					Wprowadź tutaj nazwę zarejestrowanej osoby prawnej							
Numer dokumentu: PII15-FS					Tytuł dokumentu: **Polityka zarządzania incydentami i naruszeniami PII w sektorze finansowym**							
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 7.4; Clause 7.5	Both	Supporting	Komunikacja PIMS oraz udokumentowane dowody dotyczące incydentów
ISO/IEC 27701:2025	Clause 8.1; Clause 8.2; Clause 8.3	Both	Supporting	Kontrola operacyjna oraz powiązanie z oceną ryzyka dla prywatności i postępowaniem z ryzykiem
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Monitorowanie, ocena, niezgodności, działania korygujące i doskonalenie
ISO/IEC 27701:2025	Annex A.3.11	Both	Primary	Planowanie zarządzania incydentami i przygotowanie do przetwarzania PII
ISO/IEC 27701:2025	Annex A.3.12	Both	Primary	Reagowanie na incydenty bezpieczeństwa informacji obejmujące PII
ISO/IEC 27701:2025	Annex A.3.13; Annex A.3.14	Both	Supporting	Wymagania prawne, ustawowe, regulacyjne i umowne oraz ochrona zapisów
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.6	Processor	Supporting	Umowa z klientem podmiotu przetwarzającego oraz wsparcie obowiązków klienta
GDPR	Article 5(2); Article 24	Controller	Supporting	Rozliczalność i odpowiedzialność administratora
GDPR	Article 26	Joint Controller	Supporting	Koordynacja odpowiedzialności współadministratorów za incydenty

GDPR	Article 28	Both	Supporting	Wsparcie ze strony podmiotu przetwarzającego oraz obowiązki umowne podmiotu przetwarzającego
GDPR	Article 32	Both	Supporting	Bezpieczeństwo przetwarzania i zdolność wykrywania naruszeń
GDPR	Article 33	Both	Primary	Zgłaszanie naruszeń ochrony danych osobowych i dokumentowanie naruszeń
GDPR	Article 34	Controller	Primary	Zawiadamianie osób, których dane dotyczą, o naruszeniach ochrony danych osobowych
GDPR	Article 39	Conditional	Supporting	Doradztwo DPO, monitorowanie, współpraca i wsparcie punktu kontaktowego
DORA Regulation (EU) 2022/2554	Article 17	Conditional	Primary	Proces zarządzania incydentami związanymi z ICT dla objętych zakresem podmiotów finansowych
DORA Regulation (EU) 2022/2554	Article 18	Conditional	Primary	Kryteria klasyfikacji incydentów związanych z ICT oraz znaczących cyberzagrożeń
DORA Regulation (EU) 2022/2554	Article 19	Conditional	Primary	Zgłaszanie poważnych incydentów związanych z ICT oraz powiadamianie o znaczących cyberzagrożeniach
DORA Regulation (EU) 2022/2554	Article 20	Conditional	Supporting	Treść zgłoszeń, terminy, wzory i procedury

NIS2 Directive (EU) 2022/2555	Article 23	Conditional	Supporting	Zgłaszanie istotnych incydentów, gdy ma zastosowanie
ISO/IEC 29100:2020	Clause 5.11; Clause 5.12	Both	Supporting	Zasady bezpieczeństwa informacji i zgodności w obszarze prywatności
ISO/IEC 29151:2022	Clause 16.1.2; Clause 16.1.3	Both	Supporting	Odpowiedzialności w zakresie reagowania na incydenty PII i zgłaszania zdarzeń
ISO/IEC 27002:2022	Control 5.24; Control 5.25; Control 5.26; Control 5.27; Control 5.28	Both	Supporting	Planowanie incydentów, ocena, reagowanie, wyciągnięte wnioski i gromadzenie dowodów
ISO/IEC 27035-1:2023	Clause 5.2; Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6	Both	Supporting	Cykl życia procesu zarządzania incydentami
ISO/IEC 27035-2:2023	Clause 4; Clause 6; Clause 10; Clause 11; Clause 12	Both	Supporting	Polityka, plan, budowanie świadomości, testowanie i wyciągnięte wnioski dotyczące incydentów
ISO/IEC 27035-3:2020	Clause 7; Clause 8; Clause 9; Clause 10; Clause 11; Clause 12	Both	Supporting	Działania operacyjne w zakresie wykrywania, powiadamiania, triage, analizy, reagowania i raportowania
ISO/IEC 27018:2020	Annex A.10.1	Conditional	Supporting	Oczekiwania dotyczące powiadamiania i rejestrowania naruszeń przez podmiot przetwarzający w chmurze publicznej

1. Zakres

1.1 Niniejsza polityka określa wymagania dotyczące identyfikowania, zgłaszania, triage, klasyfikowania, oceniania, powstrzymywania, powiadamiania, dokumentowania, zamykania oraz doskonalenia po incydentach PII i naruszeniach ochrony PII w zakresach PIMS sektora finansowego.

