					Sem vložte název registrované právnické osoby							
Číslo dokumentu: P23S					Název dokumentu: **Politika synchronizace času**							
Verze: 1.0		Datum účinnosti: 01.01.2025			Vlastník dokumentu:							
X	Politika		Standard		Postup		Formulář		Registr		Jiné	

Historie revizí				
Číslo revize	**Datum revize**	**Změny**	**Přezkoumal**	**Vlastník procesu**

Schválení			
Jméno	**Funkce**	**Datum**	**Podpis**

V souladu s normami a právními předpisy

Norma/právní předpis	Kapitola/článek	Komentář
ISO/IEC 27001:2022	Kapitola 8	Relevantní požadavky na opatření
ISO/IEC 27002:2022	Opatření 8	Synchronizovaný provoz systémů
NIST SP 800-53 Rev.5	SC-45, AU-8	Důvěryhodné NTP a přesnost časových razítek v protokolech
GDPR	Články 5(1)(d), 32	Přesnost, odpovědnost a integrita při zpracování osobních údajů se synchronizovanými časovými razítky
směrnice NIS2	Článek 21(2)(d)	Schopnosti monitorování a detekce podporované synchronizovanými protokoly
nařízení DORA	Články 10, 15	Provozní odolnost a přesné technické záznamy
COBIT 2019	DSS05.02, MEA03	Události s časovým razítkem a monitorování založené na důkazech

1. Účel

1.1 Tato politika stanoví povinná opatření k zajištění přesného a synchronizovaného času ve všech systémech, které ukládají, přenášejí nebo zpracovávají data organizace.

1.2 Synchronizace času je nezbytná pro zajištění dohledatelnosti systémových protokolů, přesné korelace bezpečnostních incidentů a spolehlivosti důkazů při forenzní analýze nebo právním přezkumu.

1.3 Organizace uplatňuje automatizovanou synchronizaci času jako základní požadavek pro integritu auditu, reakci na incidenty a soulad s požadavky ISO 27001, GDPR, DORA a NIS2.

1.4 Tato politika zajišťuje, aby všechny systémy používaly důvěryhodné časové zdroje, zabraňuje ručním změnám nastavení času a vyžaduje včasnou nápravu odchylek systémového času.

2. Rozsah

2.1 Tato politika se vztahuje na:

2.1.1 všechny systémy a zařízení ve vlastnictví společnosti, včetně serverů, stolních počítačů, notebooků, mobilních zařízení, firewallů, směrovačů a virtuálních strojů

2.1.2 vzdálenou a cloudově hostovanou infrastrukturu používanou v provozu (např. AWS, Microsoft 365, SaaS platformy)

2.1.3 systémy, které vytvářejí nebo ukládají protokoly událostí, záznamy o autentizaci nebo auditní stopu

2.1.4 všechny zaměstnance, dodavatele, poskytovatele služeb nebo pracovníky IT podpory odpovědné za konfiguraci nebo údržbu těchto systémů

2.2 Tato politika se vztahuje také na koncová zařízení v režimu BYOD používaná pro přístup k podnikovým systémům, pokud tato zařízení ukládají nebo vytvářejí data relevantní pro audit.

3. Cíle

3.1 Zajistit, aby všechny kritické systémy automaticky synchronizovaly čas prostřednictvím důvěryhodných serverů protokolu Network Time Protocol (NTP) nebo rovnocenných mechanismů poskytovatele cloudových služeb

3.2 Předcházet časovým nesouladům, které by mohly oslabit spolehlivost nebo korelaci systémových protokolů během auditů nebo bezpečnostních šetření

3.3 Umožnit včasnou detekci a nápravu odchylek času překračujících přípustné prahové hodnoty

3.4 Udržovat konzistentní časová razítka napříč prostředími (on-premise, cloudová a vzdálená prostředí)

3.5 Splnit technické a právní požadavky na integritu, dohledatelnost a nepopiratelnost záznamů a událostí

4. Role a odpovědnosti

4.1 generální ředitel

4.1.1 schvaluje tuto politiku a zajišťuje její dodržování v celé organizaci

4.1.2 vykonává dohled nad pravidelnými přezkumy přesnosti času na úrovni systémů a nad nedostatky v implementaci

4.1.3 schvaluje výjimky z automatizované synchronizace času, pokud jsou odůvodněné a zdokumentované

4.2 IT podpora / interní IT

4.2.1 konfiguruje synchronizaci času pro všechny systémy ve vlastnictví společnosti nebo jí spravované

4.2.2 ověřuje, že denní nebo plánovaná synchronizace funguje správně

4.2.3 prověřuje a odstraňuje události odchylky času, selhání synchronizace nebo problémy s přístupem k NTP

4.2.4 dokumentuje stav synchronizace času v rámci měsíčních kontrol provozního stavu systémů

[... Oddíly 4.3–8 nejsou součástí tohoto náhledu. Pro přístup k úplnému obsahu zakupte celý dokument. ...]

