					Wprowadź tutaj nazwę zarejestrowanej osoby prawnej							
Numer dokumentu: P23					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	-
ISO/IEC 27002:2022	Środek kontrolny 8	-
NIST SP 800-53 Rev.5	SC-45, AU-8	-
RODO	Artykuł 32	-
Dyrektywa NIS2	Artykuł 21(2)(e)	-
Rozporządzenie DORA	Artykuły 9, 10	-
COBIT 2019	DSS05.04, MEA	-

1. Cel

1.1 Celem niniejszej polityki jest zapewnienie, aby wszystkie systemy informatyczne organizacji, aplikacje, urządzenia oraz usługi chmurowe utrzymywały spójne i dokładne ustawienia czasu poprzez synchronizację z wyznaczonymi, zaufanymi źródłami czasu.

1.2 Dokładna synchronizacja czasu jest niezbędna dla wiarygodnego rejestrowania zdarzeń, bezpiecznej komunikacji, zapewnienia ścieżki audytowej, reagowania na incydenty oraz analiz informatyki śledczej. Niespójność czasu może skutkować brakiem korelacji logów, niepowodzeniem procesów uwierzytelniania oraz niekompletną sprawozdawczością regulacyjną.

1.3 Niniejsza polityka wspiera środek kontrolny 8.17 Załącznika A do normy ISO/IEC 27001 oraz powiązane normy międzynarodowe poprzez egzekwowanie dokładności czasu i wykrywania dryfu zegara w całym środowisku IT organizacji.

2. Zakres

2.1 Niniejsza polityka ma zastosowanie do:

2.1.1 wszystkich komponentów infrastruktury, w tym serwerów, stacji roboczych, urządzeń sieciowych, zapór sieciowych oraz systemów Internetu rzeczy (IoT)

2.1.2 środowisk wirtualnych i chmurowych (np. AWS, Azure, Google Cloud)

2.1.3 wszystkich systemów uczestniczących w rejestrowaniu zdarzeń, uwierzytelnianiu, przetwarzaniu transakcji lub korelacji zdarzeń bezpieczeństwa informacji

2.1.4 pracowników wewnętrznych, wykonawców oraz dostawców zewnętrznych odpowiedzialnych za systemy wrażliwe na synchronizację czasu

2.2 Za objęte zakresem uznaje się systemy generujące lub wykorzystujące zapisy opatrzone znacznikiem czasu, takie jak wpisy w logach, alerty, zapisy aktywności użytkowników lub dowody informatyki śledczej.

3. Cele

3.1 Zdefiniowanie spójnej, scentralizowanej architektury synchronizacji czasu z wykorzystaniem zatwierdzonych źródeł NTP lub rozwiązań równoważnych.

3.2 Zapewnienie, aby wszystkie systemy synchronizowały swoje zegary w określonych odstępach czasu oraz aby każdy dryf był wykrywany i korygowany automatycznie albo przy minimalnej interwencji.

3.3 Utrzymanie dokładności zegarów w środowiskach hybrydowych, infrastrukturze lokalnej oraz chmurze w celu zapewnienia:

3.3.1 wiarygodnej korelacji zdarzeń i skutecznego reagowania na incydenty

3.3.2 zgodności z normami i regulacjami, takimi jak ISO 27001, RODO, NIS2 i DORA

3.3.3 ochrony przed atakami powtórzeniowymi oraz awariami uwierzytelniania zależnymi od czasu

3.4 Ustanowienie jasnych ról, procedur obsługi odstępstw oraz mechanizmów audytowych w celu zapewnienia zgodności z polityką.

3.5 Zapewnienie, aby anomalie związane z czasem były rejestrowane, powodowały generowanie alertów oraz były eskalowane po przekroczeniu dopuszczalnych tolerancji.

4. Role i odpowiedzialności

4.1 Dyrektor ds. bezpieczeństwa informacji (CISO)

4.1.1 Odpowiada za niniejszą politykę i zapewnia jej zgodność z operacyjnymi środkami kontrolnymi SZBI oraz wymaganiami regulacyjnymi.

4.1.2 Zatwierdza wybór korporacyjnych źródeł czasu oraz weryfikuje procesy raportowania synchronizacji czasu.

4.2 Kierownik usług infrastrukturalnych / kierownik zespołu inżynierii sieciowej

4.2.1 Utrzymuje podstawowe i zapasowe serwery NTP organizacji lub konfigurację wyznaczonych źródeł czasu.

4.2.2 Zapewnia, aby wszystkie urządzenia sieciowe i instancje wirtualne synchronizowały czas w odpowiednich odstępach.

4.2.3 Monitoruje logi synchronizacji czasu, alerty dotyczące dryfu zegara oraz stany awaryjne.

[... 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 Niniejsza polityka musi podlegać przeglądowi co najmniej raz w roku lub wcześniej w następujących przypadkach:

9.1.1 wykrycia exploitów zależnych od czasu lub awarii rejestrowania

9.1.2 zmian w kluczowej infrastrukturze czasu (np. nowych korporacyjnych serwerów NTP lub aktualizacji protokołów)

9.1.3 rozbieżności dryfu czasu na platformach chmurowych lub regionalnych zmian usług

9.1.4 ustaleń po incydencie wskazujących niespójność czasu jako czynnik współwystępujący

9.2 Przegląd musi być koordynowany przez kierownika infrastruktury, przy obowiązkowym udziale SOC, bezpieczeństwa aplikacji oraz interesariuszy ds. zgodności.

