					Indsæt navnet på den registrerede juridiske enhed her							
Dokumentnummer: P23S					Dokumenttitel: **Politik for tidssynkronisering**							
Version: 1.0		Ikrafttrædelsesdato: 01.01.2025			Dokumentejer:							
X	Politik		Standard		Procedure		Formular		Register		Andet	

Revisionshistorik				
Revisionsnummer	**Revisionsdato**	**Ændringer**	**Gennemgået af**	**Procesejer**

Godkendelser			
Navn	**Stilling**	**Dato**	**Underskrift**

Tilpasset relevante standarder og regler

Standard/regulering	Klausul/artikel	Kommentar
ISO/IEC 27001:2022	Klausul 8	Relevante kontrolkrav
ISO/IEC 27002:2022	Kontrol 8	Synkroniseret systemdrift
NIST SP 800-53 Rev.5	SC-45, AU-8	Betroede NTP-kilder og nøjagtighed af tidsstempler i logfiler
EU GDPR	Artikel 5(1)(d), 32	Nøjagtighed, ansvarlighed og integritet i personoplysninger understøttet af synkroniserede tidsstempler
EU NIS2	Artikel 21(2)(d)	Overvågnings- og detektionskapacitet understøttet af synkroniserede logfiler
EU DORA	Artikel 10, 15	Operationel robusthed og nøjagtige tekniske registreringer
COBIT 2019	DSS05.02, MEA03	Tidsstemplede hændelser og evidensbaseret overvågning

1. Formål

1.1 Denne politik fastsætter obligatoriske kontroller for at opretholde nøjagtig og synkroniseret tid på tværs af alle systemer, der lagrer, overfører eller behandler organisationens data.

1.2 Tidssynkronisering er afgørende for at sikre, at systemlogfiler er sporbare, at sikkerhedshændelser kan korreleres korrekt, og at bevismateriale kan anvendes ved retsmedicinske analyser eller juridisk gennemgang.

1.3 Organisationen håndhæver automatiseret tidssynkronisering som et grundlæggende krav til revisionsintegritet, hændelseshåndtering og efterlevelse af ISO 27001, GDPR, DORA og NIS2.

1.4 Denne politik sikrer, at alle systemer anvender betroede tidskilder, forhindrer manuel tilsidesættelse af tidsindstillinger og kræver rettidig korrektion af tidsafvigelser.

2. Omfang

2.1 Denne politik gælder for:

2.1.1 Alle virksomhedsejede systemer og enheder, herunder servere, stationære computere, bærbare computere, mobile enheder, firewalls, routere og virtuelle maskiner

2.1.2 Fjernhostede og cloudbaserede infrastrukturer, der anvendes i driften (f.eks. AWS, Microsoft 365, SaaS-platforme)

2.1.3 Systemer, der genererer eller lagrer hændelseslogfiler, autentifikationsoptegnelser eller revisionsspor

2.1.4 Enhver medarbejder, kontrahent, leverandør eller IT-supportudbyder, der er ansvarlig for at konfigurere eller vedligeholde disse systemer

2.2 Politikken gælder også for BYOD-endepunkter (Bring Your Own Device), der anvendes til adgang til forretningssystemer, forudsat at disse endepunkter lagrer eller genererer revisionsrelevante data.

3. Mål

3.1 Sikre, at alle kritiske systemer automatisk synkroniserer tid ved hjælp af betroede NTP-servere (Network Time Protocol) eller tilsvarende mekanismer fra cloududbyderen

3.2 Forebygge tidsafvigelser, der kan svække pålideligheden af eller korrelationen mellem systemlogfiler under revisioner eller sikkerhedsundersøgelser

3.3 Muliggøre rettidig detektion og korrektion af tidsafvigelser ud over acceptable tærskler

3.4 Opretholde ensartet tidsstempling på tværs af miljøer (on-premises, cloud og fjernmiljøer)

3.5 Opfylde tekniske og juridiske krav til integritet, sporbarhed og uafviselighed for registreringer og hændelser

4. Roller og ansvar

4.1 Direktør

4.1.1 Godkender denne politik og sikrer organisatorisk efterlevelse

4.1.2 Fører tilsyn med periodiske gennemgange af tidsnøjagtighed på systemniveau og mangler i implementeringen

4.1.3 Godkender undtagelser fra automatiseret tidssynkronisering, når disse er begrundede og dokumenterede

4.2 IT-supportudbyder / intern IT-funktion

4.2.1 Konfigurerer tidssynkronisering for alle virksomhedsejede eller administrerede systemer

4.2.2 Verificerer, at daglig eller planlagt synkronisering fungerer korrekt

4.2.3 Undersøger og afhjælper hændelser med tidsafvigelser, synkroniseringsfejl eller problemer med adgang til NTP

4.2.4 Dokumenterer status for tidssynkronisering som led i de månedlige kontroller af systemernes tilstand

[... Afsnit 4.3–8 er ikke inkluderet i denne forhåndsvisning. Køb det fulde dokument for at få adgang til det komplette indhold. ...]

