					Wprowadź tutaj nazwę zarejestrowanej osoby prawnej							
Numer dokumentu: PII17					Tytuł dokumentu: **Polityka zarządzania udokumentowanymi informacjami i dowodami PIMS**							
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**

Nota prawna (prawa autorskie i ograniczenia użytkowania)

(C) 2025 Clarysec LLC. All rights reserved.

Niniejszy dokument stanowi własność intelektualną spółki Clarysec LLC. Żadna część tego dokumentu nie może być kopiowana, ponownie wykorzystywana, rozpowszechniana ani modyfikowana do celów komercyjnych lub wdrożeniowych bez uprzedniej wyraźnej pisemnej zgody.
Nieuprawnione użycie jest surowo zabronione i może skutkować podjęciem kroków prawnych.
W sprawach licencjonowania prosimy o kontakt: info@clarysec.com

Dostosowanie do norm i regulacji

Norma / regulacja	Klauzula / środek kontrolny / artykuł	Zastosowanie	Typ pokrycia	Komentarz
ISO/IEC 27701:2025	Clause 6.1.3	Both	Supporting	Udokumentowane informacje SoA
ISO/IEC 27701:2025	Clause 7.5	Both	Primary	Udokumentowane informacje PIMS
ISO/IEC 27701:2025	Clause 8.1	Both	Primary	Kontrola dowodów operacyjnych
ISO/IEC 27701:2025	Clause 9.1	Both	Supporting	Dowody monitorowania
ISO/IEC 27701:2025	Clause 9.2	Both	Supporting	Dowody z audytu
ISO/IEC 27701:2025	Clause 9.3	Both	Supporting	Dowody przeglądu zarządzania
ISO/IEC 27701:2025	Clause 10.2	Both	Supporting	Dowody niezgodności i działań korygujących
ISO/IEC 27701:2025	Annex A.1.2.9	Controller	Primary	Rejestry przetwarzania administratora
ISO/IEC 27701:2025	Annex A.2.2.2	Processor	Supporting	Dowody umów i poleceń dla podmiotu przetwarzającego
ISO/IEC 27701:2025	Annex A.3.14	Both	Primary	Ochrona zapisów
GDPR	Article 5(2)	Controller	Supporting	Dowody rozliczalności
GDPR	Article 24	Controller	Supporting	Środki i dowody administratora
GDPR	Article 28	Both	Supporting	Dokumentacja podmiotu przetwarzającego
GDPR	Article 30	Both	Supporting	Rejestry przetwarzania
GDPR	Article 32	Both	Supporting	Ochrona dowodów
ISO/IEC 29100:2020	Clause 5.12	Both	Supporting	Dowody zgodności w zakresie prywatności
ISO/IEC 29151:2022	Clause 18.1.4	Both	Supporting	Ochrona zapisów

ISO/IEC 27001:2022	Clause 7.5	Both	Supporting	Kontrola udokumentowanych informacji
ISO/IEC 27002:2022	Control 5.33	Both	Supporting	Ochrona zapisów
ISO/IEC 27002:2022	Control 5.34	Both	Supporting	Ochrona prywatności i PII

1. Zakres

1.1 Niniejsza polityka określa obowiązkowe wymagania dotyczące tworzenia, zatwierdzania, wersjonowania, ochrony, przechowywania, wyszukiwania, tłumaczenia, wycofywania oraz potwierdzania dowodami udokumentowanych informacji PIMS.

1.2 Niniejsza polityka ma zastosowanie do polityk PIMS, rejestrów, udokumentowanych zatwierdzeń, zapisów dowodowych, dowodów z audytu, zapisów z przeglądów zarządzania, dowodów działań korygujących oraz kontrolowanych tłumaczeń wykorzystywanych do wykazania zgodności PIMS.

1.3 Niniejsza polityka ma zastosowanie w kontekstach administratora, współadministratora, podmiotu przetwarzającego i podwykonawcy przetwarzania.

1.4 Niniejsza polityka nie tworzy odrębnego rejestru kontroli dokumentów. Dowody kontroli udokumentowanych informacji są utrzymywane za pomocą kanonicznych obiektów dowodowych PIMS od REG01 do REG12, przy czym REG03 i REG12 są używane do dowodów stosowalności zabezpieczeń, audytu, niezgodności, działań korygujących i doskonalenia.

