					Sem zadajte názov registrovanej právnickej osoby							
Číslo dokumentu: P23S					Názov dokumentu: **Politika synchronizácie času**							
Verzia: 1.0		Dátum nadobudnutia účinnosti: 01.01.2025			Vlastník dokumentu:							
X	Politika		Štandard		Postup		Formulár		Register		Iné	

História revízií				
Číslo revízie	**Dátum revízie**	**Zmeny**	**Preskúmal**	**Vlastník procesu**

Schválenia			
Meno	**Pozícia**	**Dátum**	**Podpis**

V súlade s normami a predpismi

Norma/predpis	Kapitola/článok	Poznámka
ISO/IEC 27001:2022	Kapitola 8	Relevantné požiadavky na bezpečnostné opatrenia
ISO/IEC 27002:2022	Kontrola 8	Synchronizovaná prevádzka systémov
NIST SP 800-53 Rev.5	SC-45, AU-8	Dôveryhodné NTP a presnosť časových pečiatok v logoch
Nariadenie EÚ GDPR	Články 5(1)(d), 32	Presnosť, zodpovednosť a integrita pri spracúvaní osobných údajov so synchronizovanými časovými pečiatkami
Smernica EÚ NIS2	Článok 21(2)(d)	Schopnosti monitorovania a detekcie podporené synchronizovanými logmi
Nariadenie EÚ DORA	Články 10, 15	Prevádzková odolnosť a presné technické záznamy
COBIT 2019	DSS05.02, MEA03	Udalosti s časovou pečiatkou a monitorovanie založené na dôkazoch

1. Účel

1.1 Táto politika stanovuje povinné opatrenia na udržiavanie presného a synchronizovaného času vo všetkých systémoch, ktoré ukladajú, prenášajú alebo spracúvajú údaje organizácie.

1.2 Synchronizácia času je nevyhnutná na zabezpečenie sledovateľnosti systémových logov, presnej korelácie bezpečnostných incidentov a spoľahlivej použiteľnosti dôkazového materiálu pri forenznej analýze alebo právnom preskúmaní.

1.3 Organizácia uplatňuje automatizovanú synchronizáciu času ako základnú požiadavku na integritu auditu, reakciu na incidenty a súlad s požiadavkami podľa ISO 27001, GDPR, DORA a NIS2.

1.4 Táto politika zabezpečuje, aby všetky systémy používali dôveryhodné zdroje času, bráni manuálnym zásahom do časových nastavení a vyžaduje včasnú nápravu odchýlok systémového času.

2. Rozsah

2.1 Táto politika sa vzťahuje na:

2.1.1 Všetky systémy a zariadenia vo vlastníctve spoločnosti vrátane serverov, stolných počítačov, notebookov, mobilných zariadení, firewallov, smerovačov a virtuálnych strojov

2.1.2 Vzdialenú infraštruktúru a infraštruktúru prevádzkovanú v cloudovom prostredí používanú pri prevádzke (napr. AWS, Microsoft 365, platformy SaaS)

2.1.3 Systémy, ktoré generujú alebo ukladajú logy udalostí, autentifikačné záznamy alebo auditnú stopu

2.1.4 Všetkých zamestnancov, zmluvných pracovníkov, dodávateľov alebo poskytovateľov IT podpory zodpovedných za konfiguráciu alebo údržbu týchto systémov

2.2 Táto politika sa vzťahuje aj na koncové zariadenia v režime používania vlastných zariadení (BYOD), ktoré sa používajú na prístup do podnikových systémov, za predpokladu, že tieto koncové zariadenia ukladajú alebo generujú údaje relevantné pre audit.

3. Ciele

3.1 Zabezpečiť, aby všetky kritické systémy automaticky synchronizovali čas prostredníctvom dôveryhodných serverov Network Time Protocol (NTP) alebo ekvivalentných mechanizmov poskytovateľa cloudových služieb

3.2 Predchádzať časovým nezrovnalostiam, ktoré by mohli oslabiť spoľahlivosť alebo koreláciu systémových logov počas auditov alebo bezpečnostných vyšetrovaní

3.3 Umožniť včasnú detekciu a nápravu odchýlok času nad prijateľné prahové hodnoty

3.4 Udržiavať konzistentné časové pečiatky naprieč prostrediami (on-premises, cloudové a vzdialené prostredia)

3.5 Plniť technické a právne požiadavky na integritu, sledovateľnosť a nepopierateľnosť záznamov a udalostí

4. Roly a zodpovednosti

4.1 Generálny manažér (GM)

4.1.1 Schvaľuje túto politiku a zabezpečuje jej dodržiavanie v rámci organizácie

4.1.2 Dohliada na pravidelné preskúmania presnosti času na úrovni systémov a na identifikované nedostatky v implementácii

4.1.3 Schvaľuje výnimky z automatizovanej synchronizácie času, ak sú odôvodnené a zdokumentované

4.2 Poskytovateľ IT podpory / interná IT funkcia

4.2.1 Konfiguruje synchronizáciu času pre všetky systémy vo vlastníctve spoločnosti alebo systémy spravované spoločnosťou

4.2.2 Overuje, že denná alebo plánovaná synchronizácia funguje správne

4.2.3 Vyšetruje a odstraňuje odchýlky času, zlyhania synchronizácie alebo problémy s prístupom k NTP

4.2.4 Dokumentuje stav synchronizácie času ako súčasť mesačných kontrol stavu systémov

[... Sekcie 4.3–8 nie sú súčasťou tohto náhľadu. Pre prístup k úplnému obsahu si zakúpte celý dokument. ...]

