					Wprowadź tutaj nazwę zarejestrowanej osoby prawnej							
Numer dokumentu: P28					Tytuł dokumentu: **Polityka rozwoju oprogramowania w outsourcingu**							
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/artykuł	Komentarz
ISO/IEC 27001:2022	Klauzula 8.1	N/D
ISO/IEC 27002:2022	Środki kontrolne 5.19-5.22, 8	N/D
NIST SP 800-53 Rev. 5	SA-4, SA-9, SA-10	N/D
RODO	Artykuły 28, 32	N/D
Dyrektywa NIS2	Artykuły 21(2)(a), (h), 23	N/D
Rozporządzenie DORA	Artykuły 28(1), (2)	N/D
COBIT 2019	APO10, BAI03, DSS	N/D

1. Cel

1.1 Niniejsza polityka określa obowiązkowe środki kontrolne dotyczące outsourcingu rozwoju oprogramowania lub systemów do zewnętrznych dostawców, wykonawców lub agencji, zapewniając stosowanie bezpiecznych praktyk w całym cyklu życia wytwarzania oprogramowania.

1.2 Jej celem jest zapobieganie podatnościom bezpieczeństwa, utracie danych, ujawnieniu własności intelektualnej (IP) oraz naruszeniom zgodności wynikającym ze współpracy z podmiotami zewnętrznymi realizującymi prace rozwojowe.

1.3 Polityka ustanawia wymagania w zakresie nadzoru nad dostawcami, standardów bezpiecznego tworzenia kodu, zarządzania dostępem, obowiązków monitorowania oraz zakończenia współpracy po wygaśnięciu umowy, w celu zapewnienia poufności, integralności i dostępności (CIA) tworzonego oprogramowania.

2. Zakres

2.1 Niniejsza polityka ma zastosowanie do wszystkich jednostek organizacyjnych angażujących podmioty zewnętrzne do rozwoju oprogramowania lub systemów, w tym do:

2.1.1 aplikacji webowych, aplikacji mobilnych, systemów wbudowanych, interfejsów API, skryptów, przepływów automatyzacji lub modułów platformowych,

2.1.2 rozwiązań tworzonych na zamówienie dla platform wewnętrznych, systemów dostępnych dla klientów lub produktów komercyjnych,

2.1.3 współpracy z programistami zewnętrznymi, freelancerami, agencjami lub zespołami offshore.

2.2 Polityka reguluje również zasady dotyczące każdego podmiotu zewnętrznego, który podczas prac rozwojowych uzyskuje dostęp do kodu źródłowego, środowisk testowych lub potoków CI/CD.

2.3 Wymagania mają zastosowanie niezależnie od rodzaju umowy, metodyki wytwarzania lub lokalizacji geograficznej dostawcy realizującego usługi outsourcingowe.

3. Cele

3.1 Zapewnienie stosowania praktyk bezpiecznego cyklu życia wytwarzania oprogramowania (SDLC) we wszystkich przedsięwzięciach realizowanych w modelu outsourcingowym, od planowania po walidację po wdrożeniu.

3.2 Zapewnienie, aby wszystkie umowy z zewnętrznymi programistami zawierały obowiązkowe klauzule dotyczące ochrony danych, bezpiecznego tworzenia kodu oraz zachowania praw własności intelektualnej.

3.3 Określenie wymagań dotyczących kontroli dostępu, monitorowania i audytu dla programistów zewnętrznych korzystających z systemów wewnętrznych.

3.4 Ochrona organizacji przed zagrożeniami w łańcuchu dostaw, naruszeniami przepisów oraz szkodą reputacyjną związanymi z oprogramowaniem tworzonym przez podmioty zewnętrzne.

3.5 Utrzymanie ciągłej zgodności z uznanymi ramami bezpieczeństwa, w tym ISO/IEC 27001, NIST, RODO, NIS2, DORA i COBIT 2019.

4. Role i odpowiedzialności

4.1 Kierownictwo wykonawcze

4.1.1 Zatwierdza projekty rozwojowe realizowane w modelu outsourcingowym o wysokim ryzyku oraz zatwierdza uzasadnione wyjątki od polityki.