2. Cel

2.1 Celem niniejszej polityki jest zapewnienie, aby udokumentowane informacje PIMS były dokładne, kontrolowane, dostępne dla uprawnionych użytkowników, chronione przed nieuprawnioną zmianą lub ujawnieniem, przechowywane w celu zapewnienia audytowalności oraz wycofywane, gdy staną się nieaktualne.

2.2 Niniejsza polityka wspiera gotowość do certyfikacji przez zapewnienie, że dowody potrzebne do wykazania zgodności PIMS mogą zostać zlokalizowane, zweryfikowane, pobrane i powiązane z właściwymi politykami, zabezpieczeniami, czynnościami przetwarzania, ryzykami, audytami i działaniami korygującymi.

3. Cele

3.1 Celami niniejszej polityki są:

3.1.1 określenie wymagań dotyczących kontroli udokumentowanych informacji PIMS;

3.1.2 utrzymywanie integralności dowodów w REG01 do REG12;

3.1.3 zapewnienie identyfikowalności zatwierdzania polityk i dowodów;

3.1.4 zapewnienie udokumentowania historii wersji i decyzji o wycofaniu;

3.1.5 powiązanie dowodów PIMS z Deklaracją stosowania i mapowaniami polityk;

3.1.6 kontrolowanie dostępu do dokumentów PIMS i zapisów dowodowych;

3.1.7 wspieranie kontroli wersji wielojęzycznych polityk i dowodów;

3.1.8 umożliwienie terminowego pobierania dowodów z audytu;

3.1.9 zapobieganie zbędnej biurokracji w zakresie kontroli dokumentów;

3.1.10 zachowanie zapisów gotowych do audytu na potrzeby certyfikacji, zapewnienia dla klientów i ciągłego doskonalenia.

4. Postanowienia polityki

4.1 Kontrola udokumentowanych informacji PIMS

4.1.1 [All] The Privacy Lead / PIMS Manager MUST utrzymywać indeks udokumentowanych informacji PIMS w REG12 przed pierwszą publikacją PIMS, a następnie kwartalnie.

4.1.2 [All] The Process Owner / Business Owner MUST zidentyfikować udokumentowane informacje wymagane dla każdej posiadanej czynności przetwarzania PII w REG02 przed rozpoczęciem czynności przetwarzania, a następnie corocznie.

4.1.3 [All] The Privacy Lead / PIMS Manager MUST powiązać mające zastosowanie polityki PIMS, zabezpieczenia i obowiązki dowodowe z REG03 przed każdym wydaniem polityki oraz w terminie 15 dni roboczych od każdej istotnej zmiany stosowalności zabezpieczeń.

4.1.4 [All] The Privacy Lead / PIMS Manager MUST przypisać poziom dostępu oraz klasyfikację wrażliwości dowodów do każdej kategorii udokumentowanych informacji PIMS w REG12 przed użyciem tej kategorii.

4.2 Tworzenie, zatwierdzanie, wersjonowanie i publikacja

4.2.1 [All] The Privacy Lead / PIMS Manager MUST przypisać identyfikator dokumentu, właściciela, numer wersji, status zatwierdzenia, datę wejścia w życie i datę przeglądu w REG12 przed opublikowaniem udokumentowanych informacji PIMS.

4.2.2 [All] Top Management MUST zatwierdzić podstawowe polityki PIMS oraz istotne zmiany polityk w REG12 przed publikacją.

4.2.3 [All] The Privacy Lead / PIMS Manager MUST zatwierdzić szablony dowodów PIMS lub wbudowane sekcje rejestrów w REG12 przed użyciem operacyjnym.

4.2.4 [All] The Privacy Lead / PIMS Manager MUST odnotować historię wersji i uzasadnienie zmiany w REG12 przed wydaniem zaktualizowanych udokumentowanych informacji PIMS.

4.2.5 [All] The Privacy Lead / PIMS Manager MUST odnotować komunikację zatwierdzonych zmian udokumentowanych informacji PIMS w REG11 w terminie 30 dni od publikacji.

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

9. Wyjątki

9.1.1 [All] The Process Owner / Business Owner MUST wnioskować o wyjątki dotyczące udokumentowanych informacji lub kontroli dowodów w REG12 przed odstąpieniem od niniejszej polityki.

