					Indsæt navnet på den registrerede juridiske enhed her							
Dokumentnummer: P23					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 regulering

Standard/forordning	Klausul/artikel	Kommentar
ISO/IEC 27001:2022	Klausul 8	-
ISO/IEC 27002:2022	Kontrol 8	-
NIST SP 800-53 Rev. 5	SC-45, AU-8	-
EU GDPR	Artikel 32	-
EU NIS2	Artikel 21(2)(e)	-
EU DORA	Artikel 9, 10	-
COBIT 2019	DSS05.04, MEA	-

1. Formål

1.1 Formålet med denne politik er at sikre, at alle organisationens systemer, applikationer, enheder og cloudtjenester opretholder ensartede og nøjagtige tidsindstillinger ved at synkronisere med udpegede, betroede tidskilder.

1.2 Korrekt tidssynkronisering er afgørende for pålidelig logning, sikker kommunikation, revisionssporbarhed, hændelseshåndtering og it-forensiske undersøgelser. Uoverensstemmende tid kan medføre manglende logkorrelation, mislykket autentificering og ufuldstændig regulatorisk rapportering.

1.3 Denne politik understøtter ISO/IEC 27001, bilag A, kontrol 8.17 og relaterede internationale standarder ved at håndhæve tidsnøjagtighed og detektion af urafvigelser på tværs af organisationens it-miljø.

2. Omfang

2.1 Denne politik gælder for:

2.1.1 Alle infrastrukturkomponenter, herunder servere, arbejdsstationer, netværksenheder, firewalls og IoT-systemer

2.1.2 Virtuelle miljøer og cloudmiljøer, herunder AWS, Azure og Google Cloud

2.1.3 Alle systemer, der indgår i logning, autentificering, transaktionsbehandling eller korrelation af sikkerhedshændelser

2.1.4 Interne medarbejdere, konsulenter og tredjepartsleverandører med ansvar for tidsfølsomme systemer

2.2 Systemer, der genererer eller anvender tidsstemplede registreringer, såsom logposter, alarmer, registreringer af brugeraktivitet eller it-forensisk bevismateriale, er omfattet af denne politik.

3. Mål

3.1 At definere en ensartet, centraliseret arkitektur for tidssynkronisering ved brug af godkendte NTP-kilder eller tilsvarende.

3.2 At sikre, at alle systemer synkroniserer deres ure med fastsatte intervaller, og at enhver afvigelse opdages og korrigeres automatisk eller med minimal manuel indgriben.

3.3 At opretholde urnøjagtighed på tværs af hybride miljøer, on-premises-infrastruktur og cloudmiljøer for at muliggøre:

3.3.1 Pålidelig hændelseskorrelation og hændelseshåndtering

3.3.2 Overholdelse af standarder og regulering, herunder ISO 27001, GDPR, NIS2 og DORA

3.3.3 Beskyttelse mod replay-angreb og tidsbaserede fejl i autentificering

3.4 At etablere klare roller, procedurer for undtagelseshåndtering og revisionsmekanismer for at sikre håndhævelse af politikken.

3.5 At sikre, at tidsrelaterede anomalier logges, udløser alarmer og eskaleres, når de overskrider fastsatte tolerancer.

4. Roller og ansvar

4.1 Informationssikkerhedschef (CISO)

4.1.1 Er ansvarlig for denne politik og sikrer sammenhæng med ISMS'ets operationelle kontroller og regulatoriske krav.

4.1.2 Godkender valg af fælles tidskilder for organisationen og validerer processer for rapportering om tidssynkronisering.

4.2 Leder af infrastrukturtjenester / ledende netværksspecialist

4.2.1 Vedligeholder organisationens primære og sekundære NTP-servere eller den udpegede konfiguration af tidskilder.

4.2.2 Sikrer, at alle netværkstilsluttede enheder og virtuelle instanser synkroniserer tid med passende intervaller.

4.2.3 Overvåger logfiler for tidssynkronisering, alarmer om urafvigelser og fejltilstande.

[... 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 Denne politik skal gennemgås årligt eller tidligere under følgende forhold:

9.1.1 Detektion af tidsbaserede angreb eller fejl i logning

9.1.2 Ændringer i den centrale tidsinfrastruktur, herunder nye virksomhedsbaserede NTP-servere eller protokolopdateringer

9.1.3 Uoverensstemmelser i tidsafvigelser på cloudplatforme eller regionale ændringer i tjenester

9.1.4 Konstateringer efter hændelser, der identificerer tidsmæssig uoverensstemmelse som en medvirkende faktor

9.2 Gennemgangen skal koordineres af den infrastrukturansvarlige med påkrævet input fra SOC, applikationssikkerhed og interessenter inden for compliance.