1.2 **Informacja wdrożeniowa:** Niniejsza polityka jest wariantem zastępującym PII15 dla sektora finansowego. Nie wolno jej wdrażać równocześnie z PII15 dla tego samego zakresu PIMS, jednostki biznesowej, produktu, środowiska klienta, usługi regulowanej ani granicy dowodowej. Organizacje muszą wybrać PII15 albo PII15-FS dla tego samego zakresu, aby uniknąć zdublowanych obowiązków zarządzania incydentami, zdublowanych rejestrów oraz zdublowanej pracy nad dowodami audytowymi.

1.3 Niniejsza polityka ma zastosowanie do:

1.3.1 organizacji działającej jako administrator PII w kontekście sektora finansowego;

1.3.2 organizacji działającej jako współadministrator, gdy wymagana jest koordynacja odpowiedzialności za incydent lub naruszenie;

1.3.3 organizacji działającej jako podmiot przetwarzający PII dla klientów z sektora finansowego;

1.3.4 organizacji działającej jako podwykonawca przetwarzania dla klientów z sektora finansowego lub nadrzędnych podmiotów przetwarzających;

1.3.5 systemów, aplikacji, usług, procesów, dostawców, podmiotów przetwarzających, podwykonawców przetwarzania i stron trzecich, które przetwarzają, przechowują, przesyłają, wspierają, uzyskują dostęp do PII lub w inny sposób wpływają na PII w zakresie PIMS sektora finansowego.

1.4 Niniejsza polityka wykorzystuje REG10 - rejestr incydentów i naruszeń PII jako podstawowy obiekt dowodowy na potrzeby zarządzania incydentami i naruszeniami PII w sektorze finansowym.

1.5 Niniejsza polityka wykorzystuje pomocnicze obiekty dowodowe w następujący sposób:

1.5.1 REG01 dla zakresu PIMS oraz właściwego kontekstu stron zainteresowanych, sektorowego, klienta, umownego i sprawozdawczego.

1.5.2 REG02 dla objętych incydentem czynności przetwarzania, kategorii PII, kategorii osób, których dane dotyczą, celów, systemów i usług.

1.5.3 REG03 dla Deklaracji stosowania i aktualizacji stosowania środków kontrolnych, w tym zastąpienia PII15 przez PII15-FS dla tego samego zakresu.

1.5.4 REG04 dla powiązania z ryzykiem dla prywatności, DPIA, ryzykiem rezydualnym i postępowaniem z ryzykiem.

1.5.5 REG08 dla dowodów dotyczących interfejsów incydentowych podmiotów przetwarzających, podwykonawców przetwarzania, klientów, dostawców i stron trzecich.

1.5.6 REG09 dla powiązania transferów międzynarodowych, gdy incydent wpływa na przetwarzanie transgraniczne.

1.5.7 REG11 dla dowodów szkoleń, świadomości i kompetencji w zakresie reagowania na incydenty.

1.5.8 REG12 dla dowodów audytu, niezgodności, działań korygujących, przeglądu zarządzania i doskonalenia.

1.6 Niniejsza polityka opiera się na powiązanych politykach PIMS w zakresie specjalistycznych środków kontrolnych:

1.6.1 PII03 reguluje inwentarz przetwarzania i zapisy podstaw prawnych.

1.6.2 PII04 reguluje klauzulę informacyjną i środki kontroli przejrzystości poza komunikacją dotyczącą konkretnych naruszeń.

1.6.3 PII06 reguluje wnioski osób, których dane dotyczą, powstające przed incydentem, w jego trakcie lub po nim.

1.6.4 PII07 reguluje metodykę oceny ryzyka dla prywatności i DPIA.

1.6.5 PII08 reguluje środki kontroli privacy by design i privacy by default.

1.6.6 PII10 reguluje środki kontroli dotyczące retencji, usuwania i utylizacji.

1.6.7 PII12 reguluje środki kontroli relacji w zakresie prywatności z podmiotami przetwarzającymi, podwykonawcami przetwarzania, dostawcami i stronami trzecimi.

