					Wprowadź tutaj nazwę zarejestrowanej osoby prawnej							
Numer dokumentu: PII02					Tytuł dokumentu: **Polityka ról, odpowiedzialności i rozliczalności w zakresie prywatności**							
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 / środek kontrolny / artykuł	Applicability	Coverage Type	Komentarz
ISO/IEC 27701:2025	Clause 4.1	Both	Primary	Kontekst roli PIMS
ISO/IEC 27701:2025	Clause 5.1	Both	Primary	Przywództwo i rozliczalność
ISO/IEC 27701:2025	Clause 5.3	Both	Primary	Role, odpowiedzialności i uprawnienia w PIMS
ISO/IEC 27701:2025	Clause 7.2	Both	Primary	Kompetencje związane z rolami
ISO/IEC 27701:2025	Clause 7.3	Both	Primary	Świadomość związana z rolami
ISO/IEC 27701:2025	Clause 7.4	Both	Supporting	Komunikacja dotycząca ról
ISO/IEC 27701:2025	Clause 7.5	Both	Primary	Udokumentowane informacje dotyczące ról
ISO/IEC 27701:2025	Clause 8.1	Both	Primary	Własność kontroli operacyjnej
ISO/IEC 27701:2025	Clause 9.2	Both	Supporting	Niezależna rola audytowa
ISO/IEC 27701:2025	Clause 9.3	Both	Supporting	Przegląd zarządzania dotyczący rozliczalności
ISO/IEC 27701:2025	Clause 10.2	Both	Supporting	Niezgodności i działania korygujące związane z rolami
ISO/IEC 27701:2025	Annex A.1.2.7	Controller	Supporting	Odpowiedzialność za umowę z podmiotem przetwarzającym
ISO/IEC 27701:2025	Annex A.1.2.8	Joint Controller	Primary	Role i odpowiedzialności współadministratorów
ISO/IEC 27701:2025	Annex A.1.2.9	Controller	Primary	Zapisy dotyczące rozliczalności
ISO/IEC 27701:2025	Annex A.2.2.2	Processor	Primary	Umowy i instrukcje klienta dotyczące podmiotu przetwarzającego

ISO/IEC 27701:2025	Annex A.2.2.3	Processor	Supporting	Zgodność celu podmiotu przetwarzającego
GDPR	Article 5(2)	Controller	Supporting	Dowody rozliczalności
GDPR	Article 24	Controller	Supporting	Odpowiedzialność administratora i środki
GDPR	Article 26	Joint Controller	Supporting	Uzgodnienia między współadministratorami
GDPR	Article 28	Both	Supporting	Nadzór nad podmiotami przetwarzającymi i instrukcje
GDPR	Article 30	Both	Supporting	Rejestry przetwarzania i dowody odpowiedzialności
GDPR	Article 37	Conditional	Referenced	Wyznaczenie DPO, gdy ma zastosowanie
GDPR	Article 38	Conditional	Supporting	Pozycja i niezależność DPO, gdy ma zastosowanie
GDPR	Article 39	Conditional	Supporting	Zadania DPO, gdy ma zastosowanie
ISO/IEC 29100:2020	Clause 4.1; Clause 4.2	Both	Supporting	Uczestnicy i role w strukturze ochrony prywatności
ISO/IEC 29100:2020	Clause 5.12	Both	Supporting	Rozliczalność zgodności w zakresie prywatności
ISO/IEC 29151:2022	Clause 6.1.2; Clause 6.1.3	Both	Supporting	Role ochrony PII i rozdzielenie obowiązków
ISO/IEC 27002:2022	Control 5.2	Both	Supporting	Role i odpowiedzialności w zakresie bezpieczeństwa informacji
ISO/IEC 27002:2022	Control 5.3	Both	Supporting	Rozdzielenie obowiązków

1. Zakres

1.1 Niniejsza polityka określa model ról PIMS, strukturę rozliczalności, zasady przypisywania odpowiedzialności, zasady łączenia ról, oczekiwania dotyczące eskalacji oraz wymagania dowodowe dla ładu prywatności.

1.2 Niniejsza polityka ma zastosowanie do personelu, funkcji, systemów, dostawców, podmiotów przetwarzających, podwykonawców przetwarzania oraz relacji współadministratorów, które uczestniczą w przetwarzaniu PII w zakresie PIMS lub na nie wpływają.

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

1.4 Niniejsza polityka nie tworzy nowych stanowisk organizacyjnych. Określa kanoniczne role PIMS, które mogą być przypisane istniejącemu personelowi lub funkcjom, pod warunkiem udokumentowania przypisania roli, kompetencji, niezależności oraz wymagań dotyczących konfliktu interesów.

