					Wprowadź tutaj nazwę zarejestrowanej osoby prawnej							
Numer dokumentu: P24					Tytuł dokumentu: **Polityka bezpiecznego wytwarzania 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**

1. Cel

1.1 Niniejsza polityka określa obowiązkowe wymagania bezpieczeństwa dla działań związanych z rozwojem oprogramowania i systemów w organizacji, w tym projektów wewnętrznych, prac rozwojowych realizowanych w modelu outsourcingowym oraz integracji kodu stron trzecich.

1.2 Celem polityki jest zapewnienie, że bezpieczeństwo jest wbudowane w cały cykl życia wytwarzania oprogramowania (SDLC), a podatności są identyfikowane, ograniczane i usuwane przed wdrożeniem produkcyjnym.

1.3 Niniejsza polityka wspiera stosowanie wymagań ISO/IEC 27001:2022, klauzuli 8.1 oraz środków kontrolnych Załącznika A 8.25–8 poprzez standaryzację ładu organizacyjnego bezpiecznego wytwarzania, praktyk walidacji kodu oraz nadzoru nad pracami rozwojowymi realizowanymi przez strony trzecie.

2. Zakres

2.1 Niniejsza polityka ma zastosowanie do wszystkich:

2.1.1 Programów, aplikacji, skryptów, integracji i narzędzi automatyzacji tworzonych wewnętrznie lub zewnętrznie

2.1.2 Zespołów deweloperskich, właścicieli produktów, zespołów DevOps, zespołów QA, architektów, kierowników projektów oraz wykonawców

2.1.3 Środowisk SDLC, w tym środowisk deweloperskich, testowych i przedprodukcyjnych

2.1.4 Komponentów open source i komponentów stron trzecich integrowanych z aplikacjami wewnętrznymi

2.1.5 Oprogramowania wdrażanego w infrastrukturze lokalnej, chmurze prywatnej, środowiskach hybrydowych lub chmurze publicznej

2.2 Niniejsza polityka obowiązuje wszystkich użytkowników i wszystkie podmioty uczestniczące w rozwoju, testowaniu lub wdrażaniu systemów w organizacji, w tym dostawców usług zarządzanych (MSP) oraz dostawców platform.

3. Cele

3.1 Należy wdrożyć zabezpieczenia techniczne na wszystkich etapach rozwoju oprogramowania, od projektowania po wdrożenie, tak aby ograniczanie ryzyka miało charakter proaktywny i ciągły.

3.2 Należy zapobiegać wprowadzaniu podatności możliwych do wykorzystania, takich jak podatności typu injection, niezabezpieczone mechanizmy uwierzytelniania oraz ekspozycja na znane słabości komponentów stron trzecich.

3.3 Należy ustanowić i egzekwować praktyki bezpiecznego tworzenia kodu zgodne z OWASP, SANS CWE oraz wytycznymi właściwymi dla stosowanych frameworków.

3.4 Należy zapewnić, aby cały kod przed wdrożeniem podlegał przeglądowi wzajemnemu, analizie automatycznej oraz walidacji bezpieczeństwa.

3.5 Należy zarządzać ryzykiem rozwojowym wynikającym z outsourcingu, wykorzystania kodu stron trzecich oraz ponownego użycia oprogramowania open source.

3.6 Należy chronić środowiska deweloperskie i testowe przed nieuprawnionym dostępem oraz zapobiegać wykorzystaniu danych produkcyjnych bez zatwierdzonego maskowania danych lub anonimizacji.

3.7 Należy rozwijać świadomość bezpieczeństwa wśród programistów, menedżerów produktu i specjalistów ds. zapewnienia jakości poprzez szkolenia dedykowane dla ról oraz bieżące aktualizacje dotyczące nowych zagrożeń.

4. Role i odpowiedzialności

4.1 Dyrektor ds. bezpieczeństwa informacji (CISO)

4.1.1 Odpowiada za niniejszą politykę i zapewnia egzekwowanie wymagań bezpiecznego wytwarzania w całej organizacji.

4.1.2 Zatwierdza standardy bezpiecznego tworzenia kodu oraz umowy dotyczące prac rozwojowych realizowanych przez strony trzecie.

4.1.3 Akceptuje decyzje dotyczące postępowania z ryzykiem w odniesieniu do nierozwiązanych lub odroczonych podatności.

4.2 Kierownik ds. bezpieczeństwa aplikacji / Menedżer DevSecOps

4.2.1 Opracowuje, utrzymuje i promuje wytyczne bezpiecznego tworzenia kodu.

4.2.2 Integruje statyczne i dynamiczne testy bezpieczeństwa z potokami CI/CD.

4.2.3 Prowadzi przeglądy bezpieczeństwa kodu i określa obowiązkowe działania naprawcze.

[... 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 odpowiedzi na:

9.1.1 Istotne zmiany w metodykach rozwoju lub narzędziach DevOps

9.1.2 Istotne incydenty bezpieczeństwa wynikające z podatności aplikacyjnych

9.1.3 Zmiany wymagań regulacyjnych dotyczących bezpiecznego oprogramowania (np. RODO, DORA)

9.1.4 Nowe standardy branżowe lub informacje o zagrożeniach (np. OWASP Top 10, SLSA, MITRE CWE)

9.2 Przegląd polityki prowadzi Kierownik ds. bezpieczeństwa aplikacji we współpracy z CISO, architektami oprogramowania, kierownictwem QA oraz doradcą prawnym (w zakresie skutków związanych z kodem stron trzecich).