9. Požadavky na přezkoumávání a aktualizaci

9.1 Plánovaný přezkum

9.1.1 Tato politika musí být každoročně přezkoumána generálním ředitelem, IT podporou a koordinátorem ochrany soukromí

9.1.2 Při přezkumu musí být zohledněny všechny protokoly a zprávy o stavu souladu synchronizace času

9.2 Aktualizace na základě spouštěcí události

9.2.1 Tato politika musí být aktualizována, pokud:

9.2.1.1 selhání systému způsobí významnou odchylku času

9.2.1.2 audit odhalí nedostatky v synchronizaci času

9.2.1.3 organizace zavede nové cloudové, hybridní nebo virtualizované prostředí

9.2.1.4 právní nebo regulatorní změny zavedou nové požadavky na integritu času

9.3 Řízení verzí a komunikace

9.3.1 Všechny aktualizace musí být verzovány a datovány

9.3.2 Významné změny musí být sděleny všem technickým pracovníkům

9.3.3 Předchozí verze musí být uchovávány po dobu 3 let na podporu auditu

10. Související politiky a vazby

10.1 Tato politika musí být uplatňována společně s následujícími politikami SME:

10.1.1 P22S – Politika protokolování a monitorování: Zajišťuje konzistentní časová razítka napříč protokoly pro dohledatelnost a forenzní korelaci.

10.1.2 P30S – Politika reakce na incidenty: Spoléhá na přesnost časových razítek při rekonstrukci incidentů, stanovení časových os a podpoře rozhodování o oznamování.

10.1.3 P17S – Politika ochrany dat a soukromí: Zajišťuje, aby protokoly přístupu a časové osy nakládání s daty zahrnující osobní údaje byly přesné a obhajitelné podle GDPR.

10.1.4 P12S – Politika správy aktiv: Podporuje identifikaci systémů vyžadujících synchronizaci, zejména mobilních a vzdálených zařízení.

10.1.5 P26S – Bezpečnostní politika třetích stran a dodavatelů: Zajišťuje, aby dodavatelé, kteří pro organizaci přistupují k datům nebo je protokolují, smluvně dodržovali postupy synchronizace času.

11. Referenční normy a rámce

11.1 ISO/IEC 27001:

11.1.1 Kapitola 8.1 – Vyžaduje zavedení opatření nezbytných pro bezpečný provoz, včetně protokolování a časových razítek.

11.2 ISO/IEC 27002:

11.2.1 Opatření 8.17 – Doporučuje synchronizovaný čas pro všechny systémy, které vytvářejí protokoly nebo fungují ve vzájemné součinnosti.

11.3 NIST SP 800-53 Rev.5:

11.3.1 AU-8 – Vyžaduje používání interních nebo externích časových zdrojů pro přesnost časových razítek v protokolech.

11.3.2 SC-45 – Stanoví používání důvěryhodných zdrojů NTP a zamezení ručním změnám času v kritických systémech.

11.4 GDPR:

11.4.1 Článek 5(1)(d) – Vyžaduje přesnost a odpovědnost při zpracování osobních údajů, podpořenou synchronizovanými časovými razítky.

11.4.2 Článek 32 – Vyžaduje bezpečnostní opatření zajišťující integritu dat, včetně konzistentních časových rámců protokolování.

11.5 směrnice NIS2:

11.5.1 Článek 21(2)(d) – Vyžaduje schopnosti monitorování a detekce podpořené synchronizovanými systémovými protokoly.

11.6 nařízení DORA:

11.6.1 Článek 10 – Vyžaduje provozní odolnost, která předpokládá dohledatelné protokoly ICT incidentů s časovým razítkem.

11.6.2 Článek 15 – Vyžaduje, aby poskytovatelé služeb vedli přesné technické záznamy, včetně auditní stopy s časovým razítkem.

11.7 COBIT 2019:

11.7.1 DSS05.02 – Zdůrazňuje integritu časových razítek pro detekci událostí a reakci na ně.

11.7.2 MEA03.01 – Vyžaduje monitorování výkonnosti založené na důkazech, podpořené přesnými časově synchronizovanými daty.