1.6.8 PII13 reguluje mechanizmy międzynarodowych transferów PII i zapisy ryzyka transferu.

1.6.9 PII14 reguluje zapobiegawcze i detekcyjne środki bezpieczeństwa PII oraz kontroli dostępu.

1.6.10 PII16 reguluje szkolenia, świadomość i kompetencje w zakresie prywatności.

1.6.11 PII17 reguluje udokumentowane informacje i zarządzanie dowodami.

1.6.12 PII18 reguluje monitorowanie, audyt wewnętrzny, przegląd zarządzania, niezgodności, działania korygujące i ciągłe doskonalenie.

1.6.13 PII23 reguluje środki kontrolne podmiotu przetwarzającego PII w chmurze, gdy obowiązki podmiotu przetwarzającego w chmurze są objęte zakresem.

1.7 Na potrzeby niniejszej polityki:

1.7.1 „Incydent PII” oznacza podejrzewane lub potwierdzone zdarzenie, które wpłynęło, mogło wpłynąć lub mogłoby racjonalnie wpłynąć na poufność, integralność, dostępność, zgodne z prawem przetwarzanie lub uprawnione postępowanie z PII.

1.7.2 „Naruszenie ochrony PII” oznacza potwierdzony incydent PII obejmujący nieuprawnione, niezgodne z prawem, przypadkowe lub niezamierzone zniszczenie, utratę, zmianę, ujawnienie, dostęp, niedostępność lub naruszenie bezpieczeństwa PII.

1.7.3 „Incydent PII w sektorze finansowym” oznacza incydent PII, który wpływa, może wpływać lub jest racjonalnie związany z regulowanymi usługami finansowymi, klientami z sektora finansowego, kontrahentami finansowymi, transakcjami finansowymi, operacjami finansowymi lub przetwarzaniem PII w sektorze finansowym.

1.7.4 „Poważny incydent w sektorze finansowym” oznacza incydent PII w sektorze finansowym lub powiązany incydent ICT, który spełnia udokumentowane kryteria istotności lub zgłaszania w REG10.

1.7.5 „Znaczące cyberzagrożenie” oznacza cyberzagrożenie zapisane w REG10, które mogłoby istotnie wpłynąć na objęte zakresem usługi sektora finansowego, przetwarzanie PII, klientów, kontrahentów lub operacje.

1.7.6 „Ocena naruszenia” oznacza udokumentowaną ocenę tego, czy incydent PII stanowi naruszenie ochrony PII, jakie PII i jakie osoby, których dane dotyczą, są objęte zdarzeniem, jakie ryzyka mogą powstać, jakie zgłoszenia lub komunikaty są wymagane oraz jakie działania naprawcze są potrzebne.

1.7.7 „Świadomość” oznacza moment, w którym organizacja ma uzasadniony stopień pewności, że wystąpił incydent bezpieczeństwa lub prywatności oraz że PII zostały lub mogły zostać naruszone.

1.7.8 „Incydent PII w sektorze finansowym o istotnym wpływie” oznacza incydent PII obejmujący przetwarzanie wysokiego ryzyka, szczególne kategorie lub wysoce wrażliwe PII, PII na dużą skalę, osoby podatne na zagrożenia, klientów regulowanych, istotne zakłócenie usługi, kontrahentów finansowych, transakcje finansowe, wpływ wielojurysdykcyjny, naruszenie

dostępu uprzywilejowanego, ekspozycję publiczną, ransomware, niedostępność usługi albo istotny wpływ operacyjny, kliencki, finansowy lub reputacyjny.

1.7.9 „Istotna zmiana dotycząca incydentu” oznacza nowe lub zmienione informacje wpływające na zakres incydentu, wagę, kategorie PII, wpływ na osoby, których dane dotyczą, wpływ na usługę, klasyfikację sektorową, decyzję o powiadomieniu, wpływ na klienta, przyczynę źródłową, powstrzymanie, odzyskiwanie, działanie korygujące lub obowiązki zewnętrznego raportowania.

2. Cel

2.1 Celem niniejszej polityki jest zapewnienie, aby incydenty PII i naruszenia ochrony PII w kontekstach sektora finansowego były obsługiwane spójnie, terminowo, zgodnie z prawem, bezpiecznie oraz z dowodami umożliwiającymi wykazanie zgodności podczas audytu.

