					Ange namnet på den registrerade juridiska personen här							
Dokumentnummer: P23S					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	Relevanta kontrollkrav
ISO/IEC 27002:2022	Kontroll 8	Synkroniserad systemdrift
NIST SP 800-53 Rev.5	SC-45, AU-8	Betrodda NTP-källor och korrekta tidsstämplar i loggar
EU:s GDPR	Artiklarna 5.1 d och 32	Korrekthet, ansvarsskyldighet och riktighet för personuppgifter med synkroniserade tidsstämplar
EU:s NIS2-direktiv	Artikel 21.2 d	Övervaknings- och detekteringsförmåga med stöd av synkroniserade loggar
EU:s DORA-förordning	Artiklarna 10 och 15	Operativ resiliens och korrekta tekniska underlag
COBIT 2019	DSS05.02, MEA03	Tidsstämplade händelser och övervakning baserad på underlag

1. Syfte

1.1 Denna policy fastställer obligatoriska kontroller för att upprätthålla korrekt och synkroniserad tid i alla system som lagrar, överför eller behandlar organisationens data.

1.2 Tidssynkronisering är nödvändig för att säkerställa att systemloggar är spårbara, att säkerhetsincidenter kan korreleras korrekt och att underlag kan användas för forensisk analys eller rättslig granskning.

1.3 Organisationen ska tillämpa automatiserad tidssynkronisering som ett grundläggande krav för revisionsintegritet, incidenthantering och regelefterlevnad enligt ISO 27001, GDPR, DORA och NIS2.

1.4 Denna policy säkerställer att alla system använder betrodda tidskällor, förhindrar manuell åsidosättning av tidsinställningar och kräver att klockdrift korrigeras utan dröjsmål.

2. Omfattning

2.1 Denna policy gäller för:

2.1.1 Alla företagsägda system och enheter, inklusive servrar, stationära datorer, bärbara datorer, mobila enheter, brandväggar, routrar och virtuella maskiner

2.1.2 Fjärransluten och molnbaserad infrastruktur som används i verksamheten, till exempel AWS, Microsoft 365 och SaaS-plattformar

2.1.3 System som genererar eller lagrar händelseloggar, autentiseringsuppgifter eller revisionsspår

2.1.4 Alla anställda, entreprenörer, leverantörer eller IT-supportleverantörer som ansvarar för att konfigurera eller underhålla dessa system

2.2 Policyn gäller även för BYOD-enheter som används för åtkomst till verksamhetens system, förutsatt att dessa enheter lagrar eller genererar data som är relevanta för revision.

3. Mål

3.1 Säkerställa att alla kritiska system automatiskt synkroniserar tid med hjälp av betrodda NTP-servrar (Network Time Protocol) eller likvärdiga mekanismer från molnleverantörer

3.2 Förhindra tidsavvikelser som kan undergräva tillförlitligheten i eller korrelationen mellan systemloggar vid revisioner eller säkerhetsutredningar