2. Cel

2.1 Celem niniejszej polityki jest zapewnienie, że odpowiedzialności w PIMS są jasno przypisane, zrozumiane, zakomunikowane, udokumentowane dowodowo, przeglądane i doskonalone.

2.2 Niniejsza polityka umożliwia organizacji wykazanie rozliczalności za ład prywatności, własność przetwarzania PII, ustalenie roli administratora i podmiotu przetwarzającego, podział odpowiedzialności współadministratorów, obsługę instrukcji dla podmiotu przetwarzającego, odpowiedzialność dostawców w zakresie prywatności, niezależny przegląd oraz eskalację opartą na rolach.

3. Cele

3.1 Celami niniejszej polityki są:

3.1.1 zdefiniowanie kanonicznych ról PIMS stosowanych w całym zestawie polityk PIMS;

3.1.2 zapewnienie, że każda istotna odpowiedzialność PIMS ma przypisaną rolę rozliczalną;

3.1.3 wsparcie rozliczalności administratora, współadministratora, podmiotu przetwarzającego i podwykonawcy przetwarzania;

3.1.4 umożliwienie praktycznego łączenia ról w małych i średnich organizacjach przy jednoczesnym kontrolowaniu konfliktów interesów;

3.1.5 zachowanie niezależnego przeglądu wykonywanego przez Internal Audit / Compliance Reviewer;

3.1.6 zapewnienie, że przypisania ról i zmiany ról są rejestrowane w kanonicznych obiektach dowodowych;

3.1.7 zapewnienie, że osoby pełniące role PIMS otrzymują odpowiednią komunikację i działania podnoszące świadomość;

3.1.8 zapewnienie, że luki, konflikty i niezgodności związane z rolami są eskalowane i korygowane.

4. Postanowienia polityki

4.1 Model ról PIMS i przypisanie

4.1.1 [All] Top Management MUSI zatwierdzić kanoniczny model ról PIMS w REG01 przed początkowym wdrożeniem PIMS, a następnie co roku.

4.1.2 [All] Privacy Lead / PIMS Manager MUSI utrzymywać imienne przypisania ról PIMS w REG01 przed wdrożeniem PIMS oraz w ciągu 10 dni roboczych od zmian personalnych lub organizacyjnych.

4.1.3 [All] Privacy Lead / PIMS Manager MUSI udokumentować zakres odpowiedzialności i poziom uprawnień dla każdej przypisanej roli PIMS w REG01 przed rozpoczęciem obowiązywania przypisania.

4.1.4 [All] Process Owner / Business Owner MUSI przypisać rozliczalnego właściciela przetwarzania dla każdej czynności przetwarzania PII w REG02 przed rozpoczęciem tej czynności przetwarzania.

4.1.5 [All] System Owner / Application Owner MUSI udokumentować rozliczalnego właściciela systemu dla każdego systemu przetwarzającego PII w REG02 przed uruchomieniem produkcyjnym systemu.

4.1.6 [All] Vendor / Procurement Owner MUSI udokumentować właściciela relacji dla każdego podmiotu przetwarzającego, podwykonawcy przetwarzania, udostępniania danych stronie trzeciej lub relacji współadministratorów w REG08 przed onboardingiem albo zatwierdzeniem umowy.

4.2 Łączenie ról, rozdzielenie i niezależność

4.2.1 [All] Privacy Lead / PIMS Manager MUSI udokumentować każde połączenie ról PIMS w REG01 przed rozpoczęciem obowiązywania takiego połączenia ról.

4.2.2 [All] Top Management MUSI zatwierdzić w REG01, przed przypisaniem, połączenia ról obejmujące Privacy Lead / PIMS Manager, Data Protection Officer / Privacy Advisor, Information Security Lead, Incident Response Coordinator lub Internal Audit / Compliance Reviewer.

4.2.3 [All] Internal Audit / Compliance Reviewer MUSI udokumentować w REG12 niezależność od procesu PIMS podlegającego przeglądowi przed rozpoczęciem każdego audytu PIMS lub przeglądu zgodności.

4.2.4 [All] Privacy Lead / PIMS Manager MUSI odnotować środki kompensujące dla nieuniknionych konfliktów związanych z rozdzieleniem obowiązków w REG12 przed zatwierdzeniem połączenia ról.

4.2.5 [All] Data Protection Officer / Privacy Advisor MUSI odnotować obawy dotyczące niezależności roli lub konfliktu interesów w REG12 w ciągu pięciu dni roboczych od ich zidentyfikowania.