2.2 Niniejsza polityka wspiera rozliczalność, wymagając, aby incydenty PII i naruszenia ochrony PII w sektorze finansowym były zapisywane w REG10 oraz powiązane z objętymi zdarzeniem zapisami przetwarzania, ryzykami dla prywatności, relacjami z podmiotami przetwarzającymi i podwykonawcami przetwarzania, zapisami transferów, działaniami korygującymi, zapisami szkoleń, decyzjami sprawozdawczymi dotyczącymi sektora finansowego oraz dowodami przeglądu zarządzania, gdy zostaną wyzwolone.

2.3 Niniejsza polityka zapewnia, że obowiązki administratora, współadministratora, podmiotu przetwarzającego i podwykonawcy przetwarzania są obsługiwane przez odrębne reguły stosowania, przy zachowaniu jednego zintegrowanego modelu dowodowego dla incydentów i naruszeń w sektorze finansowym.

3. Cele

3.1 Cele niniejszej polityki obejmują:

3.1.1 zapewnienie, aby podejrzewane incydenty PII w sektorze finansowym były zgłaszane i zapisywane niezwłocznie;

3.1.2 zapewnienie, aby incydenty PII w sektorze finansowym były poddawane triage i klasyfikowane według spójnych kryteriów prywatności, bezpieczeństwa, operacyjnych i sektorowych;

3.1.3 zapewnienie, aby oceny naruszeń uwzględniały objęte zdarzeniem PII, osoby, których dane dotyczą, systemy, usługi, czynności przetwarzania, podmioty przetwarzające, podwykonawców przetwarzania, transfery, ryzyka, klientów, kontrahentów i działania naprawcze;

3.1.4 zapewnienie dokumentowania decyzji administratora dotyczących zgłoszenia i komunikacji z osobami, których dane dotyczą;

3.1.5 zapewnienie, aby powiadomienia klientów lub stron nadrzędnych o naruszeniach dokonywane przez podmioty przetwarzające i podwykonawców przetwarzania były realizowane bez zbędnej zwłoki i zgodnie z właściwymi umowami;

3.1.6 zapewnienie, aby wyzwalacze raportowania w sektorze finansowym były oceniane, dokumentowane i śledzone, gdy mają zastosowanie;

3.1.7 zapewnienie zachowania i ochrony dowodów podczas obsługi incydentu;

3.1.8 zapewnienie, aby powstrzymanie, usunięcie zagrożenia, odzyskiwanie i walidacja były śledzone w REG10;

3.1.9 zapewnienie kierowania znaczących cyberzagrożeń i poważnych incydentów w sektorze finansowym do właściwych procesów decyzyjnych i sprawozdawczych;

3.1.10 zapewnienie, aby wnioski wyciągnięte z incydentów prowadziły do działań korygujących, szkoleń, doskonalenia środków kontrolnych i przeglądu zarządzania;

3.1.11 zapewnienie dostępności zapisów incydentów i naruszeń na potrzeby audytu, przeglądu zarządzania, zapewnienia dla klientów i przeglądu regulacyjnego, gdy ma to zastosowanie;

3.1.12 zapewnienie, aby PII15-FS zastępowała PII15 dla tego samego zakresu sektora finansowego i nie powodowała zdublowania prac dowodowych PII15.

4. Postanowienia polityki

4.1 Aktywacja wariantu, gotowość i przyjęcie zgłoszeń

4.1.1 [Conditional] Privacy Lead / PIMS Manager musi udokumentować aktywację PII15-FS w REG01 i REG03, zanim niniejsza polityka zostanie użyta dla zakresu PIMS sektora finansowego.

4.1.2 [Conditional] Privacy Lead / PIMS Manager musi udokumentować w REG03 i REG12, że PII15 nie jest wdrażana równocześnie dla tego samego zakresu PIMS sektora finansowego, zanim PII15-FS zostanie zatwierdzona.

4.1.3 [All] Incident Response Coordinator musi zapisać każdy zgłoszony lub wykryty podejrzewany incydent PII w sektorze finansowym w REG10 w ciągu jednego dnia roboczego od otrzymania, albo wcześniej, gdy może zostać uruchomiony właściwy termin powiadomienia, termin klienta lub termin raportowania.

