					Wprowadź tutaj nazwę zarejestrowanej osoby prawnej							
Numer dokumentu: PII14					Tytuł dokumentu: **Polityka bezpieczeństwa PII i kontroli dostępu**							
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	Zastosowanie	Typ pokrycia	Komentarz
ISO/IEC 27701:2025	Clause 6.1.3; Clause 8.1	Both	Primary	Planowanie i działanie środków kontroli bezpieczeństwa PII
ISO/IEC 27701:2025	Clause 7.5; Clause 9.1; Clause 10.2	Both	Supporting	Dowody, monitorowanie i działania korygujące
ISO/IEC 27701:2025	Annex A.3.8; Annex A.3.9	Both	Primary	Tożsamość i prawa dostępu na potrzeby przetwarzania PII
ISO/IEC 27701:2025	Annex A.3.22; Annex A.3.23	Both	Primary	Ochrona punktów końcowych i bezpieczne uwierzytelnianie
ISO/IEC 27701:2025	Annex A.3.25; Annex A.3.26	Both	Primary	Rejestrowanie i ochrona kryptograficzna
ISO/IEC 27701:2025	Annex A.3.28; Annex A.3.29	Both	Supporting	Bezpieczeństwo aplikacji i bezpieczna architektura
ISO/IEC 27701:2025	Annex A.3.14; Annex A.3.15; Annex A.3.16	Both	Supporting	Ochrona i przegląd zapisów
GDPR	Article 5(1)(f); Article 5(2); Article 24; Article 28; Article 32	Both	Primary	Bezpieczeństwo, rozliczalność i środki kontrolne dotyczące podmiotu przetwarzającego
ISO/IEC 27001:2022	Clause 6.1.3; Clause 8.1; Annex A controls 8.1, 8.2, 8.3, 8.5, 8.8, 8.9, 8.15, 8.16, 8.20, 8.24	Both	Supporting	Integracja środków kontrolnych ISMS
ISO/IEC 27002:2022	Controls 8.1, 8.2, 8.3, 8.5, 8.8, 8.9, 8.15, 8.16, 8.20, 8.24	Both	Supporting	Wytyczne wdrażania środków kontroli bezpieczeństwa
ISO/IEC 29100:2020	Clause 5.11; Clause 5.12	Both	Supporting	Zasady bezpieczeństwa

				informacji i zgodności w zakresie prywatności
ISO/IEC 29151:2022	Clause 9.4.2; Clause 9.4.3; Clause 9.4.4; Clause 9.4.5; Clause 10.1.2; Clause 10.1.3; Clause 12.1.5; Clause 18.1.5; Clause 18.2.2; Clause 18.2.3; Clause 18.2.4	Both	Supporting	Środki kontroli bezpieczeństwa dla ochrony PII

1. Zakres

1.1 Niniejsza polityka określa wymagania bezpieczeństwa i kontroli dostępu specyficzne dla PII, dotyczące systemów, aplikacji, usług, urządzeń, środowisk chmurowych i procesów operacyjnych, które przechowują, przesyłają, przetwarzają, udostępniają PII, administrują PII lub chronią PII.

1.2 Niniejsza polityka ma zastosowanie w kontekstach administratora, współadministratora, podmiotu przetwarzającego i podwykonawcy przetwarzania, w których organizacja określa, obsługuje, wspiera środki kontroli bezpieczeństwa dla przetwarzania PII lub na nich polega.

1.3 Niniejsza polityka obejmuje następujące obszary kontroli bezpieczeństwa PII:

1.3.1 bazowy zestaw wymagań bezpieczeństwa PII i integrację z istniejącymi politykami bezpieczeństwa informacji;

1.3.2 kontrolę dostępu;

1.3.3 uwierzytelnianie;

1.3.4 dostęp uprzywilejowany;

1.3.5 szyfrowanie i bezpieczne przechowywanie;

1.3.6 rejestrowanie i monitorowanie;

1.3.7 bezpieczną konfigurację i zarządzanie podatnościami;

1.3.8 środki kontroli dostępu do punktów końcowych i chmury obliczeniowej;

1.3.9 powiązanie dowodów poprzez REG02, REG08, REG10 i REG12.