3.3 Möjliggöra snabb upptäckt och korrigering av tidsdrift som överskrider godtagna tröskelvärden

3.4 Upprätthålla enhetlig tidsstämpling i alla miljöer, lokalt, i molnmiljöer och vid fjärranslutning

3.5 Uppfylla tekniska och rättsliga krav avseende riktighet, spårbarhet och oavvislighet för underlag och händelser

4. Roller och ansvar

4.1 Verkställande chef (GM)

4.1.1 Godkänner denna policy och säkerställer efterlevnad i organisationen

4.1.2 Utövar tillsyn över periodiska granskningar av korrekt tid på systemnivå och identifierade brister i genomförandet

4.1.3 Godkänner undantag från automatiserad tidssynkronisering när detta är motiverat och dokumenterat

4.2 IT-supportleverantör / intern IT-funktion

4.2.1 Konfigurerar tidssynkronisering för alla företagsägda eller hanterade system

4.2.2 Verifierar dagligen eller enligt fastställt schema att synkroniseringen fungerar korrekt

4.2.3 Utreder och åtgärdar händelser med tidsdrift, misslyckad synkronisering eller problem med åtkomst till NTP

4.2.4 Dokumenterar status för tidssynkronisering som en del av månatliga kontroller av systemhälsa

[... 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 Planerad granskning

9.1.1 Denna policy ska granskas årligen av den verkställande chefen, IT-supportleverantören och integritetssamordnaren

9.1.2 Alla loggar och statusrapporter för efterlevnad av tidssynkronisering ska beaktas vid granskningen

9.2 Uppdateringar vid utlösande händelser

9.2.1 Denna policy ska uppdateras om:

9.2.1.1 Ett systemfel leder till betydande tidsdrift

9.2.1.2 En revision identifierar brister i tidssynkronisering

9.2.1.3 Organisationen inför nya molnmiljöer, hybrida miljöer eller virtualiseringsmiljöer

9.2.1.4 Rättsliga eller regulatoriska ändringar medför nya krav på tidsintegritet

9.3 Versionshantering och kommunikation

9.3.1 Alla uppdateringar ska versionshanteras och dateras

9.3.2 Väsentliga ändringar ska kommuniceras till all teknisk personal

9.3.3 Tidigare versioner ska bevaras i tre år som stöd för revision

10. Relaterade policyer och kopplingar

10.1 Denna policy ska tillämpas tillsammans med följande SME-policyer:

10.1.1 P22S – Loggnings- och övervakningspolicy: Säkerställer enhetlig tidsstämpling i loggar för spårbarhet och forensisk korrelation.

10.1.2 P30S – Policy för incidenthantering: Bygger på korrekta tidsstämplar för att återskapa incidenter, fastställa tidslinjer och stödja beslut om avisering.

10.1.3 P17S – Policy för dataskydd och integritet: Säkerställer att åtkomstloggar och tidslinjer för datahantering som omfattar personuppgifter är korrekta och försvarbara enligt GDPR.

10.1.4 P12S – Policy för tillgångshantering: Stödjer identifiering av system som kräver synkronisering, särskilt mobila enheter och enheter för distansarbete.

10.1.5 P26S – Policy för tredjeparts- och leverantörssäkerhet: Säkerställer genom avtal att leverantörer som har åtkomst till eller loggar organisationens data följer synkroniserad tidspraxis.

11. Referensstandarder och ramverk

11.1 ISO/IEC 27001:

11.1.1 Klausul 8.1 – Kräver genomförande av kontroller som behövs för säker drift, inklusive loggning och tidsstämpling.

11.2 ISO/IEC 27002:

11.2.1 Kontroll 8.17 – Rekommenderar synkroniserad tid för alla system som producerar loggar eller samverkar i drift.

11.3 NIST SP 800-53 Rev.5:

11.3.1 AU-8 – Kräver användning av interna eller externa tidskällor för korrekta tidsstämplar i loggar.

11.3.2 SC-45 – Anger användning av betrodda NTP-källor och förhindrande av manuella tidsändringar i kritiska system.

11.4 EU:s GDPR:

11.4.1 Artikel 5.1 d – Kräver korrekthet och ansvarsskyldighet vid behandling av personuppgifter, med stöd av synkroniserade tidsstämplar.

11.4.2 Artikel 32 – Kräver säkerhetsåtgärder som säkerställer uppgifternas riktighet, vilket omfattar enhetliga tidsramar för loggning.

11.5 EU:s NIS2-direktiv:

11.5.1 Artikel 21.2 d – Kräver förmåga till övervakning och detektering, med stöd av synkroniserade systemloggar.

11.6 EU:s DORA-förordning:

11.6.1 Artikel 10 – Kräver operativ resiliens, vilket förutsätter spårbara och tidsstämplade loggar över IKT-incidenter.

11.6.2 Artikel 15 – Kräver att tjänsteleverantörer upprätthåller korrekta tekniska underlag, inklusive tidsstämplade revisionsspår.

11.7 COBIT 2019:

11.7.1 DSS05.02 – Betonar integriteten i tidsstämplar för detektering av och respons på händelser.

11.7.2 MEA03.01 – Kräver prestationsövervakning baserad på underlag, med stöd av korrekt tidssynkroniserade data.