4.1.4 [Conditional] Privacy Lead / PIMS Manager musi utrzymywać kryteria obsługi incydentów i naruszeń PII w sektorze finansowym w REG10 co najmniej raz w roku oraz po każdej istotnej zmianie zakresu PIMS, kontekstu prawnego, obowiązków wobec klientów, obowiązków umownych, sektorowego kontekstu raportowania lub przetwarzania wysokiego ryzyka.

4.1.5 [Both] Information Security Lead musi potwierdzić wymagania dotyczące zachowania dowodów incydentu w REG10 w ciągu 24 godzin po tym, jak podejrzewany incydent wpłynie na system, usługę lub aplikację przetwarzające PII.

4.1.6 [Conditional] Vendor / Procurement Owner musi utrzymywać wymagania dotyczące kontaktów incydentowych stron trzecich w sektorze finansowym i kierowania dowodów w REG08 przed onboardingiem oraz co najmniej raz w roku dla objętych zakresem podmiotów przetwarzających, podwykonawców przetwarzania, dostawców i zewnętrznych dostawców raportowania.

4.2 Klasyfikacja i ocena naruszenia

4.2.1 [All] Incident Response Coordinator musi sklasyfikować każdy wpis REG10 w ciągu 24 godzin od przyjęcia jako zdarzenie nieobejmujące PII, podejrzewany incydent PII, potwierdzony incydent PII, potwierdzone naruszenie ochrony PII, incydent PII w sektorze finansowym, poważny incydent w sektorze finansowym, znaczące cyberzagrożenie albo wpis oczekujący na klasyfikację.

4.2.2 [Conditional] Information Security Lead musi ocenić w REG10 objęte zdarzeniem usługi, klientów, kontrahentów, transakcje, niedostępność usług, zasięg geograficzny, utratę danych, krytyczność usługi i wpływ ekonomiczny, gdy incydent PII może wpływać na usługi lub operacje sektora finansowego.

4.2.3 [Both] Privacy Lead / PIMS Manager musi zidentyfikować objętą zdarzeniem czynność przetwarzania, kategorie PII, kategorie osób, których dane dotyczą, systemy, podmioty przetwarzające, podwykonawców przetwarzania, lokalizacje transferów i ryzyka dla prywatności w REG02, REG04, REG08, REG09 i REG10 przed sfinalizowaniem decyzji o zgłoszeniu naruszenia.

4.2.4 [Controller] Data Protection Officer / Privacy Advisor musi ocenić ryzyko dla objętych zdarzeniem osób, których dane dotyczą, dla każdego potwierdzonego lub racjonalnie podejrzewanego naruszenia ochrony PII oraz zapisać rekomendację dotyczącą zgłoszenia, uzasadnienie ryzyka i poradę w REG10 przed podjęciem decyzji o zewnętrznym zgłoszeniu.

4.2.5 [Joint Controller] Privacy Lead / PIMS Manager musi zapisać podział odpowiedzialności współadministratorów za incydent w REG08 i REG10 w ciągu 24 godzin po zidentyfikowaniu wspólnej odpowiedzialności za podejrzewane lub potwierdzone naruszenie ochrony PII.

4.2.6 [Processor] Privacy Lead / PIMS Manager musi ocenić polecenia klienta, umowne obowiązki powiadamiania i obowiązki współpracy w REG08 i REG10 w ciągu 24 godzin po tym, jak podejrzewane lub potwierdzone naruszenie ochrony PII wpłynie na przetwarzanie wykonywane jako podmiot przetwarzający.

4.2.7 [Subprocessor] Vendor / Procurement Owner musi zidentyfikować nadrzędny łańcuch powiadamiania i wymagane kierowanie dowodów w REG08 i REG10 w ciągu 24 godzin po tym, jak podejrzewany lub potwierdzony incydent PII wpłynie na przetwarzanie wykonywane jako podwykonawca 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 [All] Privacy Lead / PIMS Manager musi zapisać każdy wyjątek od niniejszej polityki w REG12 przed wdrożeniem albo w ciągu 24 godzin po działaniu awaryjnym, gdy wcześniejsze zatwierdzenie nie było możliwe.

9.1.2 [Conditional] Top Management musi zatwierdzić każdy wyjątek, który istotnie wpływa na termin zgłoszenia naruszenia, termin raportowania w sektorze finansowym, komunikację publiczną, zobowiązanie wobec klienta, zachowanie dowodów lub ryzyko dla osoby, której dane dotyczą, przed zamknięciem incydentu, a dowody zatwierdzenia muszą zostać zachowane w REG10 i REG12.

