					Wprowadź tutaj nazwę zarejestrowanej osoby prawnej							
Numer dokumentu: PII18					Tytuł dokumentu: **Polityka monitorowania, audytu i doskonalenia 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**

Dostosowanie do norm i regulacji

Norma / regulacja	Klauzula / środek kontrolny / artykuł	Zastosowanie	Typ pokrycia	Komentarz
ISO/IEC 27701:2025	Clause 6.2	Both	Supporting	Pomiar celów prywatności
ISO/IEC 27701:2025	Clause 7.5	Both	Primary	Udokumentowana informacja dotycząca monitorowania, audytu i doskonalenia
ISO/IEC 27701:2025	Clause 8.1	Both	Supporting	Monitorowanie planowania i nadzoru operacyjnego
ISO/IEC 27701:2025	Clause 9.1	Both	Primary	Monitorowanie, pomiary, analiza i ocena
ISO/IEC 27701:2025	Clause 9.2	Both	Primary	Audyt wewnętrzny
ISO/IEC 27701:2025	Clause 9.3	Both	Primary	Przegląd zarządzania
ISO/IEC 27701:2025	Clause 10.1	Both	Primary	Ciągłe doskonalenie
ISO/IEC 27701:2025	Clause 10.2	Both	Primary	Niezgodność i działania korygujące
ISO/IEC 27701:2025	Annex A.1.2.9	Controller	Supporting	Rejestry przetwarzania administratora wykorzystywane do audytu
ISO/IEC 27701:2025	Annex A.2.2.2	Processor	Supporting	Umowa z podmiotem przetwarzającym oraz dowody współpracy audytowej
GDPR	Article 5(2)	Controller	Supporting	Dowody rozliczalności
GDPR	Article 24	Controller	Supporting	Środki administratora i przegląd skuteczności

GDPR	Article 28	Both	Supporting	Nadzór nad audytem i współpracą podmiotu przetwarzającego
GDPR	Article 30	Both	Supporting	Rejestry przetwarzania wykorzystywane do audytu
GDPR	Article 32	Both	Supporting	Testowanie i ocenianie środków bezpieczeństwa
GDPR	Article 39	Conditional	Supporting	Monitorowanie i doradztwo audytowe DPO, gdy ma zastosowanie
ISO/IEC 29100:2020	Clause 5.12	Both	Supporting	Zgodność w zakresie prywatności, audyt i niezależny nadzór
ISO/IEC 29151:2022	Clause 18.2.2; Clause 18.2.3; Clause 18.2.4	Both	Supporting	Przegląd ochrony PII i kontrole zgodności
ISO/IEC 27001:2022	Clause 9.1	Both	Supporting	Monitorowanie i ocena bezpieczeństwa informacji
ISO/IEC 27001:2022	Clause 9.2	Both	Supporting	Wsparcie audytu wewnętrznego ISMS
ISO/IEC 27001:2022	Clause 9.3	Both	Supporting	Wsparcie przeglądu zarządzania ISMS
ISO/IEC 27001:2022	Clause 10.1	Both	Supporting	Wsparcie ciągłego doskonalenia ISMS
ISO/IEC 27001:2022	Clause 10.2	Both	Supporting	Wsparcie postępowania z niezgodnościami i działań korygujących ISMS
ISO/IEC 27002:2022	Control 5.35	Both	Supporting	Niezależny przegląd bezpieczeństwa informacji

ISO/IEC 27002:2022	Control 5.36	Both	Supporting	Przegląd zgodności polityk i norm
ISO 19011:2018	Clause 4; Clause 5; Clause 6; Clause 7	Both	Supporting	Zasady audytu systemów zarządzania, program audytu, prowadzenie audytu i kompetencje

1. Zakres

1.1 Niniejsza polityka określa wymagania organizacji dotyczące monitorowania PIMS, pomiarów, analizy, oceny, audytu wewnętrznego, przeglądu zarządzania, postępowania z niezgodnościami, działań korygujących oraz ciągłego doskonalenia.