1.4 Niniejsza polityka nie zastępuje pełnego systemu zarządzania bezpieczeństwem informacji, polityki bezpieczeństwa sieci, polityki bezpiecznego rozwoju oprogramowania, polityki tworzenia kopii zapasowych, polityki punktów końcowych, polityki bezpieczeństwa chmury obliczeniowej, standardu kryptograficznego, procedury zarządzania podatnościami ani procedury reagowania na incydenty. Jeżeli takie polityki już istnieją, niniejsza polityka określa powiązania i wymagania dowodowe specyficzne dla PII, potrzebne do zapewnienia PIMS.

1.5 Niniejsza polityka nie powiela:

1.5.1 inwentarza przetwarzania PII i odpowiedzialności za podstawę prawną w PII03;

1.5.2 metodyki oceny ryzyka dla prywatności i DPIA w PII07;

1.5.3 bramek privacy by design w PII08;

1.5.4 zasad gromadzenia, wykorzystywania, ujawniania i udostępniania danych w PII09;

1.5.5 wykonywania retencji, usuwania i utylizacji w PII10;

1.5.6 nadzoru nad cyklem życia podmiotu przetwarzającego w PII12;

1.5.7 środków kontroli mechanizmów międzynarodowego transferu w PII13;

1.5.8 procesu obsługi incydentów i naruszeń w PII15;

1.5.9 zarządzania udokumentowanymi informacjami w PII17;

1.5.10 nadzoru nad monitorowaniem, audytem i doskonaleniem PIMS w PII18.

1.6 Na potrzeby niniejszej polityki logi operacyjne, dane wyjściowe narzędzi bezpieczeństwa, eksporty z przeglądów dostępu, raporty podatności i dowody konfiguracji są źródłami dowodów dołączanymi do kanonicznych obiektów dowodowych, podsumowywanymi w nich lub przywoływanymi przez nie. Nie stanowią odrębnych rejestrów PIMS.

2. Cel

2.1 Celem niniejszej polityki jest zapewnienie, aby PII były chronione przez odpowiednie, dostosowane do ryzyka i audytowalne środki bezpieczeństwa i kontroli dostępu w całym okresie przetwarzania.

2.2 Niniejsza polityka umożliwia organizacji wykazanie, że środki kontroli bezpieczeństwa PII są planowane, wdrażane, przeglądane, monitorowane i doskonalone poprzez REG02, REG08,

REG10 i REG12, bez tworzenia zduplikowanych rejestrów bezpieczeństwa ani zastępowania istniejących polityk bezpieczeństwa informacji.

3. Cele

3.1 Celami niniejszej polityki są:

3.1.1 określenie bazowych wymagań kontroli dostępu do PII dla systemów i czynności przetwarzania;

3.1.2 zapewnienie, aby środki kontroli uwierzytelniania były odpowiednie do wrażliwości PII i kontekstu dostępu;

3.1.3 określenie wymagań dotyczących przeglądu dostępu uprzywilejowanego i zwykłego do PII;

3.1.4 określenie oczekiwań dotyczących szyfrowania i bezpiecznego przechowywania PII w spoczynku, w tranzycie oraz w odpowiednich kontekstach chmurowych lub punktów końcowych;

3.1.5 określenie oczekiwań dotyczących rejestrowania i monitorowania dostępu do PII, zmian w PII oraz administrowania PII;

3.1.6 określenie wymagań dowodowych dotyczących bezpiecznej konfiguracji i podatności dla systemów przetwarzających PII;

3.1.7 określenie oczekiwań dotyczących punktów końcowych i dostępu do chmury obliczeniowej bez tworzenia pełnej polityki bezpieczeństwa punktów końcowych lub chmury obliczeniowej;

3.1.8 powiązanie podejrzewanych incydentów bezpieczeństwa PII z REG10 bez powielania procesu obsługi incydentów;

3.1.9 integracja z istniejącymi politykami bezpieczeństwa informacji, o ile są dostępne;

3.1.10 utrzymywanie dowodów gotowych do audytu wyłącznie z wykorzystaniem REG02, REG08, REG10 i REG12.

4. Postanowienia polityki

4.1 Bazowy zestaw wymagań bezpieczeństwa PII i integracja z ISMS

4.1.1 [Both] Information Security Lead MUST określić bazowy zestaw wymagań bezpieczeństwa PII dla każdego systemu lub każdej usługi przetwarzających PII w REG12, zanim system lub usługa wejdzie do środowiska produkcyjnego lub ulegnie istotnej zmianie.

