					Sem zadajte názov registrovanej právnickej osoby							
Číslo dokumentu: P23					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**

Zosúladenie s normami a predpismi

Norma/predpis	Kapitola/článok	Poznámka
ISO/IEC 27001:2022	Kapitola 8	-
ISO/IEC 27002:2022	Kontrola 8	-
NIST SP 800-53 Rev.5	SC-45, AU-8	-
Nariadenie EÚ GDPR	Článok 32	-
Smernica EÚ NIS2	Článok 21(2)(e)	-
Nariadenie EÚ DORA	Články 9, 10	-
COBIT 2019	DSS05.04, MEA	-

1. Účel

1.1 Účelom tejto politiky je zabezpečiť, aby všetky systémy, aplikácie, zariadenia a cloudové služby organizácie udržiavali konzistentné a presné nastavenie času synchronizáciou s určenými dôveryhodnými časovými zdrojmi.

1.2 Presná synchronizácia času je nevyhnutná pre spoľahlivé logovanie, bezpečnú komunikáciu, auditnú stopu, reakciu na incidenty a forenzné vyšetrovanie. Nesúlad času môže viesť k nemožnosti korelácie logov, zlyhaniam autentifikácie a neúplnému regulačnému vykazovaniu.

1.3 Táto politika podporuje kontrolu 8.17 prílohy A normy ISO/IEC 27001 a súvisiace medzinárodné normy tým, že presadzuje presnosť času a detekciu odchýlok systémových hodín v celom IT prostredí organizácie.

2. Rozsah

2.1 Táto politika sa vzťahuje na:

2.1.1 Všetky komponenty infraštruktúry vrátane serverov, pracovných staníc, sieťových zariadení, firewallov a systémov IoT

2.1.2 Virtuálne a cloudové prostredia (napr. AWS, Azure, Google Cloud)

2.1.3 Všetky systémy zapojené do logovania, autentifikácie, spracovania transakcií alebo korelácie bezpečnostných udalostí

2.1.4 Interných zamestnancov, zmluvných pracovníkov a externých poskytovateľov služieb, ktorí nesú zodpovednosť za systémy citlivé na čas

2.2 Systémy, ktoré vytvárajú alebo používajú záznamy s časovou pečiatkou — napríklad položky logov, upozornenia, záznamy o aktivite používateľov alebo forenzné dôkazy — sa považujú za súčasť rozsahu tejto politiky.

3. Ciele

3.1 Definovať konzistentnú centralizovanú architektúru synchronizácie času s použitím schválených zdrojov NTP alebo ekvivalentného riešenia.

3.2 Zabezpečiť, aby všetky systémy synchronizovali svoje hodiny v definovaných intervaloch a aby akákoľvek odchýlka bola detegovaná a odstránená automaticky alebo s minimálnym zásahom.

3.3 Udržiavať presnosť systémových hodín v hybridných prostrediach, v on-premise infraštruktúre aj v cloudovom prostredí s cieľom umožniť:

3.3.1 Spoľahlivú koreláciu udalostí a reakciu na incidenty

3.3.2 Dodržiavanie predpisov a súlad s normami, ako sú ISO 27001, GDPR, NIS2 a DORA

3.3.3 Ochranu pred replay útokmi a zlyhaniami autentifikácie založenej na čase

3.4 Zaviesť jednoznačné roly, postupy na riadenie výnimiek a auditné mechanizmy na zabezpečenie uplatňovania tejto politiky.

3.5 Zabezpečiť, aby anomálie súvisiace s časom boli zaznamenané v logoch, vyvolali upozornenie a boli eskalované po prekročení stanovených tolerancií.

4. Roly a zodpovednosti

4.1 Riaditeľ informačnej bezpečnosti (CISO)

4.1.1 Zodpovedá za túto politiku a zabezpečuje jej súlad s prevádzkovými kontrolami ISMS a regulačnými požiadavkami.

4.1.2 Schvaľuje výber podnikových časových zdrojov a potvrdzuje procesy vykazovania synchronizácie času.

4.2 Manažér infraštruktúrnych služieb / vedúci sieťového inžinierstva

4.2.1 Spravuje primárne a sekundárne NTP servery organizácie alebo konfiguráciu určených časových zdrojov.

4.2.2 Zabezpečuje, aby všetky sieťovo pripojené zariadenia a virtuálne inštancie synchronizovali čas v primeraných intervaloch.