9.3 Zmiany muszą być dokumentowane w Rejestrze dokumentów SZBI oraz komunikowane zainteresowanym stronom wewnętrznym i stronom trzecim, których dotyczą.

9.4 Historyczne wersje polityki muszą być bezpiecznie archiwizowane, objęte kontrolą wersji oraz udostępniane na potrzeby wniosków związanych z audytem zgodności lub przeglądem prawnym.

10. Powiązane polityki i odniesienia

10.1 P1 – P01 Polityka bezpieczeństwa informacji. Ustanawia nadrzędny obowiązek zapewnienia integralności i możliwości śledzenia wszystkich systemów informatycznych, dla których dokładność czasu stanowi podstawę.

10.2 P5 – P05 Polityka zarządzania zmianą. Reguluje modyfikacje konfiguracji systemów, w tym zmiany źródeł czasu, zapewniając właściwe dokumentowanie, testowanie i plany wycofania zmian.

10.3 P22 – Polityka rejestrowania i monitorowania. Jest bezpośrednio zależna od zsynchronizowanego czasu w celu zapewnienia sekwencjonowania zdarzeń, korelacji logów oraz integralności analiz incydentowych w zróżnicowanych systemach.

10.4 P30 – Polityka reagowania na incydenty (P30). Opiera się na dokładnych znacznikach czasu na potrzeby analiz informatyki śledczej, osi czasu incydentów oraz materiału dowodowego w ramach łańcucha dowodowego. Niedokładny czas podważa wiarygodność raportów incydentowych.

10.5 P20 – Polityka ochrony punktów końcowych / ochrony przed złośliwym oprogramowaniem. Wymaga dokładnego czasowo alertowania oraz analizy behawioralnej w celu wykrywania rozprzestrzeniania się złośliwego oprogramowania, ruchu lateralnego i anomalii dostępowych.

10.6 P6 – Polityka zarządzania ryzykiem. Definiuje desynchronizację jako potencjalne ryzyko operacyjne i z zakresu informatyki śledczej, wymagające stosowania środków kontrolnych określonych w niniejszej polityce w celu ograniczenia wpływu.

11. Normy referencyjne i ramy odniesienia

11.1 ISO/IEC 27001

11.1.1 Klauzula 8.1 – Planowanie operacyjne i nadzór: wymaga integracji dokładnych zabezpieczeń technicznych, takich jak zsynchronizowane zegary systemowe, dla wiarygodnej realizacji operacyjnej.

11.2 ISO/IEC 27002:2022 – Środek kontrolny 8

11.2.1 Wzmacnia wymaganie dotyczące dokładności zegarów i nakłada obowiązek zachowania organizacyjnej spójności czasu systemowego w celu ułatwienia porównywania logów, prowadzenia dochodzeń oraz bezpiecznej walidacji transakcji.

11.3 NIST SP 800-53 Rev.5

11.3.1 SC-45 – Synchronizacja czasu systemowego: wymaga synchronizacji czasu z wykorzystaniem autorytatywnych źródeł we wszystkich komponentach mieszczących się w granicach systemu.

11.3.2 AU-8 – Znaczniki czasu: zapewnia dokładne opatrywanie zdarzeń znacznikami czasu oraz możliwość ich śledzenia na potrzeby audytu i reagowania na incydenty.

11.4 RODO (2016/679)

11.4.1 Artykuł 32 – Bezpieczeństwo przetwarzania: choć nie odnosi się wprost do czasu, wymaga stosowania odpowiednich środków technicznych, w tym ścieżek audytowych i logów, które z natury zależą od zsynchronizowanych znaczników czasu dla zachowania ważności i integralności.

11.5 Dyrektywa NIS2 (2022/2555)

11.5.1 Artykuł 21(2)(e): wymaga zdolności w zakresie rejestrowania i wykrywania, które zakładają dokładną synchronizację czasu na potrzeby korelacji między systemami i terminowej reakcji.

11.6 Rozporządzenie DORA (2022/2554)

11.6.1 Artykuł 9 – zarządzanie ryzykiem ICT: nakłada obowiązek zapewnienia dokładnych danych telemetrycznych systemu na potrzeby monitorowania ryzyka i wykrywania anomalii, co zależy od precyzyjnej synchronizacji zegarów.

11.6.2 Artykuł 10 – ciągłość działania ICT: wymusza stosowanie środków kontrolnych zapewniających integralność systemów podczas zakłóceń, w tym zapisów zdarzeń zsynchronizowanych czasowo.

11.7 COBIT 2019

11.7.1 DSS05.04 – Monitorowanie zdarzeń bezpieczeństwa: wymaga integralności znaczników czasu na potrzeby skutecznej analizy logów i wykrywania zagrożeń.

11.7.2 MEA03 – Monitorowanie, ocena i ocena zgodności: synchronizacja czasu wspiera dokładne audyty zgodności oraz cykle sprawozdawcze.