					Voer hier de naam van de geregistreerde rechtspersoon in							
Documentnummer: P23S					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	Relevante vereisten voor beheersmaatregelen
ISO/IEC 27002:2022	Beheersmaatregel 8	Gesynchroniseerde systeemwerking
NIST SP 800-53 Rev.5	SC-45, AU-8	Vertrouwde NTP en nauwkeurigheid van tijdstempels in logbestanden
AVG	Artikelen 5(1)(d), 32	Nauwkeurigheid, verantwoordingsplicht en integriteit van persoonsgegevens met gesynchroniseerde tijdstempels
NIS2-richtlijn	Artikel 21(2)(d)	Mogelijkheden voor monitoring en detectie, ondersteund door gesynchroniseerde logbestanden
DORA	Artikelen 10, 15	Operationele weerbaarheid en nauwkeurige technische registraties
COBIT 2019	DSS05.02, MEA03	Tijdgestempelde gebeurtenissen en op bewijsmateriaal gebaseerde monitoring

1. Doel

1.1 Dit beleid stelt verplichte beheersmaatregelen vast voor het handhaven van nauwkeurige, gesynchroniseerde tijd op alle systemen die organisatiegegevens opslaan, verzenden of verwerken.

1.2 Tijdsynchronisatie is essentieel om te waarborgen dat systeemlogbestanden traceerbaar zijn, beveiligingsincidenten nauwkeurig kunnen worden gecorreleerd en bewijsmateriaal betrouwbaar is tijdens forensisch onderzoek of juridische toetsing.

1.3 De organisatie verplicht geautomatiseerde tijdsynchronisatie als basisvereiste voor auditintegriteit, incidentrespons en naleving van ISO 27001, de AVG, DORA en NIS2.

1.4 Dit beleid waarborgt dat alle systemen gebruikmaken van vertrouwde tijdsbronnen, voorkomt handmatige overschrijving van tijdsinstellingen en vereist tijdige correctie van klokafwijkingen.

2. Reikwijdte

2.1 Dit beleid is van toepassing op:

2.1.1 Alle systemen en apparaten die eigendom zijn van de organisatie, waaronder servers, desktops, laptops, mobiele apparaten, firewalls, routers en virtuele machines

2.1.2 Externe en in de cloud gehoste infrastructuur die binnen de bedrijfsvoering wordt gebruikt (bijvoorbeeld AWS, Microsoft 365, SaaS-platforms)

2.1.3 Systemen die gebeurtenislogboeken, authenticatieregistraties of audittrails genereren of opslaan

2.1.4 Iedere medewerker, opdrachtnemer, leverancier of IT-supportverlener die verantwoordelijk is voor het configureren of onderhouden van deze systemen

2.2 Dit beleid is ook van toepassing op Bring Your Own Device (BYOD)-eindpunten die worden gebruikt voor toegang tot bedrijfssystemen, voor zover deze eindpunten auditrelevante gegevens opslaan of genereren.

3. Doelstellingen

3.1 Waarborgen dat alle kritieke systemen de tijd automatisch synchroniseren met vertrouwde Network Time Protocol (NTP)-servers of gelijkwaardige mechanismen van cloudproviders

3.2 Tijdsafwijkingen voorkomen die de betrouwbaarheid of correlatie van systeemlogbestanden tijdens audits of beveiligingsonderzoeken kunnen ondermijnen

3.3 Tijdige detectie en correctie van tijdsafwijkingen boven aanvaardbare drempelwaarden mogelijk maken

3.4 Consistente tijdstempeling handhaven in alle omgevingen (on-premises, cloud en extern)

3.5 Voldoen aan technische en juridische vereisten voor integriteit, traceerbaarheid en onweerlegbaarheid van registraties en gebeurtenissen

4. Rollen en verantwoordelijkheden

4.1 Algemeen directeur

4.1.1 Keurt dit beleid goed en waarborgt de naleving binnen de organisatie

4.1.2 Houdt toezicht op periodieke beoordelingen van de nauwkeurigheid van systeemtijd en op implementatiehiaten

4.1.3 Keurt uitzonderingen op geautomatiseerde tijdsynchronisatie goed, indien deze gerechtvaardigd en gedocumenteerd zijn

4.2 IT-supportverlener / interne IT-functie

4.2.1 Configureert tijdsynchronisatie voor alle systemen die eigendom zijn van de organisatie of door haar worden beheerd

4.2.2 Verifieert dat dagelijkse of geplande synchronisatie correct functioneert

4.2.3 Onderzoekt en verhelpt gebeurtenissen met tijdsafwijkingen, mislukte synchronisatie of problemen met NTP-toegang

4.2.4 Documenteert de status van tijdsynchronisatie als onderdeel van maandelijkse systeemcontroles

[... 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 Geplande beoordeling

9.1.1 Dit beleid moet jaarlijks worden beoordeeld door de algemeen directeur, de IT-supportverlener en de privacycoördinator