4.2.3 Monitoruje logy synchronizácie času, upozornenia na odchýlky systémových hodín a poruchové stavy.

[... 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 Táto politika musí byť preskúmaná každoročne alebo skôr za týchto podmienok:

9.1.1 Zistenie exploitov založených na čase alebo zlyhaní logovania

9.1.2 Zmeny v kľúčovej časovej infraštruktúre (napr. nové podnikové NTP servery alebo aktualizácie protokolov)

9.1.3 Odchýlky času na cloudových platformách alebo regionálne zmeny služieb

9.1.4 Poincidentné zistenia, ktoré identifikujú nesúlad času ako prispievajúci faktor

9.2 Preskúmanie koordinuje vedúci infraštruktúry, pričom sa vyžaduje vstup od SOC, bezpečnosti aplikácií a zainteresovaných strán pre oblasť súladu.

9.3 Revízie musia byť zdokumentované v registri dokumentov ISMS a komunikované dotknutým interným zainteresovaným stranám a tretím stranám.

9.4 Historické verzie politiky musia byť bezpečne archivované, podliehať riadeniu verzií a byť dostupné na účely požiadaviek súladu alebo právneho auditu.

10. Súvisiace politiky a väzby

10.1 P1 – Politika informačnej bezpečnosti. Stanovuje nadradený mandát na zabezpečenie integrity a sledovateľnosti všetkých informačných systémov, pričom presnosť času je jeho základným predpokladom.

10.2 P5 – Politika riadenia zmien. Upravuje zmeny konfigurácií systémov vrátane úprav časových zdrojov a zabezpečuje riadnu dokumentáciu, testovanie a plány návratu zmien.

10.3 P22 – Politika logovania a monitorovania. Je priamo závislá od synchronizovaného času na zabezpečenie sekvencovania udalostí, korelácie logov a integrity vyšetrovania incidentov naprieč rôznorodými systémami.

10.4 P30 – Politika reakcie na incidenty. Vychádza z presných časových pečiatok pre forenzné vyšetrovania, časové osi incidentov a dôkazy v reťazci zverenia. Nepresný čas oslabuje dôveryhodnosť správ o incidentoch.

10.5 P20 – Politika ochrany koncových bodov / politika ochrany pred malvérom. Vyžaduje upozorňovanie s presným časom a behaviorálnu analýzu na detekciu šírenia malvéru, laterálneho pohybu a anomálií prístupu.

10.6 P6 – Politika riadenia rizík. Definuje desynchronizáciu ako potenciálne prevádzkové a forenzné riziko, ktoré si vyžaduje kontroly definované v tejto politike na zmiernenie dopadu.

11. Referenčné normy a rámce

11.1 ISO/IEC 27001

11.1.1 Kapitola 8.1 – Prevádzkové plánovanie a riadenie: Vyžaduje integráciu presných technických kontrol, ako sú synchronizované systémové hodiny, na zabezpečenie spoľahlivého vykonávania prevádzky.

11.2 ISO/IEC 27002:2022 – Kontrola 8

11.2.1 Posilňuje požiadavku na presnosť systémových hodín a vyžaduje konzistentnosť systémového času v organizácii na uľahčenie porovnávania logov, vyšetrovania a bezpečnej validácie transakcií.

11.3 NIST SP 800-53 Rev.5

11.3.1 SC-45 – Synchronizácia systémového času: Vyžaduje synchronizáciu času s použitím autoritatívnych zdrojov vo všetkých komponentoch v rámci hranice systému.

11.3.2 AU-8 – Časové pečiatky: Zabezpečuje, aby udalosti boli presne označené časovou pečiatkou, a poskytuje sledovateľnosť na účely auditu a reakcie na incidenty.

11.4 Nariadenie EÚ GDPR (2016/679)

11.4.1 Článok 32 – Bezpečnosť spracúvania: Hoci výslovne neuvádza čas, vyžaduje použitie primeraných technických opatrení vrátane auditných stôp a logov, ktorých platnosť a integrita sú prirodzene závislé od synchronizovaných časových pečiatok.

11.5 Smernica EÚ NIS2 (2022/2555)

11.5.1 Článok 21(2)(e): Vyžaduje schopnosti logovania a detekcie, ktoré predpokladajú presnú synchronizáciu času na koreláciu naprieč systémami a včasnú reakciu.

11.6 Nariadenie EÚ DORA (2022/2554)

11.6.1 Článok 9 – Riadenie rizík IKT: Vyžaduje presnú telemetriu systémov na monitorovanie rizík a detekciu anomálií, čo závisí od presnej synchronizácie systémových hodín.

11.6.2 Článok 10 – Kontinuita činností IKT: Ukladá kontroly zabezpečujúce integritu systémov počas narušení vrátane časovo zosúladených záznamov udalostí.

11.7 COBIT 2019

11.7.1 DSS05.04 – Monitorovanie bezpečnostných udalostí: Vyžaduje integritu časových pečiatok na účinnú analýzu logov a detekciu hrozieb.

11.7.2 MEA03 – Monitorovanie, hodnotenie a posudzovanie súladu: Synchronizácia času podporuje presný audit súladu a cykly vykazovania.