					Voer hier de naam van de geregistreerde rechtspersoon in							
Documentnummer: P23					Documenttitel: **Beleid inzake tijdsynchronisatie**							
Versie: 1.0		Ingangsdatum: 01.01.2025			Documenteigenaar:							
X	Beleid		Standaard		Procedure		Formulier		Register		Overig	

Revisiegeschiedenis				
Revisienummer	**Revisiedatum**	**Wijzigingen**	**Beoordeeld door**	**Proceseigenaar**

Goedkeuringen			
Naam	**Functie**	**Datum**	**Handtekening**

Afgestemd op normen en regelgeving

Norm/regelgeving	Clausule/artikel	Opmerking
ISO/IEC 27001:2022	Clausule 8	-
ISO/IEC 27002:2022	Beheersmaatregel 8	-
NIST SP 800-53 Rev.5	SC-45, AU-8	-
AVG	Artikel 32	-
EU NIS2	Artikel 21(2)(e)	-
EU DORA	Artikelen 9, 10	-
COBIT 2019	DSS05.04, MEA	-

1. Doel

1.1 Het doel van dit beleid is te waarborgen dat alle informatiesystemen, applicaties, apparaten en cloudgehoste diensten van de organisatie consistente en nauwkeurige tijdinstellingen hanteren door synchronisatie met aangewezen, vertrouwde tijdsbronnen.

1.2 Nauwkeurige tijdsynchronisatie is essentieel voor betrouwbare logging, beveiligde communicatie, audittrailtraceerbaarheid, incidentrespons en forensisch onderzoek. Niet-gesynchroniseerde tijd kan leiden tot niet-correlabele logboeken, mislukte authenticatie en onvolledige rapportage aan toezichthouders.

1.3 Dit beleid ondersteunt ISO/IEC 27001 Bijlage A, beheersmaatregel 8.17, en gerelateerde internationale normen door de nauwkeurigheid van de systeemtijd en de detectie van klokafwijkingen binnen de IT-omgeving van de organisatie af te dwingen.

2. Reikwijdte

2.1 Dit beleid is van toepassing op:

2.1.1 alle infrastructuurcomponenten, waaronder servers, werkstations, netwerkapparatuur, firewalls en IoT-systemen

2.1.2 virtuele omgevingen en cloudgehoste omgevingen (bijv. AWS, Azure, Google Cloud)

2.1.3 alle systemen die deelnemen aan logging, authenticatie, transactieverwerking of correlatie van beveiligingsgebeurtenissen

2.1.4 interne medewerkers, contractanten en externe dienstverleners met verantwoordelijkheid voor tijdkritische systemen

2.2 Systemen die van tijdstempels voorziene registraties genereren of gebruiken, zoals logboekvermeldingen, waarschuwingen, registraties van gebruikersactiviteiten of forensisch bewijsmateriaal, vallen binnen de reikwijdte.

3. Doelstellingen

3.1 Een consistente, gecentraliseerde architectuur voor tijdsynchronisatie vaststellen met gebruik van goedgekeurde NTP-bronnen of een gelijkwaardig mechanisme.

3.2 Waarborgen dat alle systemen hun systeemtijd op vastgestelde intervallen synchroniseren en dat elke afwijking automatisch of met minimale tussenkomst wordt gedetecteerd en gecorrigeerd.

3.3 De nauwkeurigheid van de systeemtijd handhaven in hybride omgevingen, on-premises infrastructuur en cloudgehoste omgevingen om het volgende mogelijk te maken:

3.3.1 betrouwbare gebeurteniscorrelatie en incidentrespons

3.3.2 naleving van normen zoals ISO 27001, AVG, NIS2 en DORA

3.3.3 bescherming tegen replay-aanvallen en tijdsgebonden authenticatiefouten

3.4 Duidelijke rollen, procedures voor uitzonderingsbeheer en auditmechanismen vaststellen om de handhaving van dit beleid te waarborgen.

3.5 Waarborgen dat tijdgerelateerde afwijkingen worden gelogd, dat waarschuwingen worden gegenereerd en dat escalatie plaatsvindt wanneer toleranties worden overschreden.

4. Rollen en verantwoordelijkheden

4.1 Chief Information Security Officer (CISO)

4.1.1 Is eigenaar van dit beleid en waarborgt afstemming met operationele beheersmaatregelen van het ISMS en wettelijke en regelgevende vereisten.

4.1.2 Keurt de selectie van tijdsbronnen voor de organisatie goed en valideert rapportageprocessen voor tijdsynchronisatie.

4.2 Manager Infrastructuurdiensten / Lead Netwerktechniek

4.2.1 Beheert de primaire en secundaire NTP-servers van de organisatie of de configuratie van de aangewezen tijdsbron.

4.2.2 Waarborgt dat alle netwerkgebonden apparaten en virtuele instanties de tijd op passende intervallen synchroniseren.

4.2.3 Bewaakt logboeken van tijdsynchronisatie, waarschuwingen over klokafwijkingen en foutcondities.

[... Secties 4.3–8 zijn niet opgenomen in dit voorbeeld. Koop het volledige document voor toegang tot de volledige inhoud. ...]