9.3 Wszelkie zmiany muszą zostać odnotowane w rejestrze kontroli dokumentów SZBI, objęte kontrolą wersji oraz zakomunikowane zespołom, których dotyczą, za pośrednictwem informacji o wydaniu lub obowiązkowych szkoleń.

9.4 Wersje archiwalne muszą być przechowywane w repozytorium archiwalnym na potrzeby identyfikowalności prawnej i audytowej.

10. Powiązane polityki i zależności

10.1 P1 – Polityka bezpieczeństwa informacji. Określa strategiczny mandat w zakresie wbudowania bezpieczeństwa we wszystkie systemy informatyczne organizacji, którego podstawowym zabezpieczeniem operacyjnym jest bezpieczne wytwarzanie oprogramowania.

10.2 P4 – Polityka kontroli dostępu. Określa środki kontroli służące do ograniczania dostępu do środowisk deweloperskich, repozytoriów, narzędzi budowania oraz potoków CI/CD.

10.3 P5 – Polityka zarządzania zmianą. Zapewnia, że zmiany w kodzie, wydania i wdrożenia podlegają właściwemu zatwierdzeniu, planowaniu wycofania zmian oraz weryfikacji po wdrożeniu.

10.4 P12 – Polityka zarządzania aktywami. Wspiera prowadzenie ewidencji środowisk deweloperskich, repozytoriów źródłowych i systemów budowania jako zarządzanych aktywów podlegających klasyfikacji i ochronie.

10.5 P22 – Polityka rejestrowania i monitorowania. Ma zastosowanie do potoków deweloperskich i zapewnia, że procesy budowania, promowanie kodu oraz zdarzenia wdrożeniowe są rejestrowane, monitorowane i analizowane pod kątem anomalii bezpieczeństwa.

10.6 P30 – Polityka reagowania na incydenty (P30). Zapewnia ramy analizy i reagowania na defekty bezpieczeństwa wykryte po wdrożeniu lub podczas testów bezpieczeństwa aplikacji.

11. Normy i ramy odniesienia

11.1 ISO/IEC 27001

11.1.1 Klauzula 8.1 – Planowanie operacyjne i nadzór: wymaga integracji procesów i środków kontroli bezpiecznego wytwarzania z działalnością operacyjną.

11.2 ISO/IEC 27002:2022 – Środki kontrolne 8.25–8

11.2.1 Środek kontrolny Załącznika A 8.25 – Bezpieczny cykl życia rozwoju: wymaga formalnego uwzględnienia bezpieczeństwa w projektowaniu i rozwoju oprogramowania.

11.2.2 Środek kontrolny Załącznika A 8.26 – Wymagania bezpieczeństwa aplikacji: wymaga zdefiniowania zasad bezpiecznego tworzenia kodu i kryteriów akceptacji bezpieczeństwa.

11.2.3 Środek kontrolny Załącznika A 8.27 – Zasady bezpiecznej architektury systemów i inżynierii: wymaga stosowania zasad bezpiecznego projektowania oraz ograniczania znanych słabości.

11.3 NIST SP 800-53 Rev.5

11.3.1 SA-3 do SA-15: ustanawia uporządkowane praktyki bezpiecznego rozwoju aplikacji, w tym wymagania dotyczące projektu, integralności kodu i testowania.

11.3.2 SI-10 – Walidacja danych wejściowych: dotyczy zabezpieczeń związanych z bezpiecznym tworzeniem kodu.

11.3.3 SR-3 – Ochrona łańcucha dostaw: wymaga weryfikacji oprogramowania stron trzecich, komponentów i dostawców usług rozwojowych.

11.4 RODO (2016/679)

11.4.1 Artykuł 25 – Ochrona danych w fazie projektowania i domyślna ochrona danych: nakłada obowiązek wbudowania bezpieczeństwa i prywatności w rozwój systemów.

11.4.2 Artykuł 32 – Bezpieczeństwo przetwarzania: wspiera stosowanie środków technicznych, takich jak walidacja danych wejściowych, kontrola dostępu i bezpieczne wdrożenie.

11.5 Dyrektywa NIS2 (2022/2555)

11.5.1 Artykuł 21(2)(e–f): wymaga praktyk rozwoju oprogramowania obejmujących zarządzanie podatnościami, bezpieczeństwo kodu oraz zgłaszanie incydentów.

11.6 Rozporządzenie DORA (2022/2554)

11.6.1 Artykuł 9 – Zarządzanie ryzykiem ICT: wymaga bezpiecznych praktyk rozwoju dla podmiotów finansowych, w tym kontroli jakości oprogramowania i remediacji błędów.

11.6.2 Artykuł 10 – Ciągłość działania i testowanie: promuje rygorystyczne testowanie i walidację systemów ICT, w tym aplikacji.

11.7 COBIT 2019

11.7.1 BAI03 – Zarządzanie identyfikacją i budową rozwiązań: reguluje projektowanie, rozwój i integrację bezpieczeństwa z nowymi rozwiązaniami.

11.7.2 BAI07 – Zarządzanie akceptacją zmian i przejściem: zapewnia bezpieczne wdrożenie oraz ocenę po wdrożeniu.

11.7.3 DSS05 – Zarządzanie usługami bezpieczeństwa: obejmuje walidację bezpieczeństwa oprogramowania i świadczenia usług.