9.1.2 [All] The Privacy Lead / PIMS Manager MUST ocenić każdy wyjątek dotyczący udokumentowanych informacji lub kontroli dowodów w REG12 w terminie 10 dni roboczych od wniosku.

9.1.3 [All] The Data Protection Officer / Privacy Advisor MUST odnotować poradę w REG12 przed zatwierdzeniem każdego wyjątku obejmującego ujawnienie dowodów PII, rozbieżność tłumaczeniową, konflikt retencji lub ograniczenie dowodów z audytu.

9.1.4 [All] Top Management MUST zatwierdzić w REG12 wyjątki dotyczące udokumentowanych informacji przekraczające 30 dni lub wpływające na certyfikację, przetwarzanie wysokiego ryzyka lub zewnętrzne zapewnienie, zanim wyjątek zacznie obowiązywać.

9.1.5 [All] The Privacy Lead / PIMS Manager MUST ustalić w REG12 datę wygaśnięcia nieprzekraczającą 90 dni dla każdego zatwierdzonego wyjątku dotyczącego udokumentowanych informacji lub kontroli dowodów.

9.1.6 [All] The Privacy Lead / PIMS Manager MUST zamknąć lub ponownie ocenić każdy wyjątek dotyczący udokumentowanych informacji lub kontroli dowodów w REG12 w terminie pięciu dni roboczych od wygaśnięcia.

10. Egzekwowanie postanowień polityki

10.1.1 [All] The Privacy Lead / PIMS Manager MUST odnotować brakujące, niedokładne, niekontrolowane, nieaktualne lub niemożliwe do pobrania udokumentowane informacje PIMS jako niezgodność w REG12 w terminie pięciu dni roboczych od ich zidentyfikowania.

10.1.2 [All] The Privacy Lead / PIMS Manager MUST zapobiegać publikacji udokumentowanych informacji PIMS, gdy w REG12 brakuje wymaganych dowodów zatwierdzenia, wersji, właściciela lub daty wejścia w życie.

10.1.3 [All] The Process Owner / Business Owner MUST zapobiegać przekazaniu do audytu dowodów przetwarzania, w przypadku których w REG02 brakuje wymaganych dowodów właściciela, daty, statusu lub zatwierdzenia.

10.1.4 [All] The System Owner / Application Owner MUST usunąć nieuprawniony dostęp do repozytoriów udokumentowanych informacji PIMS i odnotować jego usunięcie w REG12 w terminie jednego dnia roboczego od zidentyfikowania.

10.1.5 [All] The Internal Audit / Compliance Reviewer MUST zweryfikować skuteczność działań korygujących dotyczących niezgodności w zakresie udokumentowanych informacji w REG12 podczas następnego zaplanowanego audytu albo w terminie 60 dni od zamknięcia, w zależności od tego, co nastąpi wcześniej.

11. Przegląd i utrzymanie

11.1.1 [All] The Privacy Lead / PIMS Manager MUST przeglądać niniejszą politykę corocznie oraz w terminie 30 dni od istotnej zmiany wymagań dotyczących udokumentowanych informacji PIMS.

11.1.2 [All] The Privacy Lead / PIMS Manager MUST przeglądać niniejszą politykę w terminie 30 dni po istotnym ustaleniu z audytu, niezgodności certyfikacyjnej, zmianie platformy repozytorium lub zmianie procesu publikacji wielojęzycznej.

11.1.3 [All] The Data Protection Officer / Privacy Advisor MUST przeglądać zmiany niniejszej polityki istotne z perspektywy prywatności w REG12 przed zatwierdzeniem.

11.1.4 [All] Top Management MUST zatwierdzać istotne zmiany niniejszej polityki w REG12 przed publikacją.

11.1.5 [All] The Privacy Lead / PIMS Manager MUST odnotować komunikację zatwierdzonych zmian niniejszej polityki w REG11 w terminie 30 dni od publikacji.

