dokumentnummer:<br>P23 | | | | | Dokumenttitel:<br>**Richtlinie zur Zeitsynchronisierung** | | | | | | | |
| Version:<br>1.0 | | Datum des Inkrafttretens:<br>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/Vorschrift | Klausel/Artikel | Kommentar |
|---|---|---|
| ISO/IEC 27001:2022 | Klausel 8 | - |
| ISO/IEC 27002:2022 | Maßnahme 8 | - |
| NIST SP 800-53 Rev.5 | SC-45, AU-8 | - |
| DSGVO | Artikel 32 | - |
| EU NIS2 | Artikel 21(2)(e) | - |
| EU DORA | Artikel 9, 10 | - |
| COBIT 2019 | DSS05.04, MEA03 | - |

**1. Zweck**

1.1 Zweck dieser Richtlinie ist es, sicherzustellen, dass alle Systeme, Anwendungen, Geräte und Cloud-Services der Organisation durch Synchronisierung mit festgelegten, vertrauenswürdigen Zeitquellen konsistente und genaue Zeiteinstellungen aufrechterhalten.

1.2 Eine genaue Zeitsynchronisierung ist wesentlich für eine verlässliche Protokollierung, sichere Kommunikation, Auditierbarkeit, Incident Response und forensische Untersuchungen. Abweichende Systemzeiten können zu nicht korrelierbaren Protokollen, fehlgeschlagener Authentifizierung und unvollständiger regulatorischer Berichterstattung führen.

1.3 Diese Richtlinie unterstützt ISO/IEC 27001 Anhang A, Maßnahme 8.17, sowie damit verbundene internationale Standards, indem sie Zeitgenauigkeit und die Erkennung von Zeitabweichungen in der gesamten IKT-Landschaft der Organisation verbindlich vorgibt.

**2. Geltungsbereich**

**2.1 Diese Richtlinie gilt für:**

2.1.1 sämtliche Infrastrukturkomponenten einschließlich Servern, Arbeitsplatzsystemen, Netzwerkgeräten, Firewalls und IoT-Systemen

2.1.2 virtuelle und Cloud-Umgebungen (z. B. AWS, Azure, Google Cloud)

2.1.3 alle Systeme, die an Protokollierung, Authentifizierung, Transaktionsverarbeitung oder der Korrelation von Sicherheitsereignissen beteiligt sind

2.1.4 interne Mitarbeitende, Auftragnehmer und externe IT-Dienstleister mit Verantwortung für zeitkritische Systeme

2.2 Systeme, die mit Zeitstempeln versehene Aufzeichnungen erzeugen oder verarbeiten, wie Protokolleinträge, Warnmeldungen, Aufzeichnungen über Benutzeraktivitäten oder forensische Nachweise, gelten als vom Geltungsbereich umfasst.

**3. Ziele**

3.1 Festlegung einer konsistenten, zentralen Architektur zur Zeitsynchronisierung unter Verwendung genehmigter NTP-Quellen oder gleichwertiger Mechanismen.

3.2 Sicherstellung, dass alle Systeme ihre Uhren in festgelegten Intervallen synchronisieren und dass Abweichungen erkannt und automatisch oder mit minimalem manuellem Eingriff korrigiert werden.

**3.3 Aufrechterhaltung der Uhrengenauigkeit in hybriden, lokalen und Cloud-basierten Umgebungen, um Folgendes zu ermöglichen:**

3.3.1 verlässliche Ereigniskorrelation und Incident Response

3.3.2 regulatorische Konformität mit Standards wie ISO 27001, DSGVO, NIS2 und DORA

3.3.3 Schutz vor Replay-Angriffen und zeitbasierten Authentifizierungsfehlern

3.4 Festlegung klarer Rollen, Verfahren für den Umgang mit Ausnahmen und Audit-Mechanismen zur Sicherstellung der Durchsetzung dieser Richtlinie.

3.5 Sicherstellung, dass zeitbezogene Anomalien protokolliert, mit Warnmeldungen versehen und bei Überschreitung von Toleranzwerten eskaliert werden.

**4. Rollen und Verantwortlichkeiten**

**4.1 Chief Information Security Officer (CISO)**

4.1.1 verantwortet diese Richtlinie und stellt die Ausrichtung an den operativen Kontrollen des ISMS sowie an regulatorischen Anforderungen sicher.

4.1.2 genehmigt die Auswahl organisationsweiter Zeitquellen und validiert Prozesse zur Berichterstattung über die Zeitsynchronisierung.

**4.2 Leitung Infrastrukturservices / Leitung Netzwerkengineering**

4.2.1 betreibt die primären und sekundären NTP-Server der Organisation oder die festgelegte Konfiguration der Zeitquellen.

4.2.2 stellt sicher, dass alle vernetzten Geräte und virtuellen Instanzen ihre Zeit in angemessenen Intervallen synchronisieren.

4.2.3 überwacht Protokolle zur Zeitsynchronisierung, Warnmeldungen zu Zeitabweichungen und Fehlerzustände.

