					Wprowadź tutaj nazwę zarejestrowanej osoby prawnej							
Numer dokumentu: P22S					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**

Dostosowanie do norm i regulacji

Norma/regulacja	Klauzula/artykuł	Komentarz
ISO/IEC 27001:2022	Klauzula 8	Zabezpieczenia operacyjne, w tym rejestrowanie
ISO/IEC 27002:2022	Środki kontrolne 8.15, 8.16, 8.17	Rejestrowanie zdarzeń, ochrona logów i monitorowanie
NIST SP 800-53 Rev.5	AU-2 do AU-12, SI-4	Zawartość i przegląd logów audytowych, okres przechowywania, wykrywanie anomalii, alertowanie
RODO	Artykuły 5(1)(f), 32, 33	Poufność i integralność danych, środki techniczne oraz zgłaszanie naruszeń
Dyrektywa NIS2	Artykuły 21(2)(d), 23	Mechanizmy rejestrowania służące wykrywaniu anomalii oraz zgłaszanie incydentów w ciągu 24 godzin
Rozporządzenie DORA	Artykuły 10, 15	Odporność operacyjna, monitorowanie i rejestrowanie dotyczące dostawców usług
COBIT 2019	DSS01.03, DSS05.02	Identyfikowalność działań i ochrona poprzez rejestrowanie i monitorowanie

1. Cel

1.1 Niniejsza polityka ustanawia obowiązkowe wymagania dotyczące rejestrowania i monitorowania w celu zapewnienia bezpieczeństwa, rozliczalności oraz integralności operacyjnej systemów IT organizacji.

1.2 Określa ona rodzaje zdarzeń, które muszą być rejestrowane, sposób przechowywania logów, zasady ich przeglądu oraz odpowiedzialność personelu i dostawców usług.

1.3 Rejestrowanie audytowe i monitorowanie wspierają wykrywanie zagrożeń, zgodność z wymaganiami regulacyjnymi, reagowanie na incydenty oraz analizę kryminalistyczną.

1.4 Niniejsza polityka umożliwia organizacji spełnienie wymagań w zakresie zabezpieczeń operacyjnych wynikających z ISO/IEC 27001 oraz wspiera stałą gotowość audytową, zaufanie klientów i zgodność z RODO, NIS2 oraz DORA.

2. Zakres

2.1 Niniejsza polityka ma zastosowanie do wszystkich systemów i użytkowników w organizacji, w tym do:

2.1.1 stacji roboczych, laptopów, serwerów, zapór sieciowych, przełączników, routerów oraz bezprzewodowych punktów dostępu,

2.1.2 usług chmury obliczeniowej wykorzystywanych do realizacji operacji biznesowych (np. poczty elektronicznej, przechowywania plików, kopii zapasowych, narzędzi do współpracy),

2.1.3 funkcji rejestrowania w oprogramowaniu antywirusowym, aplikacjach, systemach operacyjnych oraz urządzeniach sieciowych,

2.1.4 wszystkich pracowników, kontrahentów oraz dostawców usług zarządzanych (MSP), którzy korzystają z systemów lub nimi administrują,

2.1.5 wszelkich lokalizacji, w których wykorzystywane są firmowe systemy IT, w tym środowisk pracy zdalnej, hybrydowej lub środowisk wykorzystujących prywatne urządzenia (BYOD).

2.2 Polityka ma również zastosowanie do logów generowanych przez usługi stron trzecich, jeżeli organizacja posiada dostęp administracyjny lub umowne prawo do audytu.

3. Cele

3.1 Zapewnienie rejestrowania aktywności systemowej, w tym uwierzytelniania, zmian konfiguracji, dostępu do danych wrażliwych oraz alertów bezpieczeństwa.

3.2 Utrzymywanie bezpiecznych i dokładnych logów w celu wykrywania naruszeń polityk, błędów systemowych lub działań nieuprawnionych.

3.3 Umożliwienie szybkiego przeglądu logów podczas incydentów, postępowań wyjaśniających i audytów.

3.4 Wspieranie synchronizacji czasu w celu zapewnienia integralności oraz korelacji danych logowania.

3.5 Ochrona logów przed manipulacją, utratą lub przedwczesnym usunięciem.

3.6 Spełnienie obowiązków prawnych i regulacyjnych w zakresie rozliczalności systemów, identyfikowalności oraz reakcji na naruszenia.

4. Role i obowiązki

4.1 Dyrektor Generalny (GM)

4.1.1 Zatwierdza niniejszą politykę i zapewnia jej wdrożenie we wszystkich systemach biznesowych.

4.1.2 Dokonuje przeglądu alertów o wysokiej istotności oraz poważnych ustaleń audytowych zgłaszanych przez funkcje IT lub ochrony prywatności.

4.1.3 Zatwierdza odstępstwa w przypadkach, gdy rejestrowanie lub okres przechowywania nie mogą być wymuszone technicznie.

4.2 Dostawca wsparcia IT / wewnętrzna funkcja IT

4.2.1 Wdraża i konfiguruje rejestrowanie dla systemów operacyjnych, urządzeń sieciowych, narzędzi antywirusowych oraz kluczowych aplikacji.

4.2.2 Zapewnia, że logi są przechowywane, objęte kopiami zapasowymi i chronione przed modyfikacją.

4.2.3 Dokonuje przeglądu logów zgodnie z ustalonym harmonogramem oraz analizuje podejrzaną lub nieuprawnioną aktywność.

4.2.4 Utrzymuje mechanizmy alertowania wskazujące anomalne zachowania lub wskaźniki włamania.

[... 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 Coroczny przegląd

9.1.1 Niniejsza polityka musi podlegać przeglądowi co najmniej raz w roku przez Dyrektora Generalnego przy wsparciu dostawcy wsparcia IT oraz Koordynatora ds. prywatności.