4.1.2 [Both] System Owner / Application Owner MUST odnotować lokalizację dowodów wdrożonych środków kontroli bezpieczeństwa PII w REG12, zanim oprze zapewnienie PIMS na istniejącym środku kontroli bezpieczeństwa informacji.

4.1.3 [Controller] Process Owner / Business Owner MUST zidentyfikować wrażliwość PII, kontekst przetwarzania i potrzebę dostępu w REG02 przed złożeniem wniosku o nowy lub istotnie zmieniony dostęp do PII.

4.1.4 [Processor] Vendor / Procurement Owner MUST odnotować polecenia klienta dotyczące bezpieczeństwa, granice odpowiedzialności klienta i zobowiązania podmiotu przetwarzającego w zakresie bezpieczeństwa w REG08, zanim rozpocznie się dostęp podmiotu przetwarzającego do PII klienta lub zanim ulegnie on istotnej zmianie.

4.1.5 [Both] Privacy Lead / PIMS Manager MUST zweryfikować, czy dowody bezpieczeństwa PII są powiązane z REG02, REG08, REG10 lub REG12, zanim uzna czynność przetwarzania za możliwą do objęcia audytem PIMS.

4.2 Bazowe wymagania kontroli dostępu

4.2.1 [Both] System Owner / Application Owner MUST ograniczyć dostęp do PII do zatwierdzonych ról i upoważnionych użytkowników odnotowanych lub możliwych do prześledzenia w REG02 lub REG12 przed włączeniem dostępu.

4.2.2 [Both] Process Owner / Business Owner MUST zatwierdzić cel biznesowy dostępu do PII w REG02 lub REG12, zanim System Owner / Application Owner nada dostęp.

4.2.3 [Both] System Owner / Application Owner MUST przeglądać dostęp użytkowników do systemów przetwarzających PII o wysokim wpływie lub wrażliwe PII co najmniej raz na kwartał i odnotowywać wynik przeglądu w REG12.

4.2.4 [Both] System Owner / Application Owner MUST przeglądać dostęp użytkowników do innych systemów przetwarzających PII co najmniej raz w roku i odnotowywać wynik przeglądu w REG12.

4.2.5 [Both] System Owner / Application Owner MUST usunąć lub zmienić dostęp do PII w REG12 w ciągu jednego dnia roboczego po zmianie roli, zakończeniu zatrudnienia lub współpracy, zakończeniu umowy albo gdy dostęp nie jest już wymagany.

4.2.6 [Processor] Vendor / Procurement Owner MUST potwierdzić w REG08, że dostęp podmiotu przetwarzającego do PII klienta jest ograniczony do udokumentowanych poleceń klienta przed włączeniem lub zmianą dostępu.

4.2.7 [Subprocessor] Vendor / Procurement Owner MUST potwierdzić w REG08, że dostęp podwykonawcy przetwarzania do PII jest ograniczony do upoważnionych czynności dalszego przetwarzania przed włączeniem lub zmianą dostępu podwykonawcy przetwarzania.

[... 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 [Both] Information Security Lead MUST odnotować każdy wyjątek od wymagania bezpieczeństwa PII lub kontroli dostępu w REG12 przed aktywacją wyjątku.

9.1.2 [Both] Data Protection Officer / Privacy Advisor MUST doradzać w sprawie wyjątków dotyczących bezpieczeństwa PII o podwyższonym ryzyku w REG12 przed zatwierdzeniem.

9.1.3 [Both] Top Management MUST zatwierdzić wyjątki dotyczące bezpieczeństwa PII w REG12 przed aktywacją, gdy wyjątek wpływa na PII o wysokim wpływie, wrażliwe PII, dostęp uprzywilejowany, szyfrowanie, rejestrowanie lub nierozwiązane podatności wysokiego ryzyka.

9.1.4 [Both] Information Security Lead MUST określić termin wygaśnięcia wyjątku, środek kompensujący i datę przeglądu w REG12 przed zatwierdzeniem wyjątku.

9.1.5 [Both] System Owner / Application Owner MUST usunąć, odnowić lub zamknąć wygasłe wyjątki dotyczące bezpieczeństwa PII w REG12 w ciągu pięciu dni roboczych po wygaśnięciu.