9.1.3 [Conditional] Data Protection Officer / Privacy Advisor musi udokumentować poradę dotyczącą każdego opóźnionego zgłoszenia, decyzji o braku zgłoszenia, wyjątku raportowego lub wyjątkowego podejścia komunikacyjnego przed zamknięciem incydentu, a porada musi zostać zachowana w REG10.

9.1.4 [Both] Vendor / Procurement Owner musi zapisać wyjątki dostawcy, podmiotu przetwarzającego, podwykonawcy przetwarzania, klienta lub dostawcy outsourcingowego wpływające na reagowanie na incydenty w sektorze finansowym w REG08 i REG12 w ciągu pięciu dni roboczych po zidentyfikowaniu wyjątku.

9.1.5 [All] Privacy Lead / PIMS Manager musi przeglądać otwarte wyjątki od niniejszej polityki co najmniej miesięcznie do czasu zamknięcia, a status przeglądu musi zostać zachowany w REG12.

10. Egzekwowanie postanowień

10.1.1 [All] Process Owner / Business Owner musi eskalować brak zgłoszenia podejrzewanego incydentu PII w sektorze finansowym, zachowania dowodów, wykonania przypisanych działań lub współpracy przy ocenie naruszenia do Privacy Lead / PIMS Manager w ciągu dwóch dni roboczych po wykryciu, a dowody muszą zostać zachowane w REG12.

10.1.2 [Both] Incident Response Coordinator musi eskalować opóźnione zgłoszenie, brak klasyfikacji, brakujące dowody, pominiętą eskalację lub przeterminowane działanie powstrzymujące do Privacy Lead / PIMS Manager w ciągu jednego dnia roboczego po zidentyfikowaniu problemu, a dowody muszą zostać zachowane w REG10 i REG12.

10.1.3 [Both] Privacy Lead / PIMS Manager musi zapisać niezgodność REG12, gdy naruszenie niniejszej polityki wpływa na przyjęcie incydentu, triage, powstrzymanie, powiadamianie, raportowanie, integralność dowodów, komunikację lub działanie korygujące.

10.1.4 [Both] Vendor / Procurement Owner musi zainicjować remediację dostawcy, podmiotu przetwarzającego, podwykonawcy przetwarzania lub dostawcy outsourcingowego przez

REG08 i REG12 w ciągu pięciu dni roboczych, gdy strona trzecia nie spełnia uzgodnionych obowiązków dotyczących incydentu, naruszenia, dowodów lub raportowania.

10.1.5 [Conditional] Top Management musi przejrzeć istotne lub powtarzające się niezgodności PII15-FS podczas następnego zaplanowanego przeglądu zarządzania, a decyzje i wymagane działania muszą zostać zachowane w REG12.

10.1.6 [All] Privacy Lead / PIMS Manager musi uruchomić szkolenie naprawcze w REG11 w ciągu 30 dni kalendarzowych, gdy niezgodność z polityką dotyczy świadomości roli, opóźnionego zgłoszenia, niepowodzenia eskalacji, nieprawidłowego postępowania z dowodami lub niepowodzenia komunikacji.

11. Przegląd i utrzymanie

11.1.1 [Conditional] Privacy Lead / PIMS Manager musi przeglądać niniejszą politykę co najmniej raz w roku oraz zapisywać wynik przeglądu, wymagane zmiany i status zatwierdzenia w REG12.

11.1.2 [Conditional] Incident Response Coordinator musi uruchomić poincydentalny przegląd niniejszej polityki w ciągu 30 dni kalendarzowych po zamknięciu każdego incydentu PII w sektorze finansowym o istotnym wpływie, potwierdzonego naruszenia ochrony PII, poważnego incydentu w sektorze finansowym lub znaczącego cyberzagrożenia, a dowody przeglądu muszą zostać zachowane w REG10 i REG12.

11.1.3 [Conditional] Privacy Lead / PIMS Manager musi przejrzeć niniejszą politykę w ciągu 30 dni kalendarzowych po powzięciu wiedzy o istotnej zmianie wymagań dotyczących zgłaszania incydentów wynikających z prawa, sektora, klienta, umowy, podmiotu przetwarzającego, podwykonawcy przetwarzania, wzoru raportowego, terminu raportowania lub transferu, a dowody przeglądu muszą zostać zachowane w REG01, REG08, REG09 i REG12.

