					Wprowadź tutaj nazwę zarejestrowanej osoby prawnej							
Numer dokumentu: P16					Tytuł dokumentu: **Polityka maskowania danych i pseudonimizacji P16S**							
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 6.1	Ogólne wymagania dotyczące zarządzania ryzykiem oraz kontroli operacyjnych w zakresie maskowania danych i pseudonimizacji
ISO/IEC 27002:2022	Środki kontrolne 8.11, 8	Wytyczne dotyczące wdrażania maskowania danych i pseudonimizacji
NIST SP 800-53 Rev.5	PM-17, PT-2, PT-3, SC-12, SC-28, SC-30	Kontrole prywatności i poufności dotyczące minimalizacji danych, transformacji danych oraz ograniczania dostępu
RODO UE	Artykuły 4(5), 5(1)(c,f), 32	Podstawa prawna i wymagania dotyczące pseudonimizacji oraz środków ochrony danych
Dyrektywa UE NIS2	Artykuł 21(2)(c)	Obowiązek stosowania środków technicznych i organizacyjnych, w tym technologii zwiększających prywatność (PET)
Rozporządzenie UE DORA	Artykuły 10(1), 10(2)(e)	Zarządzanie ryzykiem ICT oraz kontrole poufności w zakresie maskowania danych i pseudonimizacji
COBIT 2019	DSS05.01, DSS06.06, MEA	Kontrole ładu zarządczego dotyczące ochrony danych z wykorzystaniem maskowania oraz oceny zgodności

1. Cel

1.1 Niniejsza polityka określa podejście organizacji do wdrażania maskowania danych i pseudonimizacji jako technologii zwiększających prywatność (PET) w celu ograniczenia możliwości identyfikacji oraz ekspozycji danych osobowych lub innych danych wrażliwych.

1.2 Wspiera bezpieczne wykorzystywanie informacji w testach, analizach i działalności operacyjnej, przy jednoczesnym zachowaniu zgodności z wymaganiami prawnymi i regulacyjnymi, ograniczaniu skutków naruszeń oraz stosowaniu zasad minimalizacji danych i poufności.

1.3 Polityka jest zgodna z ISO/IEC 27001:2022, wspiera art. 4(5) RODO w zakresie pseudonimizacji oraz integruje wdrożenie oparte na ryzyku, spójne z normami i ramami NIST, NIS2, DORA oraz COBIT 2019.

2. Zakres

2.1 Niniejsza polityka ma zastosowanie do:

2.1.1 wszystkich pracowników, wykonawców, stron trzecich i dostawców posiadających dostęp do systemów przetwarzających informacje osobowe, poufne lub wrażliwe,

2.1.2 wszystkich środowisk danych, w tym produkcyjnych, rozwojowych i testowych,

2.1.3 wszystkich form maskowania danych (np. statycznego, dynamicznego, deterministycznego, tokenizacji) oraz technik pseudonimizacji stosowanych w celu ograniczenia ryzyk dla prywatności,

2.1.4 wszystkich typów danych (ustrukturyzowanych i nieustrukturyzowanych), systemów (infrastruktura lokalna lub zasoby hostowane w chmurze) oraz aplikacji obejmujących dane osobowe lub dane podlegające regulacjom.

2.2 Zakres obejmuje wykorzystanie w:

2.2.1 rozwoju aplikacji oraz środowiskach QA/testowych,

2.2.2 platformach analitycznych i raportowych,

2.2.3 wymianie danych ze stronami trzecimi lub dostawcami usług,

2.2.4 systemach kopii zapasowych, archiwizacji i odzyskiwania.

3. Cele

3.1 Zapewnienie spójnego i skutecznego stosowania maskowania danych i pseudonimizacji w celu ograniczenia ryzyka ujawnienia danych lub ich niewłaściwego wykorzystania.

3.2 Zapewnienie, że rzeczywiste dane nigdy nie są wykorzystywane w środowiskach nieprodukcyjnych, chyba że zostały przekształcone z użyciem zatwierdzonych technik PET.

3.3 Utrzymanie integralności referencyjnej, użyteczności oraz transformacji zachowujących format, gdy jest to wymagane dla spójności operacyjnej.

3.4 Egzekwowanie ścisłych kontroli dostępu do danych oryginalnych, danych zamaskowanych oraz kluczy ponownej identyfikacji.

3.5 Traktowanie zamaskowanych lub spseudonimizowanych zbiorów danych jako danych wrażliwych, podlegających rejestrowaniu dostępu, kontrolom retencji oraz procedurom reagowania na incydenty.

3.6 Walidacja skuteczności tych kontroli poprzez ciągłe testowanie, monitorowanie oraz procedury audytowe.

4. Role i odpowiedzialności

4.1 Kierownictwo wykonawcze

4.1.1 Zatwierdza niniejszą politykę i zapewnia jej stosowanie jako elementu szerszych inicjatyw w zakresie ładu IT i ochrony danych.

4.2 Dyrektor ds. bezpieczeństwa informacji (CISO) / Kierownik systemu zarządzania bezpieczeństwem informacji

4.2.1 Nadzoruje wdrożenie i bieżącą zgodność.

4.2.2 Zapewnia zgodność z ISO/IEC 27001, klauzulą 6.1.3 (postępowanie z ryzykiem) oraz klauzulą 8.1 (planowanie i nadzór operacyjny).

