					Wprowadź tutaj nazwę zarejestrowanej osoby prawnej							
Numer dokumentu: P22					Tytuł dokumentu: **Polityka rejestrowania i monitorowania**							
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**

1. Cel

1.1 Celem niniejszej polityki jest ustanowienie jasnych i egzekwowalnych wymagań dotyczących generowania, ochrony, przeglądu i analizy logów rejestrujących kluczowe zdarzenia systemowe oraz zdarzenia związane z bezpieczeństwem informacji w całym środowisku IT organizacji.

1.2 Rejestrowanie i monitorowanie mają kluczowe znaczenie dla wykrywania anomalii, reagowania na zagrożenia, prowadzenia analiz kryminalistycznych, zapewnienia gotowości audytowej oraz spełnienia wymagań prawnych. Polityka zapewnia, że wszystkie zdarzenia generowane przez systemy są właściwie rejestrowane, przechowywane i korelowane z wykorzystaniem dzienników zsynchronizowanych czasowo.

1.3 Niniejsza polityka ma istotne znaczenie dla wsparcia zgodności z normą ISO/IEC 27001, klauzulą 8.1, oraz z załącznikiem A, środkami kontrolnymi 8.15 (rejestrowanie), 8.16 (monitorowanie) i 8.17 (synchronizacja zegarów), a także odpowiada obowiązkom regulacyjnym wynikającym z RODO, NIS2, DORA i COBIT 2019.

2. Zakres

2.1 Niniejsza polityka ma zastosowanie do wszystkich systemów, usług i środowisk, które przechowują, przetwarzają lub transmitują dane objęte Systemem Zarządzania Bezpieczeństwem Informacji (SZBI), w tym:

2.1.1 infrastruktury lokalnej, usług chmury obliczeniowej (np. IaaS, PaaS, SaaS) oraz środowisk hybrydowych,

2.1.2 systemów operacyjnych, baz danych, aplikacji i urządzeń sieciowych,

2.1.3 systemów bezpieczeństwa, takich jak systemy SIEM, zapory sieciowe, platformy EDR, koncentratory VPN oraz dostawcy tożsamości.

2.2 W zakresie niniejszej polityki znajdują się następujące grupy interesariuszy:

2.2.1 użytkownicy wewnętrzni posiadający uprawnienia systemowe lub administracyjne,

2.2.2 personel infrastruktury i operacji IT,

2.2.3 Security Operations Center (SOC) oraz zespoły wykrywania zagrożeń,

2.2.4 programiści i właściciele aplikacji,

2.2.5 dostawcy usług stron trzecich zarządzający systemami generującymi logi.

3. Cele

3.1 Zapewnić, aby wszystkie systemy krytyczne generowały logi zdarzeń bezpieczeństwa informacji oraz zapisy aktywności systemowej przechowywane zgodnie z wymaganiami regulacyjnymi, prawnymi i umownymi.

3.2 Określić minimalne typy zdarzeń oraz zawartość logów niezbędne do wykrywania działań nieuprawnionych, odtworzenia działań użytkowników oraz wspierania analiz kryminalistycznych.

3.3 Wdrożyć zabezpieczenia zapobiegające manipulacji logami, ich nieuprawnionemu usuwaniu lub niekontrolowanemu dostępowi do danych rejestrowanych.

3.4 Ustanowić scentralizowane rejestrowanie oraz systemy alertowania (np. SIEM) w celu agregacji, korelacji i eskalacji podejrzanej aktywności w czasie zbliżonym do rzeczywistego.

3.5 Zapewnić synchronizację zegarów systemowych w celu umożliwienia dokładnej korelacji między systemami oraz analizy incydentów.

3.6 Umożliwić ciągłe doskonalenie i utrzymanie zgodności przez integrację monitorowania logów z procesami audytu, zarządzania ryzykiem i zarządzania incydentami.

4. Role i odpowiedzialności

4.1 Dyrektor ds. Bezpieczeństwa Informacji (CISO)

4.1.1 Jest właścicielem niniejszej polityki i zapewnia jej zgodność z profilem ryzyka organizacji, wymaganiami audytowymi oraz obowiązkami wynikającymi z SZBI.

4.1.2 Zatwierdza zakres rejestrowania dla systemów regulowanych lub wysokiego ryzyka oraz nadzoruje raportowanie zgodności.

4.2 Kierownik Security Operations Center (SOC)

4.2.1 Eksploatuje i utrzymuje scentralizowane platformy zarządzania logami (np. SIEM).

4.2.2 Definiuje reguły agregacji logów, progi alertów oraz ścieżki eskalacji dla triage incydentów.

4.2.3 Przegląda raporty dzienne oraz zapewnia, że anomalie są analizowane, dokumentowane i eskalowane w razie potrzeby.

[... 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 być przeglądana co najmniej raz w roku lub wcześniej w odpowiedzi na:

9.1.1 istotne zmiany architektury systemów lub infrastruktury rejestrowania (np. migrację SIEM),

9.1.2 zmiany wymagań regulacyjnych dotyczących rejestrowania (np. wymogów NIS2 lub DORA w zakresie logowania),

9.1.3 ustalenia z audytów lub analiz poincydentalnych,

9.1.4 nowe zagrożenia wymagające rozszerzonego monitorowania (np. zagrożenia wewnętrzne, naruszenia łańcucha dostaw).