11.1.4 [Both] Internal Audit / Compliance Reviewer musi przeglądać wdrożenie niniejszej polityki co najmniej raz w roku w ramach programu audytu wewnętrznego PIMS, a ustalenia audytu i działania korygujące muszą zostać zachowane w REG12.

11.1.5 [Conditional] Top Management musi przeglądać trendy incydentów, istotne naruszenia, wyniki raportowania, przeterminowane działania korygujące i skuteczność polityki podczas zaplanowanego przeglądu zarządzania, a wyniki muszą zostać zachowane w REG12.

11.1.6 [Conditional] Privacy Lead / PIMS Manager musi przeglądać relację zastąpienia między PII15-FS a PII15 co najmniej raz w roku oraz po każdej zmianie zakresu PIMS, aby zweryfikować, że obie polityki nie są wdrożone dla tego samego zakresu sektora finansowego, a dowody przeglądu muszą zostać zachowane w REG03 i REG12.

12. Powiązane polityki

12.1 Niniejszą politykę należy czytać łącznie z:

12.1.1 PII01 - Polityka systemu zarządzania informacjami o prywatności

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

12.1.3 PII03 - Polityka inwentarza przetwarzania PII i podstaw prawnych

12.1.4 PII04 - Polityka klauzul informacyjnych i przejrzystości

12.1.5 PII06 - Polityka zarządzania prawami osób, których dane dotyczą

12.1.6 PII07 - Polityka oceny ryzyka dla prywatności i DPIA

12.1.7 PII08 - Polityka privacy by design i privacy by default

12.1.8 PII10 - Polityka retencji, usuwania i utylizacji PII

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

12.1.10 PII13 - Polityka międzynarodowych transferów PII

12.1.11 PII14 - Polityka bezpieczeństwa PII i kontroli dostępu

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

12.1.13 PII17 - Polityka udokumentowanych informacji i zarządzania dowodami w PIMS

12.1.14 PII18 - Polityka monitorowania, audytu i doskonalenia PIMS

12.1.15 PII23 - Polityka podmiotu przetwarzającego PII w chmurze, gdy obowiązki podmiotu przetwarzającego w chmurze w sektorze finansowym są objęte zakresem

12.2 PII15 - Polityka zarządzania incydentami i naruszeniami PII jest bazową polityką incydentów i naruszeń. PII15-FS jest wariantem zastępującym PII15 dla sektora finansowego. PII15 i PII15-FS nie mogą być wdrażane równocześnie dla tego samego zakresu PIMS, jednostki biznesowej, produktu, środowiska klienta, usługi regulowanej ani granicy dowodowej.

13. Normy i ramy odniesienia

13.1 ISO/IEC 27701:2025 - Clause 7.4; Clause 7.5. Addressed by clauses [4.4.1; 4.4.2; 4.4.3; 4.4.8; 4.5.1; 4.5.4; 4.5.5; 5.2.2; 7.1.1; 11.1.3].

13.2 ISO/IEC 27701:2025 - Clause 8.1; Clause 8.2; Clause 8.3. Addressed by clauses [4.1.3; 4.2.3; 4.3.1; 4.3.4; 4.3.5; 4.7.3; 6.1.4; 7.1.4].

13.3 ISO/IEC 27701:2025 - Clause 9.1; Clause 10.2. Addressed by clauses [4.7.1; 4.7.2; 4.7.6; 6.1.3; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 8.1.6; 9.1.1; 10.1.1; 11.1.4; 11.1.5].

13.4 ISO/IEC 27701:2025 - Annex A.3.11. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.1.6; 5.1.1; 6.1.1; 7.1.2; 7.1.6; 7.1.7].

13.5 ISO/IEC 27701:2025 - Annex A.3.12. Addressed by clauses [4.1.3; 4.1.5; 4.2.1; 4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.6.1; 4.6.2].

13.6 ISO/IEC 27701:2025 - Annex A.3.13; Annex A.3.14. Addressed by clauses [4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 4.4.6; 4.4.7; 4.4.8; 4.4.9; 4.4.10; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 4.5.6; 4.5.7; 9.1.2; 11.1.3].