[... 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] Process Owner / Business Owner MUSI wnioskować o wyjątek od rozliczalności roli w REG12 przed prowadzeniem czynności przetwarzania PII bez wymaganej przypisanej roli.

9.1.2 [All] Privacy Lead / PIMS Manager MUSI ocenić wpływ i środki łagodzące dla każdego wyjątku od rozliczalności roli w REG12 w ciągu 10 dni roboczych od wniosku.

9.1.3 [All] Top Management MUSI zatwierdzić w REG12 wyjątki od rozliczalności roli przekraczające 30 dni lub wpływające na przetwarzanie wysokiego ryzyka przed rozpoczęciem obowiązywania wyjątku.

9.1.4 [All] Privacy Lead / PIMS Manager MUSI ustalić w REG12 datę wygaśnięcia nieprzekraczającą 90 dni dla każdego zatwierdzonego wyjątku od rozliczalności roli przed zatwierdzeniem.

9.1.5 [All] Privacy Lead / PIMS Manager MUSI zamknąć lub ponownie ocenić każdy wyjątek od rozliczalności roli w REG12 w ciągu pięciu dni roboczych od jego wygaśnięcia.

10. Egzekwowanie postanowień

10.1.1 [All] Privacy Lead / PIMS Manager MUSI odnotować brakujące, niedokładne lub nieaktualne przypisania ról PIMS jako niezgodności w REG12 w ciągu pięciu dni roboczych od ich zidentyfikowania.

10.1.2 [All] Top Management MUSI wymagać działań korygujących w REG12 w ciągu 15 dni roboczych w przypadku powtarzających się lub przedłużających się uchybień w rozliczalności.

10.1.3 [All] Process Owner / Business Owner MUSI uniemożliwić uruchomienie produkcyjne nowego lub zmienionego przetwarzania PII, jeżeli wymagane dowody roli i rozliczalności są nieobecne w REG02 lub REG08.

10.1.4 [All] Internal Audit / Compliance Reviewer MUSI zweryfikować skuteczność działań korygujących dotyczących niezgodności w zakresie rozliczalności ról w REG12 podczas następnego zaplanowanego audytu albo w ciągu 60 dni od zamknięcia, w zależności od tego, co nastąpi wcześniej.

11. Przegląd i utrzymanie

11.1.1 [All] Privacy Lead / PIMS Manager MUSI dokonywać przeglądu niniejszej polityki co roku oraz w ciągu 30 dni od istotnej zmiany modelu ról PIMS.

11.1.2 [All] Data Protection Officer / Privacy Advisor MUSI przeglądać proponowane zmiany niniejszej polityki pod kątem wpływu na role związane z prywatnością w REG12 przed zatwierdzeniem.

11.1.3 [All] Top Management MUSI zatwierdzać istotne zmiany niniejszej polityki w REG12 przed publikacją.

11.1.4 [All] Privacy Lead / PIMS Manager MUSI zaktualizować REG01 i REG11 w ciągu 15 dni roboczych po zatwierdzonych zmianach ról, odpowiedzialności lub wymagań komunikacyjnych PIMS.

12. Powiązane polityki

12.1 Niniejsza polityka jest wspierana przez następujące powiązane polityki:

12.2 PII01 - Polityka systemu zarządzania informacjami o prywatności

12.3 PII03 - Polityka inwentaryzacji przetwarzania PII i podstawy prawnej

12.4 PII07 - Polityka oceny ryzyka dla prywatności i DPIA

12.5 PII08 - Polityka privacy by design i privacy by default

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

12.7 PII14 - Polityka bezpieczeństwa PII i kontroli dostępu

12.8 PII15 - Polityka zarządzania incydentami i naruszeniami dotyczącymi PII

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

12.10 PII17 - Polityka udokumentowanych informacji i zarządzania dowodami PIMS

12.11 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 wskazuje wewnętrzne klauzule, które je wdrażają lub wspierają.

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 4.1** - Zmapowano do określania kontekstu roli PIMS, stosowania roli administratora i podmiotu przetwarzającego, własności przetwarzania oraz zapisów odpowiedzialności za relacje. Addressed by clauses [4.3.5; 5.1.5; 5.1.7; 7.1.2].

13.2.2 **Clause 5.1** - Zmapowano do zatwierdzenia przez Top Management, nadzoru nad rozliczalnością, rocznego przeglądu zarządzania, wskaźników rozliczalności oraz działań korygujących w przypadku uchybień dotyczących ról. Addressed by clauses [4.1.1; 4.2.2; 5.1.1; 6.1.1; 8.1.6; 10.1.2; 11.1.3].