9.2 Proces przeglądu prowadzi Kierownik Security Operations Center (SOC) w koordynacji z CISO, zespołami zarządzania ryzykiem, zgodności oraz infrastruktury IT.

9.3 Zatwierdzone zmiany muszą być objęte kontrolą wersji w rejestrze kontroli dokumentów SZBI i przekazywane do:

9.3.1 wszystkich interesariuszy odpowiedzialnych za utrzymanie systemów rejestrowania,

9.3.2 właścicieli aplikacji i systemów,

9.3.3 dostawców stron trzecich realizujących obowiązki w zakresie telemetrii lub integracji SIEM.

9.4 Wszystkie zastąpione wersje muszą być bezpiecznie archiwizowane, a dostęp do nich ograniczony do upoważnionych depozytariuszy SZBI na potrzeby audytowe i prawne.

10. Powiązane polityki i zależności

10.1 P1 – Polityka bezpieczeństwa informacji. Ustanawia podstawowe zobowiązanie do ochrony systemów i danych, w ramach którego rejestrowanie i monitorowanie pełnią funkcję kluczowych mechanizmów detekcyjnych oraz wspierających reagowanie.

10.2 P4 – Polityka kontroli dostępu. Zapewnia, że dostęp uprzywilejowany, logowania użytkowników i zdarzenia autoryzacyjne są rejestrowane w logach i monitorowane pod kątem nadużyć lub zachowań anomalnych.

10.3 P5 – Polityka zarządzania zmianą. Nakłada obowiązek rejestrowania zmian systemowych, wdrażania poprawek oraz aktualizacji konfiguracji, które mogą wprowadzać ryzyko lub nieuprawnione modyfikacje.

10.4 P21 – Polityka bezpieczeństwa sieci. Wymaga rejestrowania na poziomie sieci (np. logów zapory sieciowej, alertów IDS/IPS, aktywności VPN) oraz integracji z SIEM w celu zapewnienia widoczności anomalii ruchu i ochrony granic sieci.

10.5 P23 – Polityka synchronizacji czasu. Wymusza spójność czasu w systemach, co jest niezbędne dla wiarygodnego rejestrowania i korelacji zdarzeń związanych z bezpieczeństwem informacji w wielu środowiskach.

10.6 P30 – Polityka reagowania na incydenty. Opiera się na danych z logów i mechanizmach alertowania w celu identyfikacji, badania i obsługi incydentów bezpieczeństwa, a także zachowania artefaktów kryminalistycznych na potrzeby przeglądu po incydencie.

11. Normy i ramy odniesienia

11.1 ISO/IEC 27001

11.1.1 Klauzula 8.1 – planowanie operacyjne i nadzór: wymaga wdrożenia środków kontrolnych dla monitorowania operacji oraz ochrony przed nieuprawnionym dostępem i niewłaściwym użyciem systemów.

11.2 ISO/IEC 27002:2022 – środki kontrolne 8.15, 8.16, 8.17

11.2.1 Określa szczegółowe wymagania dotyczące rejestrowania, w tym jakie zdarzenia muszą być rejestrowane, jak chronić i analizować logi oraz jak zapewnić wiarygodność znaczników czasu w systemach.

11.3 NIST SP 800-53 Rev. 5

11.3.1 AU-2 do AU-12: obejmuje dobór zdarzeń, rejestrowanie, ochronę, przegląd audytowy, reakcję na awarie mechanizmów audytowych oraz przechowywanie zapisów audytowych.

11.3.2 SI-4 – monitorowanie systemu: wymaga aktywnego monitorowania systemu z alertami opartymi na aktywności anomalnej.

11.3.3 SC-45 – synchronizacja czasu systemowego: wzmacnia wymaganie dokładności czasu dla identyfikowalności zdarzeń i korelacji incydentów.

11.4 RODO (2016/679)

11.4.1 Artykuł 32 – bezpieczeństwo przetwarzania: wymaga technicznych środków kontrolnych, takich jak rejestrowanie i monitorowanie, w celu zapewnienia bezpieczeństwa i rozliczalności, w szczególności w odniesieniu do dostępu do danych osobowych.

11.5 Dyrektywa NIS2 (2022/2555)

11.5.1 Artykuł 21(2)(e): nakłada obowiązek stosowania systemów rejestrowania zdarzeń i monitorowania w celu szybkiego wykrywania incydentów bezpieczeństwa oraz reagowania na nie.

11.6 Rozporządzenie DORA (2022/2554)

11.6.1 Artykuł 9 – zarządzanie ryzykiem ICT: wymaga mechanizmów wykrywania aktywności anomalnej, rejestrowania incydentów oraz przechowywania danych kryminalistycznych.

11.6.2 Artykuł 11 – testowanie planów ciągłości działania ICT: podkreśla znaczenie ciągłości monitorowania oraz weryfikacji dostępności logów podczas zakłóceń operacyjnych.

11.7 COBIT 2019

11.7.1 DSS01.05 – zarządzanie logami bezpieczeństwa: wymaga wdrożenia zdolności rejestrowania dla całej infrastruktury krytycznej.

11.7.2 DSS05.04 – monitorowanie zdarzeń bezpieczeństwa informacji: nakłada obowiązek monitorowania i analizy logów w czasie rzeczywistym w celu wykrywania zdarzeń i reagowania na nie.

11.7.3 MEA03 – monitorowanie, ocena i weryfikacja zgodności: wymaga regularnego przeglądu praktyk rejestrowania oraz ich zgodności z celami kontrolnymi.