13.7 ISO/IEC 27701:2025 - Annex A.2.2.2; Annex A.2.2.6. Addressed by clauses [4.2.6; 4.2.7; 4.3.6; 4.4.4; 4.4.5; 4.4.10; 4.5.6; 5.7.1; 7.1.3; 8.1.5; 10.1.4].

13.8 GDPR - Article 5(2); Article 24. Addressed by clauses [4.1.2; 4.2.3; 4.4.1; 4.5.1; 4.7.2; 5.2.1; 6.1.1; 8.1.2; 11.1.6].

13.9 GDPR - Article 26. Addressed by clauses [4.2.5; 4.4.6; 4.5.1].

13.10 GDPR - Article 28. Addressed by clauses [4.2.6; 4.2.7; 4.4.4; 4.4.5; 4.5.6; 7.1.3; 10.1.4].

13.11 GDPR - Article 32. Addressed by clauses [4.1.5; 4.3.1; 4.3.2; 4.3.4; 4.5.2; 4.7.3; 7.1.4].

13.12 GDPR - Article 33. Addressed by clauses [4.2.3; 4.2.4; 4.4.1; 4.4.2; 4.5.4; 8.1.2].

13.13 GDPR - Article 34. Addressed by clauses [4.4.3; 4.5.4].

13.14 GDPR - Article 39. Addressed by clauses [4.2.4; 4.4.3; 5.3.1; 6.1.4; 9.1.3].

13.15 DORA Regulation (EU) 2022/2554 - Article 17. Addressed by clauses [4.1.3; 4.1.4; 4.1.5; 4.2.1; 4.3.1; 4.3.3; 4.3.4; 4.3.6; 4.4.7; 4.5.1; 4.7.1; 5.4.1; 6.1.2; 7.1.7].

13.16 DORA Regulation (EU) 2022/2554 - Article 18. Addressed by clauses [4.2.1; 4.2.2; 4.6.1; 4.6.2; 4.6.3; 8.1.3].

13.17 DORA Regulation (EU) 2022/2554 - Article 19. Addressed by clauses [4.4.7; 4.4.8; 4.4.9; 4.4.10; 4.5.5; 8.1.3].

13.18 DORA Regulation (EU) 2022/2554 - Article 20. Addressed by clauses [4.4.8; 4.5.5; 6.1.4; 7.1.2; 8.1.3; 11.1.3].

13.19 NIS2 Directive (EU) 2022/2555 - Article 23. Addressed by clauses [4.4.7; 4.4.8; 4.5.5; 6.1.4; 8.1.3; 11.1.3].

13.20 ISO/IEC 29100:2020 - Clause 5.11; Clause 5.12. Addressed by clauses [4.1.2; 4.2.3; 4.4.1; 4.4.3; 4.5.1; 4.5.3; 4.7.2; 5.2.1; 8.1.2].

13.21 ISO/IEC 29151:2022 - Clause 16.1.2; Clause 16.1.3. Addressed by clauses [4.1.3; 4.1.5; 4.2.1; 4.3.1; 4.4.1; 4.5.1; 4.5.2; 4.7.1].

13.22 ISO/IEC 27002:2022 - Control 5.24; Control 5.25; Control 5.26; Control 5.27; Control 5.28. Addressed by clauses [4.1.4; 4.1.5; 4.2.1; 4.3.1; 4.3.2; 4.3.4; 4.3.6; 4.5.2; 4.7.1; 4.7.2; 7.1.7; 10.1.2].

13.23 ISO/IEC 27035-1:2023 - Clause 5.2; Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6. Addressed by clauses [4.1.4; 4.2.1; 4.3.1; 4.4.1; 4.5.1; 4.7.1; 7.1.7].

13.24 ISO/IEC 27035-2:2023 - Clause 4; Clause 6; Clause 10; Clause 11; Clause 12. Addressed by clauses [4.1.4; 4.1.6; 4.7.1; 4.7.5; 7.1.6; 7.1.7; 10.1.6].

13.25 ISO/IEC 27035-3:2020 - Clause 7; Clause 8; Clause 9; Clause 10; Clause 11; Clause 12. Addressed by clauses [4.1.3; 4.1.5; 4.2.1; 4.3.1; 4.3.2; 4.4.7; 4.5.1; 4.7.1].

13.26 ISO/IEC 27018:2020 - Annex A.10.1. Addressed by clauses [4.2.6; 4.2.7; 4.4.4; 4.4.5; 4.5.6; 7.1.3].