1.2 Niniejsza polityka ma zastosowanie do:

1.2.1 wszystkich procesów PIMS, środków kontrolnych, polityk, rejestrów, obiektów dowodowych, systemów, dostawców, podmiotów przetwarzających, podwykonawców przetwarzania oraz uzgodnień dotyczących udostępniania danych w zakresie PIMS;

1.2.2 kontekstów organizacji jako administratora, współadministratora, podmiotu przetwarzającego i podwykonawcy przetwarzania;

1.2.3 skonsolidowanego monitorowania wyników PIMS, celów prywatności, statusu wdrożenia środków kontrolnych, ustaleń z audytu, niezgodności, działań korygujących, działań wynikających z przeglądu zarządzania oraz działań doskonalących;

1.2.4 dowodów przechowywanych w REG12 oraz wspierających dowodów źródłowych przechowywanych w REG01 do REG11.

1.3 Niniejsza polityka nie zastępuje wymagań dotyczących monitorowania operacyjnego określonych w innych politykach PIMS. Ustanawia ona skonsolidowany cykl oceny wyników, audytu, przeglądu i doskonalenia PIMS.

1.4 Na potrzeby niniejszej polityki duża niezgodność w PIMS oznacza niespełnienie wymagania, które istotnie wpływa na zakres PIMS, cele prywatności, rozliczalność przetwarzania PII, postępowanie z ryzykiem dla prywatności, prawa osób, których dane dotyczą, bezpieczeństwo przetwarzania, nadzór nad podmiotem przetwarzającym lub podwykonawcą przetwarzania, gotowość do reagowania na naruszenia, integralność udokumentowanych dowodów, zakres certyfikacji lub powtarzające się niespełnienie tego samego wymagania w okresie 12 miesięcy.

1.5 Na potrzeby niniejszej polityki istotna zmiana oznacza każdą zmianę wpływającą na zakres PIMS, cele przetwarzania PII, kategorie PII, kategorie osób, których dane dotyczą, lokalizacje przetwarzania, przydział roli administratora lub podmiotu przetwarzającego, architekturę systemu, uzgodnienia z dostawcami lub podwykonawcami przetwarzania, profil ryzyka dla prywatności, mające zastosowanie obowiązki prawne lub umowne, zakres audytu, metodę monitorowania lub zakres certyfikacji.

2. Cel

2.1 Celem niniejszej polityki jest zapewnienie, aby organizacja oceniała wyniki PIMS, weryfikowała zgodność PIMS, identyfikowała niezgodności, korygowała słabości środków kontrolnych oraz stale doskonaliła PIMS na podstawie obiektywnych dowodów.

2.2 Niniejsza polityka umożliwia organizacji wykazanie, że działania w zakresie monitorowania PIMS, audytu, przeglądu zarządzania i doskonalenia są planowane, niezależne tam, gdzie jest to wymagane, oparte na dowodach, terminowe oraz możliwe do powiązania z odpowiedzialnymi rolami i kanonicznymi obiektami dowodowymi.

3. Cele

3.1 Celami niniejszej polityki są:

3.1.1 zdefiniowanie skonsolidowanego procesu monitorowania i pomiaru PIMS;

3.1.2 zapewnienie, aby cele prywatności i skuteczność środków kontrolnych PIMS były mierzone z wykorzystaniem udokumentowanych dowodów;

3.1.3 ustanowienie opartego na ryzyku programu audytów wewnętrznych dla PIMS;

3.1.4 zachowanie niezależności i obiektywizmu w działaniach audytowych PIMS;

3.1.5 zapewnienie, aby przegląd zarządzania otrzymywał kompletne i aktualne dane wejściowe dotyczące wyników PIMS;

3.1.6 zapewnienie, aby niezgodności były rejestrowane, oceniane, korygowane i weryfikowane;

3.1.7 zapewnienie, aby działania korygujące były śledzone do zamknięcia i poddawane przeglądowi pod kątem skuteczności;

3.1.8 identyfikowanie powtarzających się słabości i możliwości doskonalenia;

3.1.9 wspieranie gotowości do certyfikacji i odpowiedzialnego zarządzania dowodami;

3.1.10 unikanie powielania wskaźników operacyjnych już określonych w powiązanych politykach PIMS.

4. Postanowienia polityki

4.1 Ramy monitorowania i pomiaru PIMS

4.1.1 [Both] Privacy Lead / PIMS Manager MUSI zdefiniować skonsolidowany program monitorowania PIMS w REG12 przed rozpoczęciem początkowego działania PIMS, a następnie corocznie.

4.1.2 [Both] Privacy Lead / PIMS Manager MUSI zdefiniować metodę pomiaru, częstotliwość, źródło dowodów, cel oraz odpowiedzialną rolę dla każdego wskaźnika PIMS w REG12 przed rozpoczęciem cyklu pomiarowego.

