					Wprowadź tutaj nazwę zarejestrowanej osoby prawnej							
Numer dokumentu: P25					Tytuł dokumentu: **Polityka wymagań bezpieczeństwa aplikacji**							
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	—
ISO/IEC 27002:2022	Środki kontrolne 8.25–8.26	—
NIST SP 800-53 Rev. 5	SA-11, SA-15, SI-10	—
RODO	Artykuły 25, 32	—
Dyrektywa NIS2	Artykuły 21(2)(f), 23	—
Rozporządzenie DORA	Artykuły 9, 11	—
COBIT 2019	BAI03, BAI09, DSS05	—

1. Cel

1.1 Niniejsza polityka określa obowiązkowe wymagania bezpieczeństwa aplikacji dla oprogramowania opracowywanego, nabywanego, integrowanego lub wdrażanego przez organizację. Zapewnia, że wszystkie aplikacje są projektowane, wdrażane i utrzymywane zgodnie z zasadami bezpiecznego wytwarzania oprogramowania, wymogami regulacyjnymi oraz apetytem na ryzyko organizacji.

1.2 Polityka wymaga uwzględnienia bezpieczeństwa w całym cyklu życia aplikacji, obejmującym uwierzytelnianie użytkowników, przetwarzanie danych, ochronę interfejsów oraz bezpieczną komunikację z interfejsami API i usługami.

1.3 Poprzez przyjęcie niniejszej polityki organizacja dąży do zapobiegania wprowadzaniu podatności do oprogramowania, ochrony danych wrażliwych oraz zapewnienia identyfikowalności i odporności na wykorzystanie podatności oraz nadużycia.

2. Zakres

2.1 Niniejsza polityka ma zastosowanie do wszystkich:

2.1.1 aplikacji rozwijanych wewnętrznie lub pozyskiwanych z zewnątrz, w tym systemów SaaS i rozwiązań tworzonych na zamówienie,

2.1.2 aplikacji wspierających systemy krytyczne biznesowo, dostęp klientów lub przetwarzanie informacji podlegających regulacjom,

2.1.3 zespołów deweloperskich, DevOps, QA, produktowych oraz zespołu bezpieczeństwa informacji,

2.1.4 zewnętrznych programistów, dostawców oprogramowania oraz partnerów integracyjnych mających dostęp do aplikacji organizacji lub interfejsów API.

2.2 Polityka obowiązuje we wszystkich środowiskach: deweloperskim, testowym, przedprodukcyjnym, produkcyjnym oraz środowisku odtwarzania po awarii, niezależnie od tego, czy są hostowane w infrastrukturze lokalnej, prywatnych centrach danych czy środowiskach chmury publicznej.

3. Cele

3.1 Określenie bazowych wymagań bezpieczeństwa funkcjonalnego i niefunkcjonalnego, które muszą być spełnione przez wszystkie aplikacje, niezależnie od metody wytwarzania lub stosu technologicznego.

3.2 Zapewnienie wdrożenia zabezpieczeń na poziomie aplikacji, w tym walidacji danych wejściowych, kodowania danych wyjściowych, obsługi błędów oraz bezpieczeństwa sesji.

3.3 Wymaganie bezpiecznego wdrożenia mechanizmów uwierzytelniania, autoryzacji i kontroli dostępu zgodnych z politykami zarządzania tożsamością i dostępem obowiązującymi w organizacji.

3.4 Wymaganie bezpiecznej komunikacji z interfejsami API, interfejsami webowymi i komponentami stron trzecich z wykorzystaniem zatwierdzonych protokołów i środków kontrolnych bezpieczeństwa.

3.5 Umożliwienie wczesnego wykrywania i ograniczania podatności poprzez analizę statyczną i dynamiczną, przegląd kodu oraz modelowanie zagrożeń.

3.6 Ochrona danych wrażliwych zgodnie z wymogami regulacyjnymi poprzez egzekwowanie szyfrowania, klasyfikacji oraz zasad retencji danych.