9.1.2 Alle logbestanden en statusrapportages over naleving van tijdsynchronisatie moeten bij de beoordeling worden betrokken

9.2 Triggergebaseerde actualisaties

9.2.1 Dit beleid moet worden bijgewerkt indien:

9.2.1.1 Een systeemfout leidt tot een significante tijdsafwijking

9.2.1.2 Een audit tekortkomingen in tijdsynchronisatie aan het licht brengt

9.2.1.3 De organisatie nieuwe cloud-, hybride of virtualisatieomgevingen invoert

9.2.1.4 Juridische of regelgevende wijzigingen nieuwe vereisten voor tijdsintegriteit introduceren

9.3 Versiebeheer en communicatie

9.3.1 Alle actualisaties moeten onder versiebeheer worden geplaatst en van een datum worden voorzien

9.3.2 Majeure wijzigingen moeten aan al het technisch personeel worden gecommuniceerd

9.3.3 Vorige versies moeten gedurende 3 jaar worden bewaard ter ondersteuning van audits

10. Gerelateerde beleidslijnen en samenhang

10.1 Dit beleid moet worden toegepast in samenhang met de volgende mkb-beleidslijnen:

10.1.1 P22S – Logging- en monitoringbeleid: Waarborgt consistente tijdstempeling in logbestanden voor traceerbaarheid en forensische correlatie.

10.1.2 P30S – Incidentresponsbeleid: Is afhankelijk van nauwkeurige tijdstempels om incidenten te reconstrueren, tijdlijnen vast te stellen en meldingsbesluiten te onderbouwen.

10.1.3 P17S – Beleid inzake gegevensbescherming en privacy: Waarborgt dat toegangslogbestanden en tijdlijnen voor gegevensverwerking met betrekking tot persoonsgegevens nauwkeurig zijn en onder de AVG standhouden.

10.1.4 P12S – Beleid inzake beheer van bedrijfsmiddelen: Ondersteunt de identificatie van systemen die synchronisatie vereisen, in het bijzonder mobiele en externe apparaten.

10.1.5 P26S – Beleid inzake beveiliging van derden en leveranciers: Waarborgt contractueel dat leveranciers die voor de organisatie gegevens benaderen of loggen gesynchroniseerde tijdsprocedures volgen.

11. Referentienormen en -raamwerken

11.1 ISO/IEC 27001:

11.1.1 Clausule 8.1 – Vereist de implementatie van beheersmaatregelen die nodig zijn voor veilige bedrijfsvoering, waaronder logging en tijdstempeling.

11.2 ISO/IEC 27002:

11.2.1 Beheersmaatregel 8.17 – Beveelt gesynchroniseerde tijd aan voor alle systemen die logbestanden produceren of gezamenlijk functioneren.

11.3 NIST SP 800-53 Rev.5:

11.3.1 AU-8 – Vereist het gebruik van interne of externe tijdsbronnen voor nauwkeurige tijdstempels in logbestanden.

11.3.2 SC-45 – Schrijft het gebruik van vertrouwde NTP-bronnen voor en het voorkomen van handmatige tijdswijzigingen in kritieke systemen.

11.4 AVG:

11.4.1 Artikel 5(1)(d) – Vereist nauwkeurigheid en verantwoordingsplicht bij de verwerking van persoonsgegevens, ondersteund door gesynchroniseerde tijdstempels.

11.4.2 Artikel 32 – Vereist beveiligingsmaatregelen die de integriteit van gegevens waarborgen, waaronder consistente tijdvensters voor logging.

11.5 NIS2-richtlijn:

11.5.1 Artikel 21(2)(d) – Vereist mogelijkheden voor monitoring en detectie, ondersteund door gesynchroniseerde systeemlogbestanden.

11.6 DORA:

11.6.1 Artikel 10 – Vereist operationele weerbaarheid, met traceerbare en van tijdstempels voorziene logbestanden van ICT-incidenten.

11.6.2 Artikel 15 – Vereist dat dienstverleners nauwkeurige technische registraties bijhouden, waaronder audittrails met tijdstempels.

11.7 COBIT 2019:

11.7.1 DSS05.02 – Benadrukt de integriteit van tijdstempels voor het detecteren van en reageren op gebeurtenissen.

11.7.2 MEA03.01 – Vereist op bewijsmateriaal gebaseerde prestatiemonitoring, ondersteund door nauwkeurige tijdgesynchroniseerde gegevens.