					Wprowadź tutaj nazwę zarejestrowanej osoby prawnej							
Numer dokumentu: P24S					Tytuł dokumentu: **Polityka bezpiecznego rozwoju oprogramowania**							
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	Odpowiednie środki kontroli bezpieczeństwa dla praktyk operacyjnych, w tym bezpiecznego rozwoju oprogramowania
ISO/IEC 27002:2022	Środki kontrolne 8.25–8.27	Obejmuje bezpieczny cykl życia rozwoju oprogramowania, testowanie oraz obowiązki w zakresie bezpieczeństwa po stronie zewnętrznych programistów
NIST SP 800-53 Rev.5	SA-3 – SA-15, SI-10	Obejmuje bezpieczny SDLC, kontrolę dostępu oraz obsługę podatności w procesie rozwoju
RODO	Artykuł 25	Wymaga ochrony danych w fazie projektowania i domyślnej ochrony danych w procesie tworzenia oprogramowania
Dyrektywa NIS2	Artykuł 21(2)(a), (e), (h)	Nakłada obowiązek stosowania polityk bezpiecznego rozwoju oprogramowania, nadzoru nad oprogramowaniem open source oraz dokumentowania działań ograniczających ryzyko
Rozporządzenie DORA	Artykuły 6(7), 9(1)(c), 10(2)(c)	Wymaga zapewnienia bezpieczeństwa w cyklu życia systemów ICT krytycznych dla sektora finansowego
COBIT 2019	BAI	Ramy dla uporządkowanego, audytowalnego i odpornego zarządzania bezpiecznym rozwojem oprogramowania

1. Cel

1.1 Niniejsza polityka zapewnia, że całe oprogramowanie, skrypty i aplikacje internetowe tworzone lub modyfikowane przez organizację albo jej partnerów zewnętrznych są rozwijane w sposób bezpieczny, co minimalizuje ryzyko wystąpienia podatności, nieuprawnionego dostępu do danych lub zakłóceń operacyjnych.

1.2 Określa ona obowiązkowe zasady bezpiecznego rozwoju oprogramowania oraz praktyki programistyczne, których muszą przestrzegać wszyscy wewnętrzni programiści, wykonawcy i dostawcy, niezależnie od wielkości lub złożoności projektu.

1.3 Celem polityki jest ochrona danych klientów, zapobieganie incydentom bezpieczeństwa oraz zapewnienie, że oprogramowanie tworzone lub dostosowywane przez organizację lub na jej rzecz

może przejść audyty bezpieczeństwa, spełniać wymagania prawne (np. RODO, NIS2, DORA) oraz wspierać certyfikację ISO/IEC 27001.

2. Zakres

2.1 Niniejsza polityka ma zastosowanie do wszystkich osób i podmiotów zaangażowanych w rozwój, dostosowywanie, wdrażanie lub zarządzanie następującymi rozwiązaniami na rzecz organizacji:

2.1.1 stronami internetowymi, aplikacjami lub narzędziami automatyzacji,

2.1.2 skryptami lub oprogramowaniem rozwijanym wewnętrznie,

2.1.3 kodem tworzonym przez zewnętrznych programistów lub freelancerów,

2.1.4 wtyczkami, bibliotekami i komponentami oprogramowania integrowanymi z systemami produkcyjnymi.

2.2 Obejmuje ona wszystkie środowiska wykorzystywane w działaniach rozwojowych, w tym:

2.2.1 środowiska deweloperskie i testowe,

2.2.2 środowiska testowe i przedprodukcyjne,

2.2.3 systemy produkcyjne wykorzystywane do uruchamiania kodu rozwijanego na zamówienie.

2.3 Polityka reguluje również postępowanie z danymi podczas rozwoju i wdrożenia, w szczególności wszelkie wykorzystanie danych produkcyjnych w środowiskach nieprodukcyjnych.

3. Cele

3.1 Zapobieganie wprowadzaniu błędów bezpieczeństwa lub podatności do oprogramowania tworzonego na zamówienie lub rozwijanego przez strony trzecie.