3.7 Zapewnienie ciągłej walidacji profilu ryzyka w obszarze bezpieczeństwa aplikacji po wdrożeniu poprzez testowanie, monitorowanie oraz możliwość wykazania zgodności podczas audytu.

4. Role i odpowiedzialności

4.1 Dyrektor ds. Bezpieczeństwa Informacji (CISO)

4.1.1 Odpowiada za niniejszą politykę i zapewnia jej zgodność ze strategią bezpieczeństwa informacji oraz profilem ryzyka organizacji.

4.1.2 Zatwierdza wymagania bezpieczeństwa aplikacji i egzekwuje obowiązkowe środki kontrolne w obszarach wytwarzania oprogramowania i zakupów.

4.2 Kierownik ds. Bezpieczeństwa Aplikacji / Menedżer DevSecOps

4.2.1 Definiuje bazowy zestaw środków kontrolnych bezpieczeństwa oraz metodyki testowania komponentów aplikacyjnych.

4.2.2 Nadzoruje bezpieczną integrację narzędzi takich jak SAST, DAST, IAST i SCA z potokiem dostarczania oprogramowania.

4.2.3 Utrzymuje listę kontrolną wymagań bezpieczeństwa aplikacji oraz kryteria walidacji.

[... 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 przeglądana co najmniej raz w roku lub częściej w odpowiedzi na:

9.1.1 ujawnienie podatności krytycznych wpływających na powszechnie stosowane frameworki lub zależności,

9.1.2 zmiany wymogów regulacyjnych dotyczących bezpieczeństwa aplikacji, np. NIS2 i DORA,

9.1.3 istotne zmiany praktyk wytwarzania oprogramowania, wykorzystywanych narzędzi lub architektury chmurowej organizacji,

9.1.4 ustalenia z audytów wewnętrznych lub zewnętrznych testów penetracyjnych.

9.2 Przegląd musi być prowadzony przez Kierownika ds. Bezpieczeństwa Aplikacji we współpracy z Dyrektorem ds. Bezpieczeństwa Informacji (CISO), liderami DevOps i Engineering, zespołami prawnym i zgodności, zakupów oraz QA.

9.3 Wszystkie zmiany muszą podlegać kontroli wersji w Rejestrze kontroli dokumentów SZBI i być komunikowane wszystkim właściwym zespołom deweloperskim i produktowym.

9.4 Zastąpione wersje muszą być archiwizowane przez okres nie krótszy niż trzy lata w celu zapewnienia identyfikowalności, ścieżki audytowej oraz wsparcia postępowań wyjaśniających dotyczących naruszeń.

10. Powiązane polityki i zależności

10.1 P1 – Polityka bezpieczeństwa informacji. Określa podstawy ochrony systemów i danych, w ramach których wymagane są środki kontrolne na poziomie aplikacji w celu zapobiegania nieuprawnionemu dostępowi, wyciekom danych i wykorzystaniu podatności.

10.2 P4 – Polityka kontroli dostępu. Określa standardy zarządzania tożsamością i sesją, które muszą być egzekwowane przez wszystkie aplikacje, w tym silne uwierzytelnianie, zasadę najmniejszych uprawnień oraz wymagania dotyczące przeglądów dostępu.

10.3 P5 – Polityka zarządzania zmianami. Reguluje promowanie kodu aplikacyjnego i konfiguracji do środowisk produkcyjnych, zapewniając blokowanie zmian nieuprawnionych lub nieprzetestowanych.

10.4 P17 – Polityka ochrony danych i prywatności. Wymaga, aby aplikacje wdrażały privacy by design oraz zapewniały zgodne z prawem przetwarzanie danych osobowych i danych wrażliwych, ich szyfrowanie i retencję we wszystkich środowiskach.

10.5 P24 – Polityka bezpiecznego rozwoju oprogramowania. Zapewnia szersze ramy osadzania bezpieczeństwa w cyklu życia rozwoju systemów, a niniejsza polityka określa konkretne wymagania i zabezpieczenia techniczne wdrażane na poziomie aplikacji.

