					Wprowadź tutaj nazwę zarejestrowanej osoby prawnej							
Numer dokumentu: P23S					Tytuł dokumentu: **Polityka synchronizacji czasu**							
Wersja: 1.0		Data wejścia w życie: 01.01.2025			Właściciel dokumentu:							
X	Polityka		Standard		Procedura		Formularz		Rejestr		Inne	

Historia zmian				
Numer zmiany	**Data zmiany**	**Zmiany**	**Przegląd wykonał**	**Właściciel procesu**

Zatwierdzenia			
Imię i nazwisko	**Stanowisko**	**Data**	**Podpis**

Dostosowanie do norm i regulacji

Norma/regulacja	Klauzula/artykuł	Komentarz
ISO/IEC 27001:2022	Klauzula 8	Odpowiednie wymagania dotyczące zabezpieczeń
ISO/IEC 27002:2022	Środek kontrolny 8.17	Synchronizacja czasu systemowego
NIST SP 800-53 Rev.5	SC-45, AU-8	Zaufane źródła NTP i dokładność znaczników czasu w logach
RODO	Artykuły 5(1)(d), 32	Dokładność, rozliczalność i integralność danych osobowych wspierane przez zsynchronizowane znaczniki czasu
Dyrektywa NIS2	Artykuł 21(2)(d)	Zdolności monitorowania i wykrywania wspierane przez zsynchronizowane logi
Rozporządzenie DORA	Artykuły 10, 15	Odporność operacyjna i dokładna dokumentacja techniczna
COBIT 2019	DSS05.02, MEA03	Zdarzenia opatrzone znacznikiem czasu i monitorowanie oparte na dowodach

1. Cel

1.1 Niniejsza polityka ustanawia obowiązkowe zabezpieczenia służące utrzymaniu dokładnego i zsynchronizowanego czasu we wszystkich systemach, które przechowują, przesyłają lub przetwarzają dane organizacji.

1.2 Synchronizacja czasu jest niezbędna do zapewnienia audytowalności logów systemowych, prawidłowej korelacji incydentów bezpieczeństwa oraz możliwości wykorzystania materiału dowodowego w analizie kryminalistycznej lub przeglądzie prawnym.

1.3 Organizacja wymaga stosowania zautomatyzowanej synchronizacji czasu jako podstawowego wymogu zapewniającego integralność audytową, skuteczne reagowanie na incydenty oraz zgodność z wymaganiami regulacyjnymi zgodnie z ISO 27001, RODO, DORA i NIS2.

1.4 Niniejsza polityka zapewnia, że wszystkie systemy korzystają z zaufanych źródeł czasu, zapobiega ręcznemu nadpisywaniu ustawień czasu oraz wymaga terminowej korekty dryfu zegara.

2. Zakres

2.1 Niniejsza polityka ma zastosowanie do:

2.1.1 wszystkich systemów i urządzeń będących własnością firmy, w tym serwerów, komputerów stacjonarnych, laptopów, urządzeń mobilnych, zapór sieciowych, routerów i maszyn wirtualnych,

2.1.2 infrastruktury zdalnej oraz zasobów hostowanych w chmurze wykorzystywanych w działalności operacyjnej (np. AWS, Microsoft 365, platformy SaaS),

2.1.3 systemów, które generują lub przechowują logi zdarzeń, zapisy uwierzytelniania lub ścieżki audytu,

2.1.4 wszystkich pracowników, współpracowników, dostawców lub podmiotów świadczących wsparcie IT odpowiedzialnych za konfigurację lub utrzymanie tych systemów.

2.2 Polityka ma również zastosowanie do punktów końcowych wykorzystujących urządzenia prywatne (BYOD) używanych do uzyskiwania dostępu do systemów biznesowych, pod warunkiem że takie punkty końcowe przechowują dane istotne z punktu widzenia audytu lub generują takie dane.

3. Cele

3.1 Zapewnienie, że wszystkie systemy krytyczne automatycznie synchronizują czas przy użyciu zaufanych serwerów Network Time Protocol (NTP) lub równoważnych mechanizmów dostawcy chmury.

3.2 Zapobieganie rozbieżnościom czasu, które mogłyby podważyć wiarygodność lub korelację logów systemowych podczas audytów lub postępowań wyjaśniających dotyczących bezpieczeństwa.

3.3 Umożliwienie terminowego wykrywania i korygowania dryfu czasu przekraczającego dopuszczalne progi.

3.4 Utrzymanie spójnego oznaczania czasem we wszystkich środowiskach (infrastruktura lokalna, chmura i środowiska zdalne).

3.5 Spełnienie wymagań technicznych i prawnych dotyczących integralności, identyfikowalności i niezaprzeczalności zapisów oraz zdarzeń.

4. Role i odpowiedzialności

4.1 Dyrektor Generalny (GM)

4.1.1 Zatwierdza niniejszą politykę i zapewnia zgodność organizacji z jej postanowieniami.

4.1.2 Nadzoruje okresowe przeglądy dokładności czasu na poziomie systemów oraz luk we wdrożeniu.

4.1.3 Zatwierdza odstępstwa od zautomatyzowanej synchronizacji czasu, jeżeli są one uzasadnione i udokumentowane.

4.2 Dostawca wsparcia IT / wewnętrzna funkcja IT

4.2.1 Konfiguruje synchronizację czasu dla wszystkich systemów będących własnością firmy lub pozostających pod jej zarządzaniem.