3.2 Zapewnienie, że praktyki bezpiecznego tworzenia kodu oraz zapobieganie podatnościom są zintegrowane z każdym etapem cyklu życia rozwoju oprogramowania.

3.3 Ograniczenie ryzyk związanych z wykorzystaniem komponentów open source lub komponentów stron trzecich poprzez obowiązek ich właściwej weryfikacji i ewidencjonowania.

3.4 Wymaganie formalnego przeglądu kodu i testów bezpieczeństwa aplikacji przed wydaniem.

3.5 Kontrola dostępu do środowisk deweloperskich oraz zapewnienie ich odseparowania od systemów produkcyjnych.

3.6 Spełnienie obowiązkowych wymagań wynikających z norm i regulacji międzynarodowych (np. ISO/IEC 27001, RODO, DORA, NIS2).

4. Role i odpowiedzialności

4.1 Dyrektor Generalny (GM)

4.1.1 Zatwierdza niniejszą politykę i odpowiada za jej wdrożenie.

4.1.2 Zapewnia, że cały rozwój oprogramowania, zarówno wewnętrzny, jak i realizowany w outsourcingu, jest zgodny z niniejszą polityką.

4.1.3 Przegląda i podpisuje umowy rozwojowe lub umowy o świadczenie usług zawierające klauzule dotyczące bezpiecznego rozwoju oprogramowania.

4.1.4 Weryfikuje zgodność dostawców poprzez regularne przeglądy lub żądanie dowodów spełnienia wymagań bezpieczeństwa.

4.2 Wewnętrzny programista lub właściciel aplikacji

4.2.1 Stosuje praktyki bezpiecznego tworzenia kodu i bezpiecznego wdrażania.

4.2.2 Stosuje listę kontrolną bezpiecznego rozwoju oprogramowania w każdym projekcie.

4.2.3 Weryfikuje bezpieczeństwo wszystkich wykorzystywanych komponentów open source oraz komponentów stron trzecich.

4.2.4 Niezwłocznie zgłasza GM wszelkie wykryte podatności.

[... 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 przez Dyrektora Generalnego co najmniej raz w roku w celu:

9.1.1 weryfikacji dalszej zgodności z ISO/IEC 27001, RODO, NIS2 i DORA,

9.1.2 uwzględnienia zaktualizowanych zagrożeń lub zmian w dobrych praktykach bezpiecznego rozwoju oprogramowania,

9.1.3 zapewnienia zgodności z nowymi narzędziami, platformami lub relacjami z dostawcami.

9.2 Przeglądy doraźne muszą być inicjowane w przypadku:

9.2.1 każdego zgłoszonego incydentu bezpieczeństwa oprogramowania,

9.2.2 wprowadzenia nowego frameworka deweloperskiego lub platformy hostingowej,

9.2.3 zmiany partnerów realizujących rozwój po stronie trzeciej,

9.2.4 zmian regulacyjnych wpływających na obowiązki dotyczące oprogramowania lub bezpieczeństwa.

9.3 Wszystkie zmiany niniejszej polityki muszą być:

9.3.1 udokumentowane wraz z datą, podsumowaniem zmiany i zatwierdzeniem GM,

9.3.2 jasno zakomunikowane całemu personelowi wewnętrznemu i zewnętrznemu zaangażowanemu w rozwój,

9.3.3 przechowywane jako część kontroli wersji polityki i historii zmian organizacji.

9.4 Zaktualizowane wersje muszą być łatwo dostępne — za pośrednictwem platform wewnętrznych, dokumentacji papierowej lub usług chmurowych dostępnych dla dostawców.

10. Polityki powiązane i zależności

10.1 Niniejsza polityka wspiera skuteczne wdrożenie kilku innych polityk SME i jest z nimi powiązana:

10.1.1 P2S – Polityka ról i odpowiedzialności w ramach ładu zarządczego: ustanawia rozliczalność za przypisywanie i weryfikację środków kontroli bezpieczeństwa rozwoju oprogramowania w projektach i u dostawców.