4.1.2 Zapewnia, że decyzje outsourcingowe są zgodne ze strategicznymi celami organizacji oraz jej apetytem na ryzyko.

4.2 Dyrektor ds. bezpieczeństwa informacji (CISO)

4.2.1 Zatwierdza wdrożenie dostawcy z perspektywy bezpieczeństwa.

4.2.2 Określa wymagania dotyczące środków kontrolnych bezpieczeństwa dla współpracy outsourcingowej oraz dokonuje przeglądu raportów dotyczących incydentów.

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

9. Wymagania dotyczące przeglądu i aktualizacji

9.1 Niniejsza polityka musi być poddawana przeglądowi co najmniej raz w roku lub częściej w następujących okolicznościach:

9.1.1 wprowadzenie nowych modeli outsourcingu rozwoju, nowych dostawców lub nowych jurysdykcji,

9.1.2 aktualizacje ram regulacyjnych, takich jak RODO, NIS2 lub DORA,

9.1.3 po wystąpieniu incydentu bezpieczeństwa związanego z kodem, dostępem lub rezultatami prac realizowanych w modelu outsourcingowym,

9.1.4 w ramach ustaleń audytu wewnętrznego lub doskonalenia SZBI.

9.2 Dyrektor ds. bezpieczeństwa informacji (CISO) odpowiada za inicjowanie i koordynowanie przeglądu polityki w uzgodnieniu z:

9.2.1.1 działem prawnym i działem zakupów (w celu zapewnienia spójności ze stosowaniem postanowień umownych),

9.2.1.2 właścicielami projektów i produktów (w celu potwierdzenia wykonalności operacyjnej),

9.2.1.3 zespołem bezpieczeństwa informacji (w celu uwzględnienia aktualizacji dotyczących zagrożeń i środków kontrolnych),

9.2.1.4 kierownictwem wykonawczym (w celu uzyskania ostatecznej akceptacji).

9.3 Wszystkie aktualizacje polityki muszą być:

9.3.1.1 objęte kontrolą wersji i przechowywane w wyznaczonym repozytorium dokumentów,

9.3.1.2 komunikowane interesariuszom zaangażowanym w działania rozwojowe realizowane w modelu outsourcingowym,

9.3.1.3 powiązane z aktualizacjami odpowiednich polityk powiązanych lub dokumentacji proceduralnej.

9.4 Każdej wersji polityki musi towarzyszyć dziennik zmian, aby zapewnić identyfikowalność modyfikacji i zatwierdzeń.

10. Powiązane polityki i odniesienia

10.1 Niniejsza polityka wspiera i jest wspierana przez następujące dokumenty powiązane:

10.1.1 P1 - Polityka bezpieczeństwa informacji: ustanawia zasady bezpieczeństwa na poziomie organizacji, mające zastosowanie zarówno do rozwoju wewnętrznego, jak i realizowanego przez podmioty zewnętrzne.

10.1.2 P5 - Polityka zarządzania zmianami: zapewnia, że wszystkie zmiany związane z wdrożeniem kodu pochodzącego z zewnętrznych repozytoriów kodu są poddawane przeglądowi i zatwierdzane przed wdrożeniem.

10.1.3 P13 - Polityka klasyfikacji i oznaczania informacji: określa, w jaki sposób dane wrażliwe mają być identyfikowane przed ich udostępnieniem dostawcom realizującym rozwój lub repozytoriom.

10.1.4 P18 - Polityka zabezpieczeń kryptograficznych: określa zasady postępowania z kluczami, sekretami i wrażliwymi poświadczeniami podczas rozwoju i dostarczania rozwiązań.

10.1.5 P24 - Polityka bezpiecznego rozwoju oprogramowania: określa wymagania bazowe dla wewnętrznych i zewnętrznych praktyk rozwoju oprogramowania.

10.1.6 P30 - Polityka reagowania na incydenty: reguluje sposób eskalacji, badania i rozwiązywania naruszeń lub problemów bezpieczeństwa związanych z rozwojem realizowanym w modelu outsourcingowym.

10.1.7 P33 - Polityka audytu i monitorowania zgodności: określa wymagania dotyczące przeglądu działań rozwojowych realizowanych w modelu outsourcingowym podczas audytów lub przeglądów zgodności.