4.2.3 Dokonuje przeglądu logów audytowych i waliduje skuteczność kontroli.

[... 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 podlega przeglądowi co najmniej raz w roku lub wcześniej w przypadku:

9.1.1 zmian regulacyjnych wpływających na maskowanie danych lub pseudonimizację,

9.1.2 wdrożenia nowych systemów IT przetwarzających dane wrażliwe,

9.1.3 istotnych zmian w schemacie klasyfikacji organizacji,

9.1.4 ustaleń audytowych wskazujących na słabości kontroli,

9.1.5 pojawienia się nowych zagrożeń lub technologii maskowania danych.

9.2 Kierownik systemu zarządzania bezpieczeństwem informacji prowadzi przegląd w konsultacji z inspektorem ochrony danych, właścicielami danych, zespołem bezpieczeństwa IT oraz funkcją prawną.

Aktualizacje muszą podlegać kontroli wersji, zostać zatwierdzone przez kierownictwo najwyższego szczebla oraz zakomunikowane wszystkim zainteresowanym stronom, których dotyczą.

10. Powiązane polityki i zależności

10.1 P13 - Polityka klasyfikacji i oznaczania informacji. Decyzje dotyczące maskowania danych i pseudonimizacji są bezpośrednio zależne od klasyfikacji pól danych oraz poziomów wrażliwości zdefiniowanych w P13.

10.2 P14 - Polityka retencji i utylizacji danych. Przekształcone zbiory danych muszą być przechowywane i utylizowane zgodnie z zasadami cyklu życia określonymi w P14, przy zapewnieniu, że dane zamaskowane i spseudonimizowane są traktowane jako dane wrażliwe.

10.3 P17 - Polityka ochrony danych i prywatności. Określa zasady prywatności i podstawy regulacyjne stosowania pseudonimizacji jako zgodnej czynności przetwarzania na podstawie RODO i podobnych przepisów.

10.4 P22 - Polityka rejestrowania i monitorowania. Umożliwia scentralizowane audytowanie i alertowanie zdarzeń związanych z maskowaniem danych oraz pseudonimizacją zgodnie z ustalonymi protokołami monitorowania bezpieczeństwa.

11. Normy i ramy odniesienia

11.1 ISO/IEC 27001

11.1.1 Klauzula 6.1.3 - plan postępowania z ryzykiem: ustanawia maskowanie danych i pseudonimizację jako mechanizmy postępowania z ryzykiem ograniczające możliwość identyfikacji danych wrażliwych w środowiskach przetwarzania, które nie są niezbędne do działalności operacyjnej.

11.1.2 Klauzula 8.1 - planowanie i nadzór operacyjny: nakłada wymóg stosowania kontroli technicznych i proceduralnych dla bezpiecznej transformacji danych podczas przetwarzania, przechowywania lub transferu.

11.2 ISO/IEC 27002:2022

11.2.1 Środki kontrolne 8.11, 8: wytyczne dotyczące maskowania danych i pseudonimizacji w celu ograniczenia ryzyka ponownej identyfikacji i wycieków.

11.3 NIST SP 800-53 Rev.5

11.3.1 PM-17 - ochrona danych osobowych umożliwiających identyfikację osoby: wdrożenie technologii zwiększających prywatność, takich jak maskowanie danych i pseudonimizacja.

11.3.2 PT-2, PT-3 - minimalizacja i bezpieczeństwo przetwarzania danych osobowych umożliwiających identyfikację osoby: transformacja ograniczająca identyfikowalność oraz wymuszająca kontrolę dostępu.

11.3.3 SC-12, SC-28, SC-30 - poufność i integralność danych: kontrole poufności i zaciemniania danych w przechowywaniu, transmisji i użyciu.

11.4 RODO UE (2016/679)

11.4.1 Artykuł 4(5): formalna definicja pseudonimizacji.

11.4.2 Artykuł 32: bezpieczeństwo przetwarzania - organizacyjne i techniczne środki pseudonimizacji.

11.4.3 Artykuł 5(1)(c,f): minimalizacja danych i poufność z zastosowaniem pseudonimizacji/maskowania.

11.5 Dyrektywa UE NIS2 (2022/2555)

11.5.1 Artykuł 21(2)(c): wymaga stosowania technologii zwiększających prywatność, takich jak maskowanie danych i pseudonimizacja, jako środków bezpieczeństwa.

11.6 Rozporządzenie UE DORA (2022/2554)

11.6.1 Artykuł 10(1): ramy zarządzania ryzykiem ICT obejmują kontrole maskowania danych i pseudonimizacji.

11.6.2 Artykuł 10(2)(e): nakłada obowiązek stosowania technologii transformacji w celu ochrony danych osobowych i finansowych.

11.7 COBIT 2019

11.7.1 DSS05.01: Ochrona aktywów informacyjnych - wymagania dotyczące maskowania danych i pseudonimizacji.

11.7.2 DSS06.06: Bezpieczne testy i analityka - maskowanie danych w środowiskach pozaprodukcyjnych.

11.7.3 MEA03: monitorowanie zgodności w zakresie skuteczności maskowania danych i pseudonimizacji.