9. Požiadavky na preskúmanie a aktualizáciu

9.1 Plánované preskúmanie

9.1.1 Túto politiku musia každoročne preskúmať Generálny manažér, poskytovateľ IT podpory a koordinátor ochrany súkromia

9.1.2 Počas preskúmania sa musia zohľadniť všetky logy a správy o stave súladu synchronizácie času

9.2 Aktualizácie na základe spúšťacej udalosti

9.2.1 Táto politika sa musí aktualizovať, ak:

9.2.1.1 Zlyhanie systému spôsobí významnú odchýlku času

9.2.1.2 Audit odhalí nedostatky v synchronizácii času

9.2.1.3 Organizácia zavedie nové cloudové, hybridné alebo virtualizačné prostredia

9.2.1.4 Právne alebo regulačné zmeny zavedú nové požiadavky na integritu času

9.3 Riadenie verzií a komunikácia

9.3.1 Všetky aktualizácie musia podliehať riadeniu verzií a musia byť datované

9.3.2 Významné zmeny musia byť komunikované všetkým technickým pracovníkom

9.3.3 Predchádzajúce verzie sa musia uchovávať 3 roky na podporu auditu

10. Súvisiace politiky a väzby

10.1 Táto politika sa musí uplatňovať spolu s nasledujúcimi SME politikami:

10.1.1 P22S – Politika logovania a monitorovania: Zabezpečuje konzistentné časové pečiatky naprieč logmi na účely sledovateľnosti a forenznej korelácie.

10.1.2 P30S – Politika reakcie na incidenty: Opiera sa o presnosť časových pečiatok pri rekonštrukcii incidentov, určovaní časových osí a podpore rozhodnutí o notifikáciách.

10.1.3 P17S – Politika ochrany údajov a súkromia: Zabezpečuje, aby logy prístupov a časové rámce spracúvania údajov zahŕňajúce osobné údaje boli presné a obhájiteľné podľa GDPR.

10.1.4 P12S – Politika správy aktív: Podporuje identifikáciu systémov vyžadujúcich synchronizáciu, najmä mobilných a vzdialených zariadení.

10.1.5 P26S – Bezpečnostná politika pre tretie strany a dodávateľov: Zabezpečuje, aby dodávatelia, ktorí pristupujú k údajom organizácie alebo ich zaznamenávajú do logov, zmluvne dodržiavali postupy synchronizácie času.

11. Referenčné normy a rámce

11.1 ISO/IEC 27001:

11.1.1 Kapitola 8.1 – Vyžaduje implementáciu opatrení potrebných na bezpečnú prevádzku vrátane logovania a časových pečiatok.

11.2 ISO/IEC 27002:

11.2.1 Kontrola 8.17 – Odporúča synchronizovaný čas pre všetky systémy, ktoré vytvárajú logy alebo fungujú vo vzájomnej súčinnosti.

11.3 NIST SP 800-53 Rev.5:

11.3.1 AU-8 – Vyžaduje používanie interných alebo externých zdrojov času na zabezpečenie presnosti časových pečiatok logov.

11.3.2 SC-45 – Stanovuje používanie dôveryhodných zdrojov NTP a zabraňuje manuálnym zmenám času v kritických systémoch.

11.4 Nariadenie EÚ GDPR:

11.4.1 Článok 5(1)(d) – Vyžaduje presnosť a zodpovednosť pri spracúvaní osobných údajov, podporenú synchronizovanými časovými pečiatkami.

11.4.2 Článok 32 – Vyžaduje bezpečnostné opatrenia zabezpečujúce integritu údajov, čo zahŕňa aj konzistentné časové rámce logovania.

11.5 Smernica EÚ NIS2:

11.5.1 Článok 21(2)(d) – Vyžaduje schopnosti monitorovania a detekcie podporené synchronizovanými systémovými logmi.

11.6 Nariadenie EÚ DORA:

11.6.1 Článok 10 – Vyžaduje prevádzkovú odolnosť, ktorá predpokladá sledovateľné logy incidentov IKT s časovou pečiatkou.

11.6.2 Článok 15 – Vyžaduje, aby poskytovatelia služieb udržiavali presné technické záznamy vrátane auditnej stopy s časovou pečiatkou.

11.7 COBIT 2019:

11.7.1 DSS05.02 – Zdôrazňuje integritu časových pečiatok pri detekcii a reakcii na udalosti.

11.7.2 MEA03.01 – Vyžaduje monitorovanie výkonnosti založené na dôkazoch, podporené presnými časovo synchronizovanými údajmi.