					Ange namnet på den registrerade juridiska personen här							
Dokumentnummer: P23					Dokumenttitel: **Policy för tidssynkronisering**							
Version: 1.0		Ikraftträdandedatum: 01.01.2025			Dokumentägare:							
X	Policy		Standard		Rutin		Formulär		Register		Övrigt	

Revisionshistorik				
Revisionsnummer	**Revisionsdatum**	**Ändringar**	**Granskad av**	**Processägare**

Godkännanden			
Namn	**Titel**	**Datum**	**Underskrift**

Ansluten till standarder och regelverk

Standard/regelverk	Klausul/artikel	Kommentar
ISO/IEC 27001:2022	Klausul 8	-
ISO/IEC 27002:2022	Kontroll 8	-
NIST SP 800-53 Rev. 5	SC-45, AU-8	-
EU:s dataskyddsförordning (GDPR)	Artikel 32	-
EU:s NIS2-direktiv	Artikel 21.2 e	-
EU:s DORA-förordning	Artiklarna 9, 10	-
COBIT 2019	DSS05.04, MEA	-

1. Syfte

1.1 Syftet med denna policy är att säkerställa att samtliga av organisationens system, applikationer, enheter och molntjänster upprätthåller enhetliga och korrekta tidsinställningar genom synkronisering mot utsedda och betrodda tidskällor.

1.2 Korrekt tidssynkronisering är avgörande för tillförlitlig loggning, säker kommunikation, spårbarhet vid revision, incidenthantering och forensiska utredningar. Felaktigt synkroniserad tid kan leda till att loggar inte kan korreleras, att autentisering misslyckas och att regulatorisk rapportering blir ofullständig.

1.3 Denna policy stödjer ISO/IEC 27001 bilaga A, kontroll 8.17, och relaterade internationella standarder genom att säkerställa tidsnoggrannhet och detektering av klockdrift i organisationens IT-miljö.

2. Omfattning

2.1 Denna policy gäller för:

2.1.1 Alla infrastrukturkomponenter, inklusive servrar, arbetsstationer, nätverksenheter, brandväggar och IoT-system

2.1.2 Virtuella miljöer och molnmiljöer (t.ex. AWS, Azure, Google Cloud)

2.1.3 Alla system som deltar i loggning, autentisering, transaktionsbehandling eller korrelation av säkerhetshändelser

2.1.4 Interna medarbetare, entreprenörer och tredjepartsleverantörer med ansvar för tidskritiska system

2.2 System som genererar eller använder tidsstämplade poster, såsom loggposter, larm, användningsloggar eller forensisk bevisning, omfattas av denna policy.

3. Mål

3.1 Fastställa en enhetlig och centraliserad arkitektur för tidssynkronisering med godkända NTP-källor eller likvärdiga lösningar.

3.2 Säkerställa att alla system synkroniserar sina klockor med fastställda intervall samt att eventuell drift upptäcks och korrigeras automatiskt eller med minimal manuell insats.

3.3 Upprätthålla korrekt tid i hybrida miljöer, både lokalt och i molnmiljöer, för att möjliggöra:

3.3.1 Tillförlitlig händelsekorrelation och incidenthantering

3.3.2 Regelefterlevnad i förhållande till standarder såsom ISO 27001, GDPR, NIS2 och DORA

3.3.3 Skydd mot återspelningsattacker och tidsbaserade autentiseringsfel

3.4 Fastställa tydliga roller, rutiner för undantagshantering och revisionsmekanismer för att säkerställa efterlevnad av policyn.

3.5 Säkerställa att tidsrelaterade avvikelser loggas, genererar larm och eskaleras när de överskrider fastställda toleransvärden.

4. Roller och ansvar

4.1 Informationssäkerhetschef (CISO)

4.1.1 Äger denna policy och säkerställer anpassning till operativa kontroller inom ISMS samt regulatoriska krav.

4.1.2 Godkänner organisationens tidskällor och validerar processer för rapportering av tidssynkronisering.

4.2 Chef för infrastrukturtjänster / ledande nätverksingenjör

4.2.1 Förvaltar organisationens primära och sekundära NTP-servrar eller annan utsedd konfiguration för tidskällor.

4.2.2 Säkerställer att alla nätverksanslutna enheter och virtuella instanser synkroniserar tid med lämpliga intervall.

4.2.3 Övervakar loggar för tidssynkronisering, larm om klockdrift och feltillstånd.

[... Avsnitt 4.3–8 ingår inte i denna förhandsvisning. Köp det fullständiga dokumentet för att få tillgång till hela innehållet. ...]