12. Powiązane polityki

12.1 Niniejsza polityka jest wspierana przez następujące powiązane polityki:

12.2 PII01 - Polityka systemu zarządzania informacjami o prywatności

12.3 PII02 - Polityka ról, odpowiedzialności i rozliczalności w zakresie prywatności

12.4 PII03 - Polityka inwentaryzacji przetwarzania PII i podstaw prawnych

12.5 PII04 - Polityka klauzul informacyjnych i przejrzystości

12.6 PII05 - Polityka zarządzania zgodami i preferencjami

12.7 PII06 - Polityka zarządzania prawami osób, których dane dotyczą

12.8 PII07 - Polityka oceny ryzyka dla prywatności i DPIA

12.9 PII08 - Polityka privacy by design i privacy by default

12.10 PII09 - Polityka zbierania, wykorzystywania, ujawniania i udostępniania PII

12.11 PII10 - Polityka retencji, usuwania i utylizacji PII

12.12 PII11 - Polityka prawidłowości i jakości PII

12.13 PII12 - Polityka zarządzania prywatnością podmiotów przetwarzających, podwykonawców przetwarzania i stron trzecich

12.14 PII13 - Polityka międzynarodowych transferów PII

12.15 PII14 - Polityka bezpieczeństwa PII i kontroli dostępu

12.16 PII15 - Polityka zarządzania incydentami i naruszeniami PII

12.17 PII16 - Polityka szkoleń, świadomości i kompetencji w zakresie prywatności

12.18 PII18 - Polityka monitorowania, audytu i doskonalenia PIMS

13. Normy i ramy odniesienia

13.1 Niniejsza polityka jest zmapowana do następujących norm i regulacji. Mapowanie wyjaśnia, w jaki sposób polityka wspiera przywołane wymagania, oraz identyfikuje wewnętrzne klauzule, które je wdrażają lub wspierają.

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 6.1.3** - Zmapowano do utrzymywania Deklaracji stosowania PIMS, zapisów stosowalności zabezpieczeń oraz powiązania polityk z dowodami. Addressed by clauses [4.1.3; 4.3.3; 6.1.3; 7.1.2].

13.2.2 **Clause 7.5** - Zmapowano do identyfikacji udokumentowanych informacji, zatwierdzania, kontroli wersji, dostępu, pobierania, zachowania, wycofywania, powiązania wersji tłumaczeń oraz metadanych retencji. Addressed by clauses [4.1.1; 4.1.4; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.3.1; 4.3.5; 4.4.1; 4.4.2; 4.4.4; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.6.1; 4.6.2; 4.6.3; 4.6.4].

13.2.3 **Clause 8.1** - Zmapowano do dowodów planowania i kontroli operacyjnej dotyczących rejestrów przetwarzania, szablonów dowodów, jakości dowodów operacyjnych oraz dowodów dostarczanych zewnętrznie. Addressed by clauses [4.1.2; 4.2.3; 4.3.2; 7.1.3; 7.1.4].

13.2.4 **Clause 9.1** - Zmapowano do utrzymywania udokumentowanych dowodów pomiarów, efektywności pobierania, luk dowodowych, niezgodności tłumaczeń oraz ukończenia przeglądu dostępu do repozytorium. Addressed by clauses [8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 8.1.6].

13.2.5 **Clause 9.2** - Zmapowano do pobierania dowodów z audytu, próbkowania audytowego, identyfikowalności dowodów z audytu oraz ustaleń z audytu dotyczących kontroli udokumentowanych informacji. Addressed by clauses [4.3.4; 4.4.4; 6.1.3; 8.1.3; 10.1.5].

13.2.6 **Clause 9.3** - Zmapowano do dowodów przeglądu zarządzania, uwzględniania kontroli udokumentowanych informacji w przeglądzie zarządzania oraz przeglądu wyników kontroli dowodów przez Top Management. Addressed by clauses [6.1.2; 8.1.1; 8.1.2; 11.1.4].

13.2.7 **Clause 10.2** - Zmapowano do niezgodności dotyczących udokumentowanych informacji, działań korygujących, obsługi wyjątków, zamknięcia oraz weryfikacji skuteczności. Addressed by clauses [4.3.4; 6.1.4; 9.1.1; 9.1.2; 9.1.4; 9.1.5; 9.1.6; 10.1.1; 10.1.5].

13.2.8 **Annex A.1.2.9** - Zmapowano do rejestrów przetwarzania administratora, zapisów rozliczalności, jakości dowodów przetwarzania oraz przechowywania dowodów wspierających obowiązki administratora. Addressed by clauses [4.1.2; 4.3.2; 4.5.1; 7.1.3].

13.2.9 **Annex A.2.2.2** - Zmapowano do umów podmiotu przetwarzającego, poleceń klientów, dowodów dostarczanych zewnętrznie oraz kontroli dowodów relacji z podmiotem przetwarzającym. Addressed by clauses [5.1.7; 7.1.4].