4.2.2 Weryfikuje, czy codzienna lub zaplanowana synchronizacja działa prawidłowo.

4.2.3 Analizuje i usuwa przyczyny dryfu czasu, niepowodzeń synchronizacji lub problemów z dostępem do NTP.

4.2.4 Dokumentuje status synchronizacji czasu jako element comiesięcznych kontroli stanu systemów.

[... Sekcje 4.3–8 nie są uwzględnione w tej wersji zapoznawczej. Zakup pełny dokument, aby uzyskać dostęp do pełnej treści. ...]

9. Wymagania dotyczące przeglądu i aktualizacji

9.1 Planowany przegląd

9.1.1 Niniejsza polityka musi podlegać corocznemu przeglądowi przez Dyrektora Generalnego, Dostawcę wsparcia IT oraz Koordynatora ds. prywatności.

9.1.2 W ramach przeglądu należy uwzględnić wszystkie logi oraz raporty statusowe dotyczące zgodności synchronizacji czasu.

9.2 Aktualizacje inicjowane zdarzeniem

9.2.1 Niniejsza polityka musi zostać zaktualizowana, jeżeli:

9.2.1.1 awaria systemu spowoduje istotny dryf czasu,

9.2.1.2 audyt wykaże słabości w synchronizacji czasu,

9.2.1.3 organizacja wdroży nowe środowiska chmurowe, środowiska hybrydowe lub środowiska wirtualizacyjne,

9.2.1.4 zmiany prawne lub regulacyjne wprowadzą nowe wymagania dotyczące integralności czasu.

9.3 Kontrola wersji i komunikacja

9.3.1 Wszystkie aktualizacje muszą być wersjonowane i datowane.

9.3.2 Istotne zmiany muszą być komunikowane całemu personelowi technicznemu.

9.3.3 Poprzednie wersje muszą być przechowywane przez 3 lata na potrzeby audytu.

10. Powiązane polityki i zależności

10.1 Niniejszą politykę należy stosować łącznie z następującymi politykami SME:

10.1.1 P22S – Polityka rejestrowania i monitorowania: zapewnia spójne oznaczanie czasem w logach na potrzeby identyfikowalności i korelacji kryminalistycznej.

10.1.2 P30S – Polityka reagowania na incydenty: opiera się na dokładności znaczników czasu w celu odtworzenia incydentów, ustalenia osi czasu i wsparcia decyzji dotyczących powiadomień.

10.1.3 P17S – Polityka ochrony danych i prywatności: zapewnia, że logi dostępu oraz harmonogramy czynności przetwarzania danych dotyczących danych osobowych są dokładne i możliwe do obrony zgodnie z RODO.

10.1.4 P12S – Polityka zarządzania aktywami: wspiera identyfikację systemów wymagających synchronizacji, w szczególności urządzeń mobilnych i zdalnych.

10.1.5 P26S – Polityka bezpieczeństwa stron trzecich i dostawców: zapewnia, że dostawcy uzyskujący dostęp do danych organizacji lub rejestrujący takie dane są zobowiązani umownie do stosowania zsynchronizowanego czasu.

11. Normy i ramy odniesienia

11.1 ISO/IEC 27001:

11.1.1 Klauzula 8.1 – Wymaga wdrożenia zabezpieczeń niezbędnych do bezpiecznej działalności operacyjnej, w tym rejestrowania i oznaczania czasem.

11.2 ISO/IEC 27002:

11.2.1 Środek kontrolny 8.17 – Zaleca stosowanie zsynchronizowanego czasu we wszystkich systemach, które wytwarzają logi lub współdziałają operacyjnie.

11.3 NIST SP 800-53 Rev.5:

11.3.1 AU-8 – Wymaga stosowania wewnętrznych lub zewnętrznych źródeł czasu w celu zapewnienia dokładności znaczników czasu w logach.

11.3.2 SC-45 – Określa stosowanie zaufanych źródeł NTP oraz zapobieganie ręcznym zmianom czasu w systemach krytycznych.

11.4 RODO:

11.4.1 Artykuł 5(1)(d) – Wymaga dokładności i rozliczalności w przetwarzaniu danych osobowych, wspieranych przez zsynchronizowane znaczniki czasu.

11.4.2 Artykuł 32 – Wymaga stosowania środków bezpieczeństwa zapewniających integralność danych, co obejmuje spójne ramy czasowe rejestrowania.

11.5 Dyrektywa NIS2:

11.5.1 Artykuł 21(2)(d) – Wymaga zdolności monitorowania i wykrywania wspieranych przez zsynchronizowane logi systemowe.

11.6 Rozporządzenie DORA:

11.6.1 Artykuł 10 – Wymaga odporności operacyjnej, w tym możliwych do prześledzenia i opatrzonych znacznikiem czasu logów incydentów ICT.

11.6.2 Artykuł 15 – Wymaga od dostawców usług utrzymywania dokładnych zapisów technicznych, w tym ścieżek audytu opatrzonych znacznikiem czasu.

11.7 COBIT 2019:

11.7.1 DSS05.02 – Podkreśla znaczenie integralności znaczników czasu dla wykrywania zdarzeń i reagowania na nie.

11.7.2 MEA03.01 – Wymaga monitorowania skuteczności opartego na dowodach, wspieranego przez dokładne dane zsynchronizowane czasowo.