9. Eisen voor herziening en actualisering

9.1 Dit beleid moet jaarlijks worden herzien, of eerder onder de volgende omstandigheden:

9.1.1 detectie van tijdsgebonden exploits of storingen in logging

9.1.2 wijzigingen in de kerninfrastructuur voor tijdsvoorziening (bijv. nieuwe NTP-servers voor de organisatie of protocolupdates)

9.1.3 afwijkingen in klokdrift op cloudplatforms of regionale wijzigingen in dienstverlening

9.1.4 bevindingen na een incident waarbij onjuiste tijdsuitlijning als bijdragende factor is vastgesteld

9.2 De herziening moet worden gecoördineerd door de infrastructuurverantwoordelijke, met verplichte input van het SOC, applicatiebeveiliging en compliance-stakeholders.

9.3 Herzieningen moeten worden gedocumenteerd in het ISMS-documentenregister en worden gecommuniceerd aan betrokken interne en externe stakeholders.

9.4 Historische versies van het beleid moeten veilig worden gearchiveerd, onder versiebeheer worden gehouden en beschikbaar worden gesteld voor verzoeken in het kader van compliance of juridische audits.

10. Gerelateerde beleidsdocumenten en samenhang

10.1 P1 – Informatiebeveiligingsbeleid. Stelt het overkoepelende mandaat vast om de integriteit en traceerbaarheid van alle informatiesystemen te waarborgen, waarvoor nauwkeurige tijdsynchronisatie een basisvoorwaarde is.

10.2 P5 – Wijzigingsbeheerbeleid. Regelt wijzigingen in systeemconfiguraties, waaronder aanpassingen aan tijdsbronnen, en waarborgt passende documentatie, testen en rollbackplannen.

10.3 P22 – Logging- en monitoringbeleid. Is direct afhankelijk van gesynchroniseerde tijd om gebeurtenisvolgorde, logcorrelatie en de integriteit van incidentonderzoek over uiteenlopende systemen heen te waarborgen.

10.4 P30 – Incidentresponsbeleid (P30). Steunt op nauwkeurige tijdstempels voor forensisch onderzoek, incidenttijdlijnen en chain-of-custody-bewijsmateriaal. Onnauwkeurige tijd ondermijnt de geloofwaardigheid van incidentrapportages.

10.5 P20 – Beleid inzake endpointbescherming / malwarebeleid. Vereist tijdnauwkeurige waarschuwingen en gedragsanalyse om malwareverspreiding, laterale verplaatsing en afwijkingen in toegang te detecteren.

10.6 P6 – Beleid inzake risicobeheer. Definieert desynchronisatie als een potentieel operationeel en forensisch risico en vereist de in dit beleid vastgestelde beheersmaatregelen om de impact te beperken.

11. Referentienormen en -raamwerken

11.1 ISO/IEC 27001

11.1.1 Clausule 8.1 – Operationele planning en beheersing: vereist integratie van nauwkeurige technische beheersmaatregelen, zoals gesynchroniseerde systeemklokken, voor betrouwbare operationele uitvoering.

11.2 ISO/IEC 27002:2022 – Beheersmaatregel 8

11.2.1 Bekrachtigt de vereiste van nauwkeurige systeemtijd en schrijft organisatorische consistentie van systeemtijd voor om vergelijking van logboeken, onderzoek en veilige validatie van transacties mogelijk te maken.

11.3 NIST SP 800-53 Rev.5

11.3.1 SC-45 – Systeemtijdsynchronisatie: vereist tijdsynchronisatie met gezaghebbende bronnen voor alle componenten binnen een systeemgrens.

11.3.2 AU-8 – Tijdstempels: waarborgt dat gebeurtenissen van nauwkeurige tijdstempels worden voorzien en levert traceerbaarheid voor audit en incidentrespons.

11.4 AVG (2016/679)

11.4.1 Artikel 32 – Beveiliging van de verwerking: noemt tijd niet expliciet, maar schrijft passende technische maatregelen voor, waaronder audittrails en logboeken, die voor geldigheid en integriteit inherent afhankelijk zijn van gesynchroniseerde tijdstempels.

11.5 EU NIS2-richtlijn (2022/2555)

11.5.1 Artikel 21(2)(e): vereist logging- en detectiecapaciteiten die nauwkeurige tijdsynchronisatie veronderstellen voor correlatie tussen systemen en tijdige respons.

11.6 EU DORA (2022/2554)

11.6.1 Artikel 9 – ICT-risicomanagement: schrijft nauwkeurige systeemtelemetrie voor ten behoeve van risicobewaking en anomaliedetectie, wat afhankelijk is van nauwkeurige kloksynchronisatie.

11.6.2 Artikel 10 – ICT-bedrijfscontinuïteit: verplicht beheersmaatregelen die de integriteit van systemen tijdens verstoringen waarborgen, waaronder in de tijd uitgelijnde gebeurtenisregistraties.

11.7 COBIT 2019

11.7.1 DSS05.04 – Beveiligingsgebeurtenissen bewaken: vereist integriteit van tijdstempels voor doeltreffende loganalyse en dreigingsdetectie.

11.7.2 MEA03 – Naleving monitoren, evalueren en assesseren: tijdsynchronisatie ondersteunt nauwkeurige compliance-audits en rapportagecycli.