13.2.10 **Annex A.3.14** - Zmapowano do ochrony zapisów PIMS przed utratą, nieuprawnioną zmianą, nieuprawnionym dostępem, nieuprawnionym wydaniem oraz niewłaściwą utylizacją. Addressed by clauses [4.1.4; 4.4.1; 4.4.2; 4.4.3; 4.4.5; 4.5.2; 4.5.4; 4.5.5; 10.1.4].

13.3 GDPR

13.3.1 **Article 5(2)** - Zmapowano do dowodów rozliczalności, identyfikowalności dowodów, pobierania dowodów, zapisów niezgodności oraz zapisów gotowych do audytu, które wykazują zgodność. Addressed by clauses [4.1.1; 4.3.2; 4.3.3; 4.4.4; 4.5.4; 6.1.3; 8.1.3; 10.1.1].

13.3.2 **Article 24** - Zmapowano do dowodów zarządzania po stronie administratora, zapisów zatwierdzeń, kontroli polityk, środków rozliczalności, udokumentowanego przeglądu oraz nadzoru Top Management. Addressed by clauses [4.2.2; 4.3.3; 6.1.2; 9.1.4; 11.1.4].

13.3.3 **Article 28** - Zmapowano do dokumentacji podmiotów przetwarzających i podwykonawców przetwarzania, dowodów poleceń klientów, zewnętrznie dostarczanych dowodów procesu oraz kontroli ujawniania dowodów. Addressed by clauses [4.4.5; 5.1.7; 7.1.4].

13.3.4 **Article 30** - Zmapowano do dowodów rejestrów przetwarzania, wymagań jakości dowodów, odniesień do czynności przetwarzania oraz metadanych właściciela/statusu dowodów przetwarzania. Addressed by clauses [4.1.2; 4.3.2; 7.1.3; 10.1.3].

13.3.5 **Article 32** - Zmapowano do ochrony repozytoriów dowodów, ograniczeń dostępu, zatwierdzeń dostępu, przeglądu ochrony repozytoriów oraz usuwania nieuprawnionego dostępu. Addressed by clauses [4.1.4; 4.4.1; 4.4.2; 4.4.3; 4.4.5; 4.5.5; 10.1.4].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 5.12** - Zmapowano do dowodów zgodności w zakresie prywatności, pobierania dowodów z audytu, identyfikowalności dowodów, wsparcia niezależnego przeglądu oraz dowodów działań korygujących. Addressed by clauses [4.3.3; 4.4.4; 4.6.3; 6.1.3; 8.1.3; 10.1.5].

13.5 ISO/IEC 29151:2022

13.5.1 **Clause 18.1.4** - Zmapowano do ochrony zapisów związanych z PII, zachowania zapisów oraz kontroli dostępu do repozytoriów dowodów i usuwania. Addressed by clauses [4.1.4; 4.4.1; 4.4.2; 4.4.3; 4.5.2; 4.5.5; 10.1.4].

13.6 ISO/IEC 27001:2022

13.6.1 **Clause 7.5** - Zmapowano do identyfikacji udokumentowanych informacji, zatwierdzania, dostępności, ochrony, kontroli wersji, retencji, rozporządzania oraz kontroli udokumentowanych informacji wymaganych zewnętrznie. Addressed by clauses [4.1.1; 4.2.1; 4.2.4; 4.3.1; 4.4.1; 4.5.1; 4.5.2; 4.5.3; 4.6.1; 4.6.2; 4.6.4].

13.7 ISO/IEC 27002:2022

13.7.1 Control 5.33 - Zmapowano do ochrony zapisów PIMS przed utratą, zniszczeniem, fałszowaniem, nieuprawnionym dostępem, nieuprawnionym wydaniem oraz niewłaściwą utylizacją. Addressed by clauses [4.1.4; 4.4.1; 4.4.2; 4.4.3; 4.4.5; 4.5.5; 10.1.4].

13.7.2 Control 5.34 - Zmapowano do ochrony prywatności i PII w udokumentowanych informacjach, repozytoriach dowodów, ujawnieniach oraz zapisach objętych kontrolą dostępu. Addressed by clauses [4.1.4; 4.4.2; 4.4.3; 4.4.5; 4.5.5; 6.1.5].