[ ... 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 ist jährlich oder früher unter den folgenden Bedingungen zu überprüfen:**

9.1.1 Erkennung zeitbasierter Exploits oder Ausfälle der Protokollierung

9.1.2 Änderungen an der zentralen Zeitinfrastruktur (z. B. neue organisationsweite NTP-Server oder Protokollaktualisierungen)

9.1.3 Abweichungen der Zeitdrift auf Cloud-Plattformen oder regionale Serviceänderungen

9.1.4 Erkenntnisse aus Vorfällen, die eine Zeitabweichung als mitursächlichen Faktor identifizieren

9.2 Die Überprüfung ist durch die Leitung Infrastruktur zu koordinieren; erforderliche Beiträge kommen von SOC, Anwendungssicherheit und den für Compliance zuständigen Funktionen.

9.3 Überarbeitungen müssen im ISMS-Dokumentenregister dokumentiert und den betroffenen internen und externen Parteien kommuniziert werden.

9.4 Frühere Versionen der Richtlinie müssen sicher archiviert, versionskontrolliert und für Anfragen im Rahmen von Compliance- oder Rechtsaudits verfügbar gemacht werden.

**10. Verwandte Richtlinien und Verknüpfungen**

10.1 P1 – Informationssicherheitsrichtlinie. Legt den übergreifenden Auftrag fest, die Integrität und Nachvollziehbarkeit aller Informationssysteme sicherzustellen, wofür Zeitgenauigkeit eine Grundvoraussetzung ist.

10.2 P5 – Änderungsmanagement-Richtlinie. Regelt Änderungen an Systemkonfigurationen einschließlich Anpassungen von Zeitquellen und stellt eine ordnungsgemäße Dokumentation, Tests und Rollback-Pläne sicher.

10.3 P22 – Richtlinie zur Protokollierung und Überwachung. Ist unmittelbar auf synchronisierte Zeit angewiesen, um die Reihenfolge von Ereignissen, die Log-Korrelation und die Integrität von Vorfalluntersuchungen über unterschiedliche Systeme hinweg sicherzustellen.

10.4 P30 – Incident-Response-Richtlinie (P30). Stützt sich auf präzise Zeitstempel für forensische Untersuchungen, Vorfallszeitachsen und Nachweise der Beweismittelkette. Ungenaue Zeitangaben untergraben die Glaubwürdigkeit von Vorfallberichten.

10.5 P20 – Richtlinie zum Endpunktschutz / Malware-Richtlinie. Erfordert zeitgenaue Warnmeldungen und Verhaltensanalysen, um die Verbreitung von Schadsoftware, laterale Bewegungen und Anmeldeanomalien zu erkennen.

10.6 P6 – Risikomanagement-Richtlinie. Definiert Desynchronisierung als potenzielles betriebliches und forensisches Risiko und verlangt die in dieser Richtlinie festgelegten Kontrollen zur Minderung der Auswirkungen.

## 11. Referenzstandards und Rahmenwerke

### 11.1 ISO/IEC 27001

11.1.1 Klausel 8.1 – Betriebliche Planung und Steuerung: verlangt die Einbindung genauer technischer Kontrollen wie synchronisierter Systemuhren für eine verlässliche operative Ausführung.

### 11.2 ISO/IEC 27002:2022 – Maßnahme 8

11.2.1 Bekräftigt die Genauigkeit von Uhren und verlangt organisationsweite Konsistenz der Systemzeit, um Protokollvergleiche, Untersuchungen und die sichere Validierung von Transaktionen zu ermöglichen.

### 11.3 NIST SP 800-53 Rev.5

11.3.1 SC-45 – Systemzeitsynchronisierung: verlangt die Zeitsynchronisierung unter Verwendung maßgeblicher Quellen über alle Komponenten innerhalb einer Systemgrenze hinweg.

11.3.2 AU-8 – Zeitstempel: stellt sicher, dass Ereignisse korrekt mit Zeitstempeln versehen werden, und schafft Nachvollziehbarkeit für Audits und Incident Response.

### 11.4 DSGVO (2016/679)

11.4.1 Artikel 32 – Sicherheit der Verarbeitung: nennt Zeit nicht ausdrücklich, verlangt jedoch geeignete technische Maßnahmen, einschließlich Audit-Trails und Protokollen, deren Gültigkeit und Integrität inhärent von synchronisierten Zeitstempeln abhängen.

### 11.5 EU NIS2-Richtlinie (2022/2555)

11.5.1 Artikel 21(2)(e): verlangt Protokollierungs- und Erkennungsfähigkeiten, die für systemübergreifende Korrelation und rechtzeitige Reaktion eine genaue Zeitsynchronisierung voraussetzen.

### 11.6 EU DORA (2022/2554)

11.6.1 Artikel 9 – IKT-Risikomanagement: verlangt genaue Systemtelemetrie für die Risikoüberwachung und Anomalieerkennung, die von präziser Uhrensynchronisierung abhängt.

11.6.2 Artikel 10 – IKT-Business-Continuity: verlangt Kontrollen zur Sicherstellung der Systemintegrität bei Störungen, einschließlich zeitlich abgestimmter Ereignisaufzeichnungen.

### 11.7 COBIT 2019

11.7.1 DSS05.04 – Sicherheitsereignisse überwachen: verlangt die Integrität von Zeitstempeln für eine wirksame Log-Analyse und Bedrohungserkennung.

11.7.2 MEA03 – Einhaltung überwachen, evaluieren und beurteilen: Zeitsynchronisierung unterstützt genaue Compliance-Audits und Berichtszyklen.