9.3 Revisioner af politikken skal dokumenteres i ISMS'ets dokumentregister og kommunikeres til berørte interne interessenter og tredjeparter.

9.4 Historiske versioner af politikken skal arkiveres sikkert, være versionsstyrede og stilles til rådighed ved anmodninger om revision eller juridisk vurdering.

10. Relaterede politikker og sammenhænge

10.1 P1 – Informationssikkerhedspolitik. Fastlægger det overordnede mandat til at sikre integritet og sporbarhed i alle informationssystemer, hvor tidsnøjagtighed er et grundlæggende element.

10.2 P5 – Politik for ændringsstyring. Regulerer ændringer i systemkonfigurationer, herunder justeringer af tidskilder, og sikrer korrekt dokumentation, test og rollback-planer.

10.3 P22 – Politik for logning og overvågning. Er direkte afhængig af synkroniseret tid for at sikre hændelsessekvensering, logkorrelation og integritet i hændelsesundersøgelser på tværs af forskellige systemer.

10.4 P30 – Politik for hændelseshåndtering. Er afhængig af nøjagtige tidsstempler til it-forensiske undersøgelser, hændelsestidslinjer og chain of custody-bevismateriale. Unøjagtig tid underminerer troværdigheden af hændelsesrapporter.

10.5 P20 – Politik for endpoint-beskyttelse / malwarepolitik. Kræver tidsnøjagtig alarmering og adfærdsanalyse for at opdage spredning af malware, lateral bevægelse og adgangsanomalier.

10.6 P6 – Politik for risikostyring. Definerer behandling af desynkronisering som en potentiel driftsmæssig og it-forensisk risiko og kræver de kontroller, der er fastsat i denne politik, for at begrænse konsekvensen.

11. Referencestandarder og rammeværker

11.1 ISO/IEC 27001

11.1.1 Klausul 8.1 – operationel planlægning og styring: Kræver integration af nøjagtige tekniske kontroller såsom synkroniserede systemure for pålidelig operationel udførelse.

11.2 ISO/IEC 27002:2022 – Kontrol 8

11.2.1 Understreger urnøjagtighed og kræver organisatorisk ensartethed i systemtid for at understøtte sammenligning af logfiler, undersøgelser og sikker validering af transaktioner.

11.3 NIST SP 800-53 Rev. 5

11.3.1 SC-45 – tidssynkronisering af systemtid: Kræver tidssynkronisering med autoritative kilder på tværs af alle komponenter inden for et systems afgrænsning.

11.3.2 AU-8 – tidsstempler: Sikrer, at hændelser tidsstemples korrekt og giver sporbarhed til revision og hændelseshåndtering.

11.4 EU GDPR (2016/679)

11.4.1 Artikel 32 – behandlingssikkerhed: Henviser ikke eksplicit til tid, men kræver passende tekniske foranstaltninger, herunder revisionsspor og logfiler, som i praksis afhænger af synkroniserede tidsstempler for gyldighed og integritet.

11.5 EU NIS2-direktivet (2022/2555)

11.5.1 Artikel 21(2)(e): Kræver lognings- og detektionskapaciteter, som forudsætter korrekt tidssynkronisering til korrelation på tværs af systemer og rettidig respons.

11.6 EU DORA (2022/2554)

11.6.1 Artikel 9 – styring af IKT-risiko: Kræver nøjagtig systemtelemetri til risikoovervågning og anomalidetektion, hvilket afhænger af præcis synkronisering af systemure.

11.6.2 Artikel 10 – IKT-forretningskontinuitet: Kræver kontroller, der sikrer systemintegritet under driftsforstyrrelser, herunder tidsmæssigt afstemte hændelsesregistreringer.

11.7 COBIT 2019

11.7.1 DSS05.04 – Overvåg sikkerhedshændelser: Kræver integritet i tidsstempler for effektiv loganalyse og trusselsdetektion.

11.7.2 MEA03 – Overvåg, evaluer og vurder efterlevelse: Tidssynkronisering understøtter præcis efterlevelseskontrol og korrekte rapporteringscyklusser.