9.1.6 [Processor] Vendor / Procurement Owner MUST odnotować wyjątki dotyczące bezpieczeństwa podmiotu przetwarzającego lub podwykonawcy przetwarzania wpływające na PII klienta w REG08 i REG12 przed akceptacją.

10. Egzekwowanie postanowień

10.1.1 [Both] Privacy Lead / PIMS Manager MUST odnotowywać niezgodności dotyczące brakujących lub niekompletnych dowodów bezpieczeństwa PII w REG12 w ciągu pięciu dni roboczych od identyfikacji.

10.1.2 [Both] Information Security Lead MUST przypisać odpowiedzialność za remediację nieskuteczności środków kontroli bezpieczeństwa PII w REG12 w ciągu pięciu dni roboczych od walidacji.

10.1.3 [Both] System Owner / Application Owner MUST wyłączyć lub ograniczyć nieuprawniony, nadmierny lub niepoparty dowodami dostęp do PII w ciągu jednego dnia roboczego od walidacji i odnotować działanie w REG12.

10.1.4 [Conditional] Incident Response Coordinator MUST powiązać działania egzekwujące z REG10 w ciągu jednego dnia roboczego, gdy sprawa egzekwowania dotyczy podejrzewanego lub potwierdzonego incydentu dotyczącego PII.

10.1.5 [Both] Top Management MUST przeglądać powtarzające się lub wysokiego ryzyka niezgodności dotyczące bezpieczeństwa PII w REG12 przed przeglądem zarządzania.

11. Przegląd i utrzymanie

11.1.1 [All] Privacy Lead / PIMS Manager MUST przeglądać niniejszą politykę z Information Security Lead co najmniej raz w roku i odnotowywać wynik przeglądu w REG12.

11.1.2 [Both] Information Security Lead MUST przeglądać bazowy zestaw wymagań bezpieczeństwa PII w REG12 w ciągu 30 dni po istotnej zmianie technologii, zagrożeń, audytu, incydentu lub regulacyjnej wpływającej na bezpieczeństwo PII.

11.1.3 [Both] System Owner / Application Owner MUST aktualizować dowody bezpieczeństwa PII na poziomie systemu w REG12 w ciągu 30 dni po istotnej zmianie architektury, dostępu, konfiguracji, podatności lub rejestrowania.

11.1.4 [Processor] Vendor / Procurement Owner MUST przeglądać dowody odpowiedzialności za bezpieczeństwo PII podmiotów przetwarzających i podwykonawców przetwarzania w REG08 w ciągu 30 dni po istotnej zmianie usługi, polecenia klienta lub podwykonawcy przetwarzania.

11.1.5 [All] Internal Audit / Compliance Reviewer MUST weryfikować dowody przeglądu polityki oraz wybrane dowody środków kontroli bezpieczeństwa PII w REG12 zgodnie z zatwierdzonym planem audytu.

12. Powiązane polityki

12.1 Niniejszą politykę należy czytać łącznie z:

12.2 PII01 - Polityka systemu zarządzania informacjami o prywatności;

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

12.4 PII03 - Polityka inwentarza przetwarzania PII i podstawy prawnej;

12.5 PII07 - Polityka oceny ryzyka dla prywatności i DPIA;

12.6 PII08 - Polityka privacy by design i privacy by default;

12.7 PII09 - Polityka gromadzenia, wykorzystywania, ujawniania i udostępniania PII;

12.8 PII10 - Polityka retencji, usuwania i utylizacji PII;

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

12.10 PII13 - Polityka międzynarodowego transferu PII;

12.11 PII15 - Polityka zarządzania incydentami i naruszeniami dotyczącymi PII;

12.12 PII16 - Polityka szkoleń, świadomości i kompetencji w zakresie prywatności;

12.13 PII17 - Polityka zarządzania udokumentowanymi informacjami i dowodami PIMS;

12.14 PII18 - Polityka monitorowania, audytu i doskonalenia PIMS.

13. Normy i ramy odniesienia

13.1 ISO/IEC 27701:2025 - Clause 6.1.3; Clause 8.1. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.1.4; 4.1.5; 4.7.1; 4.7.2; 4.7.3; 4.7.4; 4.7.5; 4.7.7; 4.8.1; 4.8.2; 4.8.3; 4.8.4; 4.8.5; 5.1.4; 5.1.6; 6.1.2; 7.1.1; 7.1.2].