13.2.3 **Clause 5.3** - Zmapowano do przypisywania, dokumentowania, komunikowania i utrzymywania ról, odpowiedzialności i uprawnień PIMS, własności systemu, własności przetwarzania, własności relacji z dostawcami, własności eskalacji incydentów oraz odpowiedzialności za niezależny przegląd. Addressed by clauses [4.1.2; 4.1.3; 4.1.4; 4.1.5; 4.1.6; 4.4.2; 4.4.3; 5.1.2; 5.1.3; 5.1.4; 5.1.5; 5.1.6; 5.1.7; 5.1.8; 5.1.9].

13.2.4 **Clause 7.2** - Zmapowano do dowodów kompetencji i świadomości specyficznych dla roli w odniesieniu do przypisanych odpowiedzialności PIMS. Addressed by clauses [7.1.4; 8.1.5].

13.2.5 **Clause 7.3** - Zmapowano do świadomości przypisanych odpowiedzialności PIMS, dowodów potwierdzenia przyjęcia do wiadomości oraz rocznego raportowania świadomości dotyczącej ról. Addressed by clauses [4.5.1; 4.5.2; 7.1.4; 8.1.5].

13.2.6 **Clause 7.4** - Zmapowano do komunikacji dotyczącej przypisań ról, zmian ról, eskalacji oraz informacji o przekazaniu roli. Addressed by clauses [4.5.1; 4.5.4; 6.1.5; 7.1.6].

13.2.7 **Clause 7.5** - Zmapowano do udokumentowanych informacji dotyczących przypisań ról PIMS, zakresów odpowiedzialności, poziomów uprawnień, rocznego przechowywania dowodów oraz utrzymania macierzy ról. Addressed by clauses [4.1.2; 4.1.3; 4.5.3; 7.1.1; 11.1.4].

13.2.8 **Clause 8.1** - Zmapowano do własności kontroli operacyjnej dla czynności przetwarzania, systemów, dostawców, podmiotów przetwarzających, podwykonawców przetwarzania, relacji współadministratorów oraz kontroli uruchomienia produkcyjnego. Addressed by clauses [4.1.4; 4.1.5; 4.1.6; 7.1.2; 7.1.3; 7.1.5; 10.1.3].

13.2.9 **Clause 9.2** - Zmapowano do niezależnego audytu i przeglądu zgodności dowodów przypisania ról, dowodów łączenia ról, dowodów niezależności, ustaleń oraz zamknięcia działań korygujących. Addressed by clauses [4.2.3; 5.1.9; 6.1.4; 8.1.4; 10.1.4].

13.2.10 **Clause 9.3** - Zmapowano do przeglądu zarządzania dotyczącego kompletności przypisania ról PIMS, konfliktów ról, wyjątków, wskaźników rozliczalności oraz wyników przeglądu rozliczalności. Addressed by clauses [5.1.1; 6.1.1; 8.1.6; 11.1.1].

13.2.11 **Clause 10.2** - Zmapowano do eskalacji, rejestrowania niezgodności, działań korygujących, zamykania wyjątków oraz weryfikacji skuteczności w odniesieniu do kwestii rozliczalności ról. Addressed by clauses [4.2.5; 4.4.5; 6.1.5; 9.1.5; 10.1.1; 10.1.2; 10.1.4].

13.2.12 **Annex A.1.2.7** - Zmapowano do przypisywania i dokumentowania odpowiedzialności za umowę z podmiotem przetwarzającym oraz eskalacji odpowiedzialności strony trzeciej przed zatwierdzeniem lub odnowieniem umowy. Addressed by clauses [4.1.6; 4.4.4; 5.1.7; 7.1.3].

13.2.13 **Annex A.1.2.8** - Zmapowano do dokumentowania podziału odpowiedzialności współadministratorów oraz dowodów odpowiedzialności za relację przed rozpoczęciem przetwarzania przez współadministratorów. Addressed by clauses [4.3.2; 5.1.7; 7.1.3; 8.1.3].

13.2.14 **Annex A.1.2.9** - Zmapowano do utrzymywania zapisów rozliczalności dotyczących własności przetwarzania przez administratora, klasyfikacji ról i własności dowodów. Addressed by clauses [4.3.1; 4.3.5; 4.5.3; 8.1.1].

13.2.15 **Annex A.2.2.2** - Zmapowano do odpowiedzialności za umowę klienta podmiotu przetwarzającego, własności instrukcji klienta oraz dowodów relacji z podmiotem przetwarzającym. Addressed by clauses [4.3.3; 5.1.7; 7.1.3; 8.1.3].