9. Krav för granskning och uppdatering

9.1 Denna policy ska granskas årligen, eller tidigare under följande förutsättningar:

9.1.1 Detektering av tidsbaserade angrepp eller loggningsfel

9.1.2 Förändringar i den centrala tidsinfrastrukturen (t.ex. nya NTP-servrar för organisationen eller protokolluppdateringar)

9.1.3 Avvikelser i klockdrift på molnplattformar eller regionala förändringar i tjänster

9.1.4 Efterincidentgranskning som identifierar felaktig tidsjustering som en bidragande faktor

9.2 Granskningen ska samordnas av infrastrukturansvarig, med nödvändig medverkan från SOC, applikationssäkerhet och intressenter inom regelefterlevnad.

9.3 Revideringar ska dokumenteras i ISMS-dokumentregistret och kommuniceras till berörda interna intressenter och tredje parter.

9.4 Historiska versioner av policyn ska arkiveras säkert, versionshanteras och göras tillgängliga vid begäran om granskning inom regelefterlevnad eller juridisk revision.

10. Relaterade policyer och kopplingar

10.1 P1 – Informationssäkerhetspolicy. Fastställer det övergripande kravet att säkerställa riktighet och spårbarhet i alla informationssystem, där tidsnoggrannhet är grundläggande.

10.2 P5 – Ändringshanteringspolicy. Reglerar ändringar i systemkonfigurationer, inklusive justeringar av tidskällor, och säkerställer korrekt dokumentation, testning och återgångsplaner.

10.3 P22 – Loggnings- och övervakningspolicy. Är direkt beroende av synkroniserad tid för att säkerställa händelsesekvensering, loggkorrelation och korrekt incidentutredning i olika system.

10.4 P30 – Incidenthanteringspolicy. Är beroende av korrekta tidsstämplar för forensiska utredningar, incidenttidslinjer och dokumentation av beviskedjan. Felaktig tid undergräver incidentrapporters trovärdighet.

10.5 P20 – Policy för endpointskydd / skadlig kod. Kräver korrekt tidsättning av larm och beteendeanalys för att upptäcka spridning av skadlig kod, lateral förflyttning och avvikelser i åtkomst.

10.6 P6 – Riskhanteringspolicy. Definierar desynkronisering som en potentiell operativ och forensisk risk och kräver de kontroller som anges i denna policy för att begränsa konsekvensen.

11. Referensstandarder och ramverk

11.1 ISO/IEC 27001

11.1.1 Klausul 8.1 – Operativ planering och styrning: Kräver integrering av korrekta tekniska kontroller, såsom synkroniserade systemklockor, för tillförlitligt operativt genomförande.

11.2 ISO/IEC 27002:2022 – Kontroll 8

11.2.1 Förstärker kravet på korrekt systemtid och kräver organisatorisk enhetlighet i systemtid för att möjliggöra loggjämförelse, utredning och säker validering av transaktioner.

11.3 NIST SP 800-53 Rev. 5

11.3.1 SC-45 – Tidssynkronisering för system: Kräver tidssynkronisering med auktoritativa källor för alla komponenter inom ett systems kontrollgräns.

11.3.2 AU-8 – Tidsstämplar: Säkerställer att händelser förses med korrekta tidsstämplar och möjliggör spårbarhet för revision och incidenthantering.

11.4 EU:s dataskyddsförordning (GDPR) (2016/679)

11.4.1 Artikel 32 – Säkerhet i behandlingen: Även om tid inte uttryckligen nämns krävs lämpliga tekniska åtgärder, inklusive revisionsspår och loggar, som i praktiken är beroende av synkroniserade tidsstämplar för giltighet och riktighet.

11.5 EU:s NIS2-direktiv (2022/2555)

11.5.1 Artikel 21.2 e: Kräver loggnings- och detekteringsförmåga som förutsätter korrekt tidssynkronisering för korrelation mellan system och snabb respons.

11.6 EU:s DORA-förordning (2022/2554)

11.6.1 Artikel 9 – IKT-riskhantering: Kräver korrekta telemetridata från system för riskövervakning och anomalidetektering, vilket är beroende av exakt tidssynkronisering.

11.6.2 Artikel 10 – IKT-verksamhetskontinuitet: Kräver kontroller som säkerställer systemintegritet vid störningar, inklusive tidssynkroniserade händelseposter.

11.7 COBIT 2019

11.7.1 DSS05.04 – Övervaka säkerhetshändelser: Kräver integritet i tidsstämplar för effektiv logganalys och hotdetektering.

11.7.2 MEA03 – Övervaka, utvärdera och bedöma efterlevnad: Tidssynkronisering stödjer korrekt granskning av efterlevnad och rapporteringscykler.