4.1.3 [Both] Process Owner / Business Owner MUSI przekazywać Privacy Lead / PIMS Manager kwartalnie dane wejściowe dotyczące monitorowania czynności przetwarzania PII z REG02.

4.1.4 [Both] Information Security Lead MUSI przekazywać Privacy Lead / PIMS Manager kwartalnie dane wejściowe dotyczące statusu środków kontrolnych bezpieczeństwa PII z REG03.

4.1.5 [Both] Vendor / Procurement Owner MUSI przekazywać Privacy Lead / PIMS Manager kwartalnie dane wejściowe dotyczące statusu podmiotów przetwarzających, podwykonawców przetwarzania, udostępniania danych stronom trzecim oraz zapewnienia dostawców z REG08.

4.1.6 [All] Incident Response Coordinator MUSI przekazywać Privacy Lead / PIMS Manager miesięcznie oraz w ciągu 10 dni roboczych po zamknięciu poważnego incydentu dane wejściowe dotyczące trendów incydentów prywatności i naruszeń z REG10.

4.1.7 [Both] Privacy Lead / PIMS Manager MUSI kwartalnie konsolidować wyniki monitorowania PIMS w REG12.

4.2 Program audytów wewnętrznych PIMS

4.2.1 [All] Internal Audit / Compliance Reviewer MUSI corocznie przygotować oparty na ryzyku program audytów wewnętrznych PIMS w REG12 przed pierwszym planowanym cyklem audytu PIMS.

4.2.2 [All] Internal Audit / Compliance Reviewer MUSI zdefiniować cel, kryteria, zakres, metodę, podstawę doboru próby oraz termin raportowania dla każdego audytu PIMS w REG12 przed rozpoczęciem czynności audytowych.

4.2.3 [All] Internal Audit / Compliance Reviewer MUSI przed każdym przydziałem audytowym odnotować w REG12 weryfikację niezależności audytora i konfliktu interesów.

4.2.4 [All] Privacy Lead / PIMS Manager MUSI udostępnić wymagane kontrolowane udokumentowane informacje PIMS oraz dowody z rejestrów za pośrednictwem REG12 w ciągu 10 dni roboczych od zatwierdzonego wniosku audytowego.

4.2.5 [Both] Internal Audit / Compliance Reviewer MUSI podczas każdego audytu PIMS testować status wdrożenia mających zastosowanie środków kontrolnych PIMS względem REG03.

4.2.6 [Both] Internal Audit / Compliance Reviewer MUSI podczas każdego audytu PIMS odnotować w REG12 wybraną próbę dowodów dotyczących przetwarzania PII.

4.2.7 [All] Internal Audit / Compliance Reviewer MUSI odnotować wyniki audytu PIMS w REG12 w ciągu 15 dni roboczych po zakończeniu audytu.

4.2.8 [All] Privacy Lead / PIMS Manager MUSI przypisać właścicieli działań korygujących dla zaakceptowanych ustaleń z audytu PIMS w REG12 w ciągu 10 dni roboczych od zaakceptowania wyników audytu.

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

9. Wyjątki

9.1 Wyjątki dotyczące monitorowania, audytu i doskonalenia

9.1.1 [All] Process Owner / Business Owner MUSI wystąpić o każdy wyjątek od niniejszej polityki w REG12 przed wystąpieniem odstępstwa.

9.1.2 [All] Privacy Lead / PIMS Manager MUSI ocenić wpływ każdego wnioskowanego wyjątku na prywatność, certyfikację, audyt i działania korygujące w REG12 w ciągu 10 dni roboczych od wniosku.

9.1.3 [All] Data Protection Officer / Privacy Advisor MUSI odnotować poradę w REG12 przed zatwierdzeniem każdego wyjątku wpływającego na obowiązki prawne, prawa osób, których dane dotyczą, zobowiązania wynikające z DPIA, obowiązki audytowe wobec klientów lub przetwarzanie wysokiego ryzyka.

9.1.4 [All] Top Management MUSI zatwierdzić wyjątki wpływające na realizację harmonogramu audytu, przegląd zarządzania, duże niezgodności w PIMS, zakres certyfikacji lub przetwarzanie wysokiego ryzyka w REG12 przed wejściem wyjątku w życie.