13.2.16 **Annex A.2.2.3** - Zmapowano do zgodności celu i instrukcji podmiotu przetwarzającego poprzez własność instrukcji klienta oraz weryfikację roli administratora/podmiotu przetwarzającego. Addressed by clauses [4.3.3; 4.3.5; 5.1.7].

13.3 GDPR

13.3.1 **Article 5(2)** - Zmapowano do dowodów rozliczalności dla przypisań ról, własności przetwarzania, przeglądów ról, niezgodności oraz ustaleń z audytu. Addressed by clauses [4.5.3; 6.1.2; 8.1.1; 10.1.1].

13.3.2 **Article 24** - Zmapowano do odpowiedzialności administratora, rozliczalnej własności przetwarzania, nadzoru Top Management, rocznego przeglądu oraz środków rozliczalności. Addressed by clauses [4.1.1; 4.3.1; 5.1.1; 6.1.1; 8.1.6].

13.3.3 **Article 26** - Zmapowano do dokumentowania podziału odpowiedzialności współadministratorów oraz dowodów odpowiedzialności za relację przed rozpoczęciem przetwarzania przez współadministratorów. Addressed by clauses [4.3.2; 5.1.7; 7.1.3; 8.1.3].

13.3.4 **Article 28** - Zmapowano do podziału odpowiedzialności podmiotu przetwarzającego i podwykonawcy przetwarzania, własności instrukcji klienta, odpowiedzialności za umowę oraz ścieżek eskalacji stron trzecich. Addressed by clauses [4.3.3; 4.3.4; 4.4.4; 5.1.7; 7.1.3].

13.3.5 **Article 30** - Zmapowano do rejestrów przetwarzania, własności przetwarzania, klasyfikacji ról PIMS oraz weryfikacji roli administratora/podmiotu przetwarzającego. Addressed by clauses [4.1.4; 4.3.1; 4.3.5; 8.1.1].

13.3.6 **Article 37** - Zmapowano do dokumentowania roli Data Protection Officer / Privacy Advisor, gdy wyznaczenie ma zastosowanie lub nastąpiło dobrowolnie. Addressed by clauses [4.1.2; 4.1.3; 5.1.3; 11.1.2].

13.3.7 **Article 38** - Zmapowano do pozycji, niezależności, zaangażowania oraz obsługi konfliktu interesów Data Protection Officer / Privacy Advisor, gdy ma zastosowanie. Addressed by clauses [4.2.5; 5.1.3; 6.1.3; 11.1.2].

13.3.8 **Article 39** - Zmapowano do porad dotyczących prywatności, obserwacji z monitorowania, przeglądu doradczego oraz przeglądu wpływu na prywatność związanego z rolą przez Data Protection Officer / Privacy Advisor, gdy ma zastosowanie. Addressed by clauses [4.4.1; 5.1.3; 6.1.3; 11.1.2].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 4.1; Clause 4.2** - Zmapowano do uczestników struktury ochrony prywatności i alokacji ról dla osób, których dane dotyczą, administratorów PII, podmiotów przetwarzających PII, stron trzecich oraz klasyfikacji ról PIMS. Addressed by clauses [4.1.4; 4.1.6; 4.3.5; 5.1.5; 5.1.7].

13.4.2 **Clause 5.12** - Zmapowano do rozliczalności zgodności w zakresie prywatności, dowodów ról, przeglądu, ustaleń z audytu oraz weryfikacji działań korygujących. Addressed by clauses [4.5.3; 6.1.2; 8.1.4; 10.1.4].

13.5 ISO/IEC 29151:2022

13.5.1 **Clause 6.1.2; Clause 6.1.3** - Zmapowano do definiowania ról ochrony PII, dokumentowania ról, komunikacji dotyczącej ról, koordynacji bezpieczeństwa/prywatności oraz rozdzielenia obowiązków w zakresie ochrony PII. Addressed by clauses [4.1.1; 4.2.1; 4.2.3; 4.2.4; 4.4.2; 5.1.4; 7.1.4].

13.6 ISO/IEC 27002:2022

13.6.1 Control 5.2 - Zmapowano do definiowania, alokowania, dokumentowania, komunikowania i utrzymywania odpowiedzialności PIMS oraz odpowiedzialności w zakresie bezpieczeństwa informacji. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.2.1; 4.4.2; 4.5.1; 5.1.4; 7.1.1].

13.6.2 Control 5.3 - Zmapowano do rozdzielenia obowiązków, zatwierdzania połączeń ról, niezależnego przeglądu, kontroli konfliktów oraz weryfikacji działań korygujących dotyczących konfliktów ról. Addressed by clauses [4.2.2; 4.2.3; 4.2.4; 9.1.2; 10.1.4].