10.1.2 P4S – Polityka kontroli dostępu: określa podstawowe zasady ograniczania dostępu do środowisk deweloperskich i repozytoriów kodu, w tym rozdzielenie obowiązków.

10.1.3 P8S – Polityka świadomości i szkoleń w zakresie bezpieczeństwa informacji: zapewnia, że wewnętrzni programiści i wykonawcy rozumieją praktyki bezpiecznego tworzenia kodu oraz powiązane obowiązki w zakresie bezpieczeństwa.

10.1.4 P17S – Polityka ochrony danych i prywatności: wyjaśnia, w jaki sposób należy postępować z danymi osobowymi podczas procesów rozwoju, testowania i rejestrowania, aby zachować zgodność z RODO.

10.1.5 P30S – Polityka reagowania na incydenty (P30): określa, w jaki sposób incydenty bezpieczeństwa związane z rozwojem oprogramowania muszą być zgłaszane, oceniane i obsługiwane, w tym przypadki ekspozycji związanej z kodem.

10.2 Każda z tych polityk współdziała z pozostałymi, aby bezpieczny rozwój oprogramowania był możliwy do wdrożenia i wykazania, nawet w małej organizacji lub organizacji o ograniczonych kompetencjach technicznych.

11. Normy i ramy odniesienia

11.1 ISO/IEC 27001

11.1.1 Klauzula 8.1 – wymaga wdrożenia środków kontroli operacyjnej, w tym bezpiecznego rozwoju oprogramowania, zgodnych z celami biznesowymi i profilem ryzyka.

11.2 ISO/IEC 27002

11.2.1 Środek kontrolny 8.25 – zaleca integrację bezpieczeństwa w całym cyklu życia oprogramowania, w tym w kontroli kodu źródłowego, wersjonowaniu i dostępie programistów.

11.2.2 Środek kontrolny 8.26 – określa metody testowania aplikacji i weryfikacji funkcji bezpieczeństwa przed uruchomieniem produkcyjnym.

11.2.3 Środek kontrolny 8.27 – wymaga, aby zewnętrzni programiści przestrzegali tych samych standardów rozwoju, a ich obowiązki w zakresie bezpieczeństwa były jednoznacznie określone.

11.3 NIST SP 800-53 Rev.5

11.3.1 SA-3 do SA-15 – definiują procesy bezpiecznego rozwoju oprogramowania, w tym kontrolę dostępu programistów, testowanie, modelowanie zagrożeń i dokumentację.

11.3.2 SI-10 – wymaga, aby programiści identyfikowali i ograniczali typowe słabości oprogramowania oraz stosowali narzędzia automatyczne tam, gdzie ma to zastosowanie.

11.4 RODO (2016/679)

11.4.1 Artykuł 25 – „ochrona danych w fazie projektowania i domyślna ochrona danych” nakazuje uwzględnianie zabezpieczeń bezpieczeństwa i prywatności podczas projektowania i rozwoju oprogramowania, w szczególności tam, gdzie przetwarzane są dane osobowe.

11.5 Dyrektywa UE NIS2 (2022/2555)

11.5.1 Artykuł 21(2)(a), (e) i (h) – wymaga polityk bezpiecznego rozwoju oprogramowania, nadzoru nad wykorzystaniem open source oraz udokumentowanego ograniczania ryzyk związanych z aplikacjami w podmiotach kluczowych i ważnych.

11.6 Rozporządzenie DORA (2022/2554)

11.6.1 Artykuły 6(7), 9(1)(c) i 10(2)(c) – nakładają obowiązki dotyczące bezpieczeństwa w cyklu życia rozwoju dla podmiotów sektora finansowego, w tym MŚP, w szczególności w odniesieniu do krytycznych systemów ICT.

11.7 COBIT 2019

11.7.1 BAI03 – „Manage Solutions Identification and Build” wspiera wdrożenie uporządkowanych środków kontroli rozwoju, które kładą nacisk na bezpieczeństwo, identyfikowalność i odporność, z uwzględnieniem ograniczeń właściwych dla MŚP.