9.1.5 [All] Privacy Lead / PIMS Manager MUSI ustalić w REG12 datę wygaśnięcia nieprzekraczającą 90 dni dla każdego zatwierdzonego wyjątku dotyczącego monitorowania, audytu lub doskonalenia.

9.1.6 [All] Privacy Lead / PIMS Manager MUSI zamknąć lub ponownie ocenić każdy wyjątek dotyczący monitorowania, audytu lub doskonalenia w REG12 w ciągu pięciu dni roboczych od wygaśnięcia.

10. Egzekwowanie

10.1 Egzekwowanie wymagań dotyczących monitorowania, audytu i doskonalenia

10.1.1 [All] Privacy Lead / PIMS Manager MUSI odnotować pominięty cykl monitorowania, pominięty audyt PIMS, przeterminowany przegląd zarządzania, brakujące dowody audytowe, przeterminowane działanie korygujące lub przeterminowane działanie doskonalące jako niezgodność w REG12 w ciągu pięciu dni roboczych od zidentyfikowania.

10.1.2 [All] Internal Audit / Compliance Reviewer MUSI odnotować wagę ustalenia z audytu w REG12 przed wydaniem raportu z audytu.

10.1.3 [All] Top Management MUSI wymagać działania korygującego dla każdej dużej niezgodności w PIMS w REG12 w ciągu 10 dni roboczych od eskalacji.

10.1.4 [All] Process Owner / Business Owner MUSI uniemożliwić uruchomienie produkcyjne lub przedłożenie zewnętrznego zapewnienia dla przetwarzania wysokiego ryzyka, gdy wymagane dowody działań korygujących nie znajdują się w REG12 przed uruchomieniem produkcyjnym lub przedłożeniem.

10.1.5 [All] Privacy Lead / PIMS Manager MUSI eskalować powtarzające się niedotrzymanie terminów monitorowania lub działań korygujących do Top Management w REG12 w ciągu pięciu dni roboczych po drugim wystąpieniu w okresie 12 miesięcy.

10.1.6 [All] Internal Audit / Compliance Reviewer MUSI zweryfikować zamknięcie działania egzekwującego w REG12 podczas następnego zaplanowanego audytu albo w ciągu 60 dni od zgłoszonego zamknięcia, w zależności od tego, co nastąpi wcześniej.

11. Przegląd i utrzymanie

11.1 Przegląd i utrzymanie polityki

11.1.1 [All] Privacy Lead / PIMS Manager MUSI dokonywać przeglądu niniejszej polityki w REG12 corocznie oraz w ciągu 30 dni od istotnej zmiany wymagań dotyczących monitorowania PIMS, audytu, przeglądu zarządzania, działań korygujących lub certyfikacji.

11.1.2 [All] Internal Audit / Compliance Reviewer MUSI corocznie, po ostatnim zaplanowanym audycie w roku operacyjnym PIMS, dokonać przeglądu skuteczności programu audytów PIMS w REG12.

11.1.3 [All] Data Protection Officer / Privacy Advisor MUSI przed zatwierdzeniem przejrzeć w REG12 zmiany niniejszej polityki istotne z punktu widzenia prywatności.

11.1.4 [All] Top Management MUSI zatwierdzić istotne zmiany niniejszej polityki w REG12 przed publikacją.

11.1.5 [All] Privacy Lead / PIMS Manager MUSI zaktualizować REG01 i REG03 w ciągu 15 dni roboczych po zatwierdzonych zmianach niniejszej polityki, które zmieniają zakres PIMS lub stosowalność zabezpieczeń.

11.1.6 [All] Privacy Lead / PIMS Manager MUSI odnotować komunikację zatwierdzonych zmian niniejszej polityki w REG11 w ciągu 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, obowiązków 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 okresu przechowywania, 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 międzynarodowego transferu PII

12.15 PII14 - Polityka bezpieczeństwa PII i kontroli dostępu

12.16 PII15 - Polityka zarządzania incydentami PII i naruszeniami ochrony PII

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

12.18 PII17 - Polityka udokumentowanej informacji i zarządzania dowodami PIMS

13. Normy i ramy odniesienia

13.1 Niniejsza polityka jest zmapowana na następujące normy i regulacje. Mapowanie wyjaśnia, w jaki sposób polityka wspiera wskazane wymagania, oraz identyfikuje wewnętrzne klauzule, które je wdrażają lub wspierają.