10.6 P30 – Polityka reagowania na incydenty. Wymaga uporządkowanej obsługi incydentów bezpieczeństwa aplikacji, w tym podatności zidentyfikowanych po wdrożeniu lub podczas testów penetracyjnych, oraz określa procedury eskalacji, ograniczania skutków i odtwarzania.

11. Normy i ramy odniesienia

11.1 ISO/IEC 27001:2022

11.1.1 Klauzula 8.1 – Planowanie operacyjne i nadzór: wymaga uwzględnienia bezpieczeństwa aplikacji w procesach i systemach w celu zapewnienia poufności, integralności i dostępności (CIA).

11.2 ISO/IEC 27002:2022

11.2.1 Środki kontrolne 8.25–8.26: określają oczekiwania dotyczące bezpieczeństwa aplikacji, w tym praktyki bezpiecznego tworzenia kodu, modelowanie zagrożeń, zabezpieczenia architektoniczne oraz walidację oprogramowania stron trzecich.

11.2.2 Załącznik A, środek kontrolny 8.25 – Cykl życia bezpiecznego rozwoju oprogramowania: wymaga integracji bezpieczeństwa w całym cyklu życia aplikacji.

11.2.3 Załącznik A, środek kontrolny 8.26 – Wymagania bezpieczeństwa aplikacji: wymaga definiowania i egzekwowania zabezpieczeń technicznych chroniących aplikacje przed niewłaściwym użyciem i naruszeniem bezpieczeństwa.

11.3 NIST SP 800-53 Rev. 5

11.3.1 SA-11 – Testowanie bezpieczeństwa i ocena przez deweloperów: wymaga testów statycznych, dynamicznych i penetracyjnych podczas wytwarzania oprogramowania.

11.3.2 SA-15 – Proces rozwoju, standardy i narzędzia: ustanawia formalne standardy bezpiecznego wytwarzania aplikacji.

11.3.3 SI-10 – Walidacja danych wejściowych: wymaga mechanizmów kontrolnych zapobiegających atakom typu injection i atakom na analizę składniową.

11.4 RODO (2016/679)

11.4.1 Artykuł 25 – Ochrona danych w fazie projektowania i domyślna ochrona danych: wymaga integracji ochrony danych i prywatności z logiką aplikacji oraz przepływami pracy.

11.4.2 Artykuł 32 – Bezpieczeństwo przetwarzania: wymaga odpowiednich środków technicznych, takich jak walidacja danych wejściowych, szyfrowanie i bezpieczne mechanizmy kontroli dostępu.

11.5 Dyrektywa UE NIS2 (2022/2555)

11.5.1 Artykuł 21(2)(f): wymaga zarządzania podatnościami oraz stosowania praktyk bezpiecznego cyklu życia aplikacji przez podmioty kluczowe i ważne.

11.5.2 Artykuł 23 – Zgłaszanie incydentów bezpieczeństwa: wymaga zdolności do rejestrowania i monitorowania na poziomie aplikacji w celu wykrywania i zgłaszania istotnych incydentów.

11.6 Rozporządzenie DORA (2022/2554)

11.6.1 Artykuł 9 – zarządzanie ryzykiem ICT: nakłada na podmioty finansowe obowiązek zapewnienia, że aplikacje są bezpieczne, testowane i odporne na zagrożenia cybernetyczne.

11.6.2 Artykuł 11 – Testowanie narzędzi ICT: promuje okresowe testy penetracyjne i ćwiczenia red team dla aplikacji i usług krytycznych.

11.7 COBIT 2019

11.7.1 BAI03 – Zarządzanie identyfikacją i budową rozwiązań: ustanawia wymagania projektowe i kontrolne podczas rozwoju aplikacji.

11.7.2 BAI09 – Zarządzanie aplikacjami: podkreśla znaczenie bezpiecznego utrzymania, monitorowania i rozwoju systemów produkcyjnych.

11.7.3 DSS05 – Zarządzanie usługami bezpieczeństwa: łączy ochronę aplikacji z szerszymi operacjami bezpieczeństwa i środkami kontrolnymi organizacji.