13.2 ISO/IEC 27701:2025 - Clause 7.5; Clause 9.1; Clause 10.2. Addressed by clauses [4.1.5; 4.2.3; 4.2.4; 4.4.2; 4.4.3; 4.5.5; 4.6.3; 4.6.4; 4.7.5; 5.1.2; 6.1.1; 6.1.3; 6.1.4; 7.1.3; 7.1.6; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 9.1.1; 10.1.1; 10.1.2; 11.1.1; 11.1.5].

13.3 ISO/IEC 27701:2025 - Annex A.3.8; Annex A.3.9. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.2.6; 4.2.7; 4.3.1; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 4.4.6; 10.1.3].

13.4 ISO/IEC 27701:2025 - Annex A.3.22; Annex A.3.23. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 4.8.1; 4.8.2; 4.8.3; 4.8.4; 4.8.5].

13.5 ISO/IEC 27701:2025 - Annex A.3.25; Annex A.3.26. Addressed by clauses [4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 4.6.1; 4.6.2; 4.6.3; 4.6.4; 4.6.5; 4.6.6].

13.6 ISO/IEC 27701:2025 - Annex A.3.28; Annex A.3.29. Addressed by clauses [4.1.1; 4.1.2; 4.7.1; 4.7.2; 4.7.3; 4.7.4; 4.7.5; 4.7.6; 4.7.7; 4.8.4; 7.1.1; 7.1.2].

13.7 ISO/IEC 27701:2025 - Annex A.3.14; Annex A.3.15; Annex A.3.16. Addressed by clauses [4.1.5; 4.2.3; 4.2.4; 4.4.2; 4.4.3; 4.6.2; 4.6.3; 4.6.4; 4.7.2; 4.7.3; 5.1.9; 6.1.6; 8.1.4; 10.1.1; 11.1.5].

13.8 GDPR - Article 5(1)(f); Article 5(2); Article 24; Article 28; Article 32. Addressed by clauses [4.1.1; 4.1.4; 4.2.1; 4.2.5; 4.2.6; 4.2.7; 4.3.2; 4.4.4; 4.5.1; 4.5.2; 4.6.1; 4.6.6; 4.7.5; 4.7.6; 4.7.7; 4.8.4; 4.8.5; 5.1.1; 5.1.7; 6.1.4; 7.1.4; 9.1.3; 10.1.4].

13.9 ISO/IEC 27001:2022 - Clause 6.1.3; Clause 8.1; Annex A controls 8.1, 8.2, 8.3, 8.5, 8.8, 8.9, 8.15, 8.16, 8.20, 8.24. Addressed by clauses [4.1.1; 4.1.2; 4.2.1; 4.2.3; 4.3.2; 4.4.1; 4.4.2; 4.5.1; 4.5.2; 4.6.1; 4.6.3; 4.7.1; 4.7.4; 4.7.5; 4.8.1; 4.8.2; 7.1.1; 7.1.2].

13.10 ISO/IEC 27002:2022 - Controls 8.1, 8.2, 8.3, 8.5, 8.8, 8.9, 8.15, 8.16, 8.20, 8.24. Addressed by clauses [4.1.1; 4.1.2; 4.2.1; 4.2.3; 4.3.2; 4.4.1; 4.4.2; 4.5.1; 4.5.2; 4.6.1; 4.6.3; 4.7.1; 4.7.4; 4.7.5; 4.8.1; 4.8.2; 7.1.1; 7.1.2].

13.11 ISO/IEC 29100:2020 - Clause 5.11; Clause 5.12. Addressed by clauses [4.1.5; 4.2.1; 4.5.1; 4.6.2; 4.6.6; 4.7.6; 5.1.2; 6.1.1; 8.1.4; 10.1.1; 11.1.1].

13.12 ISO/IEC 29151:2022 - Clause 9.4.2; Clause 9.4.3; Clause 9.4.4; Clause 9.4.5; Clause 10.1.2; Clause 10.1.3; Clause 12.1.5; Clause 18.1.5; Clause 18.2.2; Clause 18.2.3; Clause 18.2.4. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.4.1; 4.4.2; 4.4.5; 4.5.1; 4.5.2; 4.5.3; 4.6.1; 4.6.2; 4.7.1; 4.7.2; 4.7.4; 4.8.1; 4.8.2; 6.1.6; 11.1.5].