11. Normy i ramy odniesienia

11.1 Niniejsza polityka jest zgodna z uznanymi międzynarodowo ramami bezpieczeństwa i regulacjami w celu zapewnienia bezpiecznego outsourcingu rozwoju oprogramowania oraz właściwych praktyk zarządzania dostawcami.

11.2 ISO/IEC 27001

11.2.1 Klauzula 8.1 - Planowanie operacyjne i nadzór operacyjny: ustanawia środki kontroli procesów dla bezpiecznego rozwoju i dostarczania rozwiązań przez podmioty zewnętrzne.

11.3 ISO/IEC 27002:2022 - Środki kontrolne 5.19 do 5.21, 8.

11.3.1 Załącznik A, środek kontrolny 5.19 - Zarządzanie relacjami z dostawcami: wymaga formalnych umów zawierających klauzule dotyczące bezpieczeństwa i zgodności.

11.3.2 Załącznik A, środek kontrolny 5.20 - Uwzględnianie bezpieczeństwa informacji w umowach z dostawcami: zapewnia uwzględnienie w umowach środków kontrolnych właściwych dla rozwoju.

11.3.3 Załącznik A, środek kontrolny 5.21 - Zarządzanie świadczeniem usług przez dostawcę: obejmuje monitorowanie produktów prac i ryzyk związanych z rozwojem realizowanym przez podmioty zewnętrzne.

11.3.4 Załącznik A, środek kontrolny 8.27 - Rozwój realizowany w modelu outsourcingowym: wymaga zdefiniowanych wymagań bezpieczeństwa i kontroli dostępu do oprogramowania tworzonego przez podmioty zewnętrzne.

11.3.5 Środki te określają uporządkowane wymagania dotyczące wyboru, kontraktowania i nadzoru nad zewnętrznymi programistami, w tym praktyk bezpiecznego rozwoju, postępowania z kodem oraz walidacji jakości wykonania.

11.4 NIST SP 800-53 Rev. 5

11.4.1 SA-4 - Proces pozyskania: wymaga określenia wymagań bezpiecznego rozwoju na etapie pozyskania.

11.4.2 SA-9 - Usługi systemów zewnętrznych: reguluje bezpieczny sposób interakcji programistów zewnętrznych z usługami wewnętrznymi.

11.4.3 SA-10 - Zarządzanie konfiguracją przez dewelopera: odpowiada obowiązkom z zakresu kontroli wersji, dostępu do kodu i śledzenia zmian dla zespołów zewnętrznych.

11.5 RODO (2016/679)

11.5.1 Artykuł 28 - Obowiązki podmiotu przetwarzającego: wymaga, aby umowy z zewnętrznymi programistami określały wymagania bezpieczeństwa, kontroli i audytu dotyczące przetwarzania danych osobowych.

11.5.2 Artykuł 32 - Bezpieczeństwo przetwarzania: wymaga stosowania odpowiednich środków bezpieczeństwa (np. szyfrowania, kontroli dostępu) podczas tworzenia systemów przetwarzających dane osobowe.

11.6 Dyrektywa UE NIS2 (2022/2555)

11.6.1 Artykuły 21(2)(a), (h), 23: wymagają stosowania praktyk bezpiecznego rozwoju we współpracy z podmiotami zewnętrznymi i w cyfrowych łańcuchach dostaw, wraz z nadzorem i weryfikacją techniczną.

11.7 Rozporządzenie DORA (2022/2554)

11.7.1 Artykuły 28(1), (2): wymagają, aby podmioty finansowe zarządzały ryzykiem ICT stron trzecich poprzez środki kontrolne umowne oraz nadzór nad bezpiecznym rozwojem, w szczególności w odniesieniu do krytycznych prac rozwojowych realizowanych w modelu outsourcingowym.

11.8 COBIT 2019

11.8.1 APO10 - Zarządzanie dostawcami: ustanawia uporządkowane wymagania dotyczące oceny dostawców, umów i monitorowania jakości wykonania.

11.8.2 BAI03 - Zarządzanie budową rozwiązań: bezpośrednio odnosi się do bezpiecznych procesów SDLC, przeglądów kodu i walidacji rozwoju.

11.8.3 DSS05 - Zarządzanie usługami bezpieczeństwa: jest zgodne z monitorowaniem i ochroną systemów tworzonych zewnętrznie lub przez podmioty zewnętrzne.