9.2 Przesłanki przeglądu

9.2.1 Niezaplanowane przeglądy muszą być przeprowadzane w odpowiedzi na:

9.2.1.1 ustalenia dotyczące logów wynikające z audytów wewnętrznych lub zewnętrznych,

9.2.1.2 incydenty bezpieczeństwa, w których logi były niedostępne, uszkodzone lub niewystarczające,

9.2.1.3 istotne zmiany w infrastrukturze IT (np. migrację do platform rejestrowania w chmurze obliczeniowej),

9.2.1.4 aktualizacje obowiązków prawnych lub regulacyjnych (np. RODO, NIS2, DORA).

9.3 Kontrola wersji

9.3.1 Wszystkie zmiany w niniejszej polityce muszą być rejestrowane wraz z numerem wersji, datą i podsumowaniem zmian.

9.3.2 Poprzednie wersje muszą być archiwizowane i przechowywane przez co najmniej 3 lata.

9.3.3 Zaktualizowane polityki muszą być komunikowane interesariuszom, których dotyczą, w szczególności osobom posiadającym dostęp na poziomie systemowym.

10. Powiązane polityki i zależności

10.1 Niniejsza polityka bezpośrednio wspiera i jest wspierana przez następujące polityki bezpieczeństwa informacji dla SME:

10.1.1 P17S – Polityka ochrony danych i prywatności: zapewnia, że dane w logach zawierające informacje osobowe są zarządzane z zachowaniem integralności, okresu przechowywania i zabezpieczeń dostępu zgodnie z wymaganiami RODO.

10.1.2 P21S – Polityka bezpieczeństwa sieci: stanowi podstawę pozyskiwania logów związanych z zaporami sieciowymi, dostępem bezprzewodowym, VPN oraz monitorowaniem segmentacji.

10.1.3 P24S – Polityka bezpiecznego rozwoju oprogramowania: zapewnia, że logi aplikacyjne (np. dotyczące prób logowania, błędów i wyjątków) są uwzględnione w projektowaniu i eksploatacji oprogramowania.

10.1.4 P30S – Polityka reagowania na incydenty: opiera się na dokładnych i kompletnych danych z logów w celu wykrywania, analizy i reagowania na zdarzenia bezpieczeństwa informacji.

10.1.5 P23S – Polityka synchronizacji czasu: zapewnia spójne i możliwe do prześledzenia znaczniki czasu we wszystkich systemach, umożliwiając korelację logów podczas postępowań wyjaśniających.

11. Normy i ramy odniesienia

11.1 ISO/IEC 27001

11.1.1 Klauzula 8.1 – wymaga wdrożenia zabezpieczeń operacyjnych w celu ograniczania ryzyk bezpieczeństwa informacji, w tym rejestrowania.

11.2 ISO/IEC 27002

11.2.1 Środek kontrolny 8.15 – wymaga rejestrowania zdarzeń w celu wspierania wykrywania anomalii i rozliczalności.

11.2.2 Środek kontrolny 8.16 – wymaga ochrony logów przed manipulacją i nieuprawnionym dostępem.

11.2.3 Środek kontrolny 8.17 – wymaga monitorowania systemów pod kątem nietypowej aktywności oraz potwierdzania skuteczności środków monitorowania.

11.3 NIST SP 800-53 Rev.5

11.3.1 AU-2 do AU-12 – obejmują zawartość logów audytowych, ich przegląd, okres przechowywania oraz automatyczne alertowanie.

11.3.2 SI-4 – wymaga wykrywania anomalii systemowych oraz zgłaszania podejrzanych zdarzeń.

11.4 RODO

11.4.1 Artykuł 5(1)(f) – wymaga zapewnienia integralności i poufności danych osobowych, co obejmuje również rejestrowanie dostępu.

11.4.2 Artykuł 32 – nakłada obowiązek stosowania środków technicznych i organizacyjnych zapewniających bezpieczeństwo, w tym rejestrowania i monitorowania.

11.4.3 Artykuł 33 – wymaga terminowego zgłaszania naruszeń, wspieranego przez logi umożliwiające analizę przyczyny źródłowej.

11.5 Dyrektywa UE NIS2

11.5.1 Artykuł 21(2)(d) – wymaga mechanizmów rejestrowania wykrywających anomalie i wspierających dochodzenia incydentowe.

11.5.2 Artykuł 23 – nakłada obowiązek zgłaszania incydentów w ciągu 24 godzin, co zależy od dokładnych i terminowo dostępnych danych z logów.

11.6 Rozporządzenie DORA

11.6.1 Artykuł 10 – wymaga zapewnienia cyfrowej odporności operacyjnej, w tym identyfikowalności incydentów związanych z ICT poprzez rejestrowanie.

11.6.2 Artykuł 15 – zobowiązuje do monitorowania dostawców usług, w tym do zapewnienia praw dostępu do logów i ich przeglądu.

11.7 COBIT 2019

11.7.1 DSS01.03 – wymaga identyfikowalności aktywności systemowej poprzez rejestrowanie i monitorowanie.

11.7.2 DSS05.02 – wskazuje rejestrowanie jako kluczowy środek kontrolny w ochronie przed złośliwym oprogramowaniem i inną nieuprawnioną aktywnością.