9. Krav til gennemgang og opdatering

9.1 Planlagt gennemgang

9.1.1 Denne politik skal gennemgås årligt af direktør, IT-supportudbyderen og databeskyttelseskoordinatoren

9.1.2 Alle logfiler og statusrapporter om efterlevelse af tidssynkronisering skal indgå i gennemgangen

9.2 Opdateringer udløst af hændelser

9.2.1 Denne politik skal opdateres, hvis:

9.2.1.1 Et systemsvigt medfører væsentlig tidsafvigelse

9.2.1.2 En revision afdækker mangler i tidssynkroniseringen

9.2.1.3 Organisationen tager nye cloudbaserede, hybride eller virtualiserede miljøer i brug

9.2.1.4 Juridiske eller regulatoriske ændringer indfører nye krav til tidsintegritet

9.3 Versionsstyring og kommunikation

9.3.1 Alle opdateringer skal versionsstyres og dateres

9.3.2 Væsentlige ændringer skal kommunikeres til alt teknisk personale

9.3.3 Tidligere versioner skal opbevares i 3 år som revisionsdokumentation

10. Relaterede politikker og sammenhænge

10.1 Denne politik skal anvendes sammen med følgende SME-politikker:

10.1.1 P22S – Lognings- og overvågningspolitik: Sikrer ensartet tidsstempling på tværs af logfiler med henblik på sporbarhed og retsmedicinsk korrelation.

10.1.2 P30S – Politik for hændelseshåndtering: Er afhængig af nøjagtige tidsstempler for at rekonstruere hændelser, fastlægge tidslinjer og understøtte beslutninger om underretning.

10.1.3 P17S – Databeskyttelses- og privatlivspolitik: Sikrer, at adgangslogfiler og tidslinjer for datahåndtering, der omfatter personoplysninger, er nøjagtige og juridisk forsvarlige efter GDPR.

10.1.4 P12S – Politik for styring af aktiver: Understøtter identifikation af systemer, der kræver synkronisering, navnlig mobile enheder og fjernenheder.

10.1.5 P26S – Politik for sikkerhed hos tredjeparter og leverandører: Sikrer kontraktmæssigt, at leverandører, der tilgår eller logger data for organisationen, følger praksis for synkroniseret tid.

11. Referencestandarder og rammeværker

11.1 ISO/IEC 27001:

11.1.1 Klausul 8.1 – Kræver implementering af nødvendige kontroller for sikker drift, herunder logning og tidsstempling.

11.2 ISO/IEC 27002:

11.2.1 Kontrol 8.17 – Anbefaler synkroniseret tid for alle systemer, der producerer logfiler eller arbejder sammen.

11.3 NIST SP 800-53 Rev.5:

11.3.1 AU-8 – Kræver anvendelse af interne eller eksterne tidskilder for nøjagtige tidsstempler i logfiler.

11.3.2 SC-45 – Specificerer brugen af betroede NTP-kilder og forebyggelse af manuelle tidsændringer i kritiske systemer.

11.4 EU GDPR:

11.4.1 Artikel 5(1)(d) – Kræver nøjagtighed og ansvarlighed i behandlingen af personoplysninger, understøttet af synkroniserede tidsstempler.

11.4.2 Artikel 32 – Kræver sikkerhedsforanstaltninger, der sikrer dataintegritet, herunder ensartede tidsrammer for logning.

11.5 EU NIS2-direktivet:

11.5.1 Artikel 21(2)(d) – Kræver overvågnings- og detektionskapacitet understøttet af synkroniserede systemlogfiler.

11.6 EU DORA:

11.6.1 Artikel 10 – Kræver operationel robusthed, hvilket forudsætter sporbare og tidsstemplede logfiler for IKT-hændelser.

11.6.2 Artikel 15 – Kræver, at tjenesteudbydere opretholder nøjagtige tekniske registreringer, herunder tidsstemplede revisionsspor.

11.7 COBIT 2019:

11.7.1 DSS05.02 – Fremhæver integriteten af tidsstempler ved detektion af og respons på hændelser.

11.7.2 MEA03.01 – Kræver evidensbaseret overvågning af ydeevne, understøttet af nøjagtige og tidsmæssigt synkroniserede data.