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 6.2** - Zmapowano na definiowanie, mierzenie, raportowanie i przegląd celów PIMS oraz wskaźników wyników PIMS. Addressed by clauses [4.1.2; 4.3.4; 8.1.1].

13.2.2 **Clause 7.5** - Zmapowano na utrzymywanie udokumentowanej informacji dotyczącej wyników monitorowania, programów audytu, wyników audytu, dowodów przeglądu zarządzania, niezgodności, działań korygujących i działań doskonalących. Addressed by clauses [4.1.7; 4.2.4; 4.2.7; 4.3.1; 4.4.1; 7.1.8; 11.1.1].

13.2.3 **Clause 8.1** - Zmapowano na prowadzenie zaplanowanego cyklu monitorowania PIMS, audytu, działań korygujących i doskonalenia jako elementu nadzoru operacyjnego PIMS. Addressed by clauses [4.1.1; 4.2.1; 7.1.1; 7.1.6].

13.2.4 **Clause 9.1** - Zmapowano na definiowanie, co jest monitorowane i mierzone, konsolidowanie wyników monitorowania, ocenę wyników PIMS oraz utrzymywanie dowodów pomiaru. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.1.4; 4.1.5; 4.1.6; 4.1.7; 8.1.1; 8.1.2; 8.1.4; 8.1.7].

13.2.5 **Clause 9.2** - Zmapowano na utrzymywanie programu audytu wewnętrznego, planowanie audytu, weryfikacje niezależności audytora, dobór próbek dowodów, wyniki audytu oraz działania następcze dotyczące ustaleń z audytu. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.2.6; 4.2.7; 8.1.3; 10.1.2].

13.2.6 **Clause 9.3** - Zmapowano na planowanie przeglądu zarządzania, przegląd wyników PIMS, przegląd trendów audytów i działań korygujących, zatwierdzanie wyników oraz decyzje dotyczące zasobów. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 4.3.6; 6.1.7].

13.2.7 **Clause 10.1** - Zmapowano na identyfikowanie, zatwierdzanie, wdrażanie i śledzenie możliwości ciągłego doskonalenia odpowiedniości, adekwatności i skuteczności PIMS. Addressed by clauses [4.3.7; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 4.5.6; 7.1.6].

13.2.8 **Clause 10.2** - Zmapowano na rejestrowanie niezgodności, analizę przyczyny źródłowej, planowanie działań korygujących, wdrożenie działań korygujących, weryfikację skuteczności, eskalację i egzekwowanie. Addressed by clauses [4.2.8; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 4.4.6; 4.4.7; 4.4.8; 10.1.1; 10.1.3; 10.1.6].

13.2.9 **Annex A.1.2.9** - Zmapowano na rejestry przetwarzania administratora wykorzystywane jako źródła dowodów na potrzeby monitorowania, doboru próbek audytowych i wskaźników aktualności inwentaryzacji przetwarzania. Addressed by clauses [4.1.3; 4.2.6; 8.1.7].

13.2.10 **Annex A.2.2.2** - Zmapowano na umowę z podmiotem przetwarzającym, audyt klienta, odpowiedź zapewniającą oraz dowody współpracy podmiotu przetwarzającego śledzone w procesach zapewnienia dostawców i klientów. Addressed by clauses [4.1.5; 5.1.7; 7.1.5; 8.1.8].

13.3 GDPR

13.3.1 **Article 5(2)** - Zmapowano na dowody rozliczalności dotyczące monitorowania, audytu, przeglądu zarządzania, działań korygujących i ciągłego doskonalenia. Addressed by clauses [4.1.7; 4.2.7; 4.3.2; 4.4.2; 4.5.1].

13.3.2 **Article 24** - Zmapowano na środki nadzoru administratora, przegląd skuteczności, przegląd zarządzania, działania korygujące i udokumentowane dowody doskonalenia. Addressed by clauses [4.3.4; 4.3.5; 4.3.6; 4.5.2; 10.1.3].

13.3.3 **Article 28** - Zmapowano na dowody dotyczące podmiotów przetwarzających, podwykonawców przetwarzania, audytu klienta, zapewnienia stron trzecich oraz współpracy dostawców. Addressed by clauses [4.1.5; 5.1.7; 7.1.5; 8.1.8].

13.3.4 **Article 30** - Zmapowano na rejestry przetwarzania wykorzystywane jako dowody monitorowania, doboru próbek audytowych, kompletności obiektów dowodowych i aktualności inwentaryzacji przetwarzania. Addressed by clauses [4.1.3; 4.2.6; 8.1.7].

13.3.5 **Article 32** - Zmapowano na monitorowanie i ocenę statusu środków kontrolnych bezpieczeństwa PII, dowody technicznych środków kontrolnych oraz dowody skuteczności związane z bezpieczeństwem. Addressed by clauses [4.1.4; 4.2.5; 5.1.4; 7.1.4; 8.1.2].

13.3.6 **Article 39** - Zmapowano na porady w zakresie prywatności, obserwacje z monitorowania, wsparcie audytowe oraz przegląd trendów zgodności w zakresie prywatności przez Data Protection Officer / Privacy Advisor, gdy ma zastosowanie. Addressed by clauses [5.1.3; 6.1.6; 9.1.3; 11.1.3].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 5.12** - Zmapowano na weryfikację zgodności w zakresie prywatności, audyty wewnętrzne lub niezależne, kontrole wewnętrzne, mechanizmy nadzoru oraz dowody oceny ryzyka dla prywatności. Addressed by clauses [4.2.1; 4.2.3; 4.2.7; 4.5.1; 6.1.6; 8.1.7].

13.5 ISO/IEC 29151:2022

13.5.1 **Clause 18.2.2; Clause 18.2.3; Clause 18.2.4** - Zmapowano na niezależny przegląd bezpieczeństwa informacji związanego z PII, zgodność z politykami i normami oraz techniczny przegląd zgodności w zakresie ochrony PII. Addressed by clauses [4.2.3; 4.2.5; 7.1.4; 8.1.2; 10.1.6].

13.6 ISO/IEC 27001:2022

13.6.1 **Clause 9.1** - Zmapowano na dane wejściowe dotyczące monitorowania i oceny bezpieczeństwa informacji, które wspierają pomiar wyników PIMS i status środków kontrolnych bezpieczeństwa PII. Addressed by clauses [4.1.4; 8.1.2].

13.6.2 **Clause 9.2** - Zmapowano na wsparcie audytu wewnętrznego ISMS dla planowania audytu PIMS, dowodów audytowych, wyników audytu i realizacji programu audytów. Addressed by clauses [4.2.1; 4.2.2; 4.2.7; 8.1.3].

13.6.3 **Clause 9.3** - Zmapowano na dane wejściowe i wyjściowe przeglądu zarządzania na potrzeby zintegrowanego nadzoru nad wynikami PIMS i bezpieczeństwa informacji. Addressed by clauses [4.3.1; 4.3.2; 4.3.5; 4.3.6].

13.6.4 **Clause 10.1** - Zmapowano na ciągłe doskonalenie PIMS oraz wspierającego środowiska środków kontrolnych bezpieczeństwa informacji. Addressed by clauses [4.5.1; 4.5.2; 4.5.6].

13.6.5 **Clause 10.2** - Zmapowano na postępowanie z niezgodnościami, planowanie działań korygujących, wdrożenie działań korygujących i weryfikację skuteczności. Addressed by clauses [4.4.2; 4.4.4; 4.4.6; 4.4.7; 10.1.1].

13.7 ISO/IEC 27002:2022

13.7.1 Control 5.35 - Zmapowano na niezależny przegląd, weryfikacje niezależności audytora, testowanie dowodów audytowych oraz niezależną weryfikację skuteczności działań korygujących. Addressed by clauses [4.2.3; 4.2.5; 4.4.7; 10.1.6].

13.7.2 Control 5.36 - Zmapowano na przegląd zgodności polityk PIMS i bezpieczeństwa informacji, statusu wdrożenia środków kontrolnych oraz dowodów zgodności z normami. Addressed by clauses [4.1.4; 4.2.5; 4.5.3; 8.1.2].

13.8 ISO 19011:2018

13.8.1 **Clause 4; Clause 5; Clause 6; Clause 7** - Zmapowano na zasady audytu, zarządzanie programem audytu, prowadzenie audytu, raportowanie audytu oparte na dowodach, działania następcze po audycie oraz oczekiwania dotyczące kompetencji audytora dla audytów PIMS. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.6; 4.2.7; 4.4.7; 5.1.9; 11.1.2].