					Wprowadź tutaj nazwę zarejestrowanej osoby prawnej							
Numer dokumentu: P25S					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	Zabezpieczenia operacyjne, w tym bezpieczeństwo aplikacji
ISO/IEC 27002:2022	Środki kontrolne 8.25–8.26	Bezpieczne projektowanie, rozwój, testowanie i przegląd kodu
NIST SP 800-53 Rev.5	SA-11, SI-10	Testowanie przez programistów / testowanie aplikacji, analiza kodu, zapobieganie błędom
RODO	Artykuł 25	Ochrona danych w fazie projektowania i domyślna ochrona danych
Dyrektywa NIS2	Artykuł 21(2)(a), (e)	Środki techniczne służące zabezpieczeniu aplikacji i wykrywaniu ryzyk
Rozporządzenie DORA	Artykuły 9(2)(c), 10(2)(c)	Bezpieczeństwo aplikacji na potrzeby cyfrowej odporności operacyjnej
COBIT 2019	BAI03	Zarządzanie bezpiecznym wytwarzaniem lub pozyskiwaniem oprogramowania

1. Cel

1.1 Niniejsza polityka określa minimalne obowiązkowe zabezpieczenia bezpieczeństwa aplikacji wymagane dla wszystkich rozwiązań programowych i systemowych wykorzystywanych przez organizację, niezależnie od tego, czy są one opracowywane wewnętrznie, czy pozyskiwane od dostawców zewnętrznych.

1.2 Zapewnia ona, że aplikacje są projektowane, wdrażane i utrzymywane w sposób chroniący dane klientów, pracowników i dane biznesowe przed nieuprawnionym dostępem, niewłaściwym użyciem, modyfikacją lub zniszczeniem.

1.3 Niniejsza polityka wspiera działania organizacji ukierunkowane na uzyskanie i utrzymanie certyfikacji ISO/IEC 27001, spełnienie obowiązków wynikających z RODO i NIS2 oraz ograniczenie ryzyk operacyjnych związanych z wdrażaniem niezabezpieczonego oprogramowania.

1.4 Pomaga ona ustanowić spójne i możliwe do prześledzenia w audycie podejście do bezpieczeństwa aplikacji dla SME poprzez określenie jednolitej listy kontrolnej funkcji bezpieczeństwa i praktyk, dostosowanej do środowisk o ograniczonych wewnętrznych zasobach technicznych.

2. Zakres

2.1 Niniejsza polityka ma zastosowanie do wszystkich aplikacji, systemów, narzędzi i platform, które:

2.1.1 Są tworzone wewnętrznie, dostosowywane lub skryptowane do użytku wewnętrznego

2.1.2 Są nabywane jako oprogramowanie komercyjne, systemy SaaS lub systemy chmurowe

2.1.3 Przetwarzają, przechowują lub przesyłają dane osobowe, dokumentację biznesową lub wrażliwe informacje operacyjne

2.1.4 Są używane przez pracowników, kontrahentów, klientów lub partnerów za pośrednictwem sieci wewnętrznych, Internetu lub platform mobilnych

2.2 Polityka obejmuje:

2.2.1 Programistów (wewnętrznych lub zakontraktowanych)

2.2.2 Dostawców oprogramowania i dostawców usług chmurowych

2.2.3 Personel wsparcia IT lub administratorów odpowiedzialnych za wdrożenie i wsparcie

2.2.4 Właścicieli aplikacji i użytkowników biznesowych zaangażowanych w zatwierdzanie systemów i nadzór nad nimi

3. Cele

3.1 Zapewnienie, aby wszystkie aplikacje używane przez organizację posiadały wbudowane i weryfikowalne zabezpieczenia ograniczające typowe podatności oprogramowania.

3.2 Ochrona poufności, integralności i dostępności (CIA) danych przetwarzanych przez aplikacje, niezależnie od miejsca ich hostowania.

3.3 Wymaganie formalnego testowania, przeglądu i walidacji bezpieczeństwa aplikacji przed zatwierdzeniem każdej nowej aplikacji lub istotnej aktualizacji do użytku produkcyjnego.

3.4 Umożliwienie spójnego i bezpiecznego postępowania z danymi uwierzytelniającymi użytkowników, danymi sesji i uprawnieniami dostępu we wszystkich systemach krytycznych biznesowo.

3.5 Wymaganie bezpiecznych mechanizmów rejestrowania, możliwości audytowych oraz funkcji monitorowania we wszystkich aplikacjach w celu wspierania wykrywania podejrzanej aktywności i reagowania na nią.

3.6 Ograniczenie ryzyk prawnych i ryzyk zgodności poprzez zapewnienie, że aplikacje spełniają mające zastosowanie wymagania regulacyjne w zakresie bezpieczeństwa.

4. Role i odpowiedzialności

4.1 Dyrektor Generalny (GM)

4.1.1 Ponosi ogólną odpowiedzialność za bezpieczeństwo aplikacji w całej organizacji.

4.1.2 Zatwierdza niniejszą politykę i zapewnia, że wszystkie zakupy oraz projekty rozwojowe są z nią zgodne.

4.1.3 Zapewnia, że dostawcy i usługodawcy są związani umownie wymaganiami dotyczącymi bezpieczeństwa aplikacji.

4.1.4 Dokonuje przeglądu i zatwierdza akceptację ryzyka w przypadkach, gdy pełna zgodność nie może zostać osiągnięta z uwagi na ograniczenia biznesowe.

4.2 Właściciel aplikacji (jeżeli został wyznaczony)

4.2.1 Identyfikuje specyficzne potrzeby bezpieczeństwa aplikacji na etapie wyboru systemu lub rozpoczęcia projektu.

4.2.2 Weryfikuje, że uwzględniono kluczowe funkcje, takie jak ochrona logowania, szyfrowanie i rejestrowanie aktywności.

4.2.3 Uczestniczy w przeglądach przedwdrożeniowych i potwierdza, że zabezpieczenia odpowiadają potrzebom biznesowym.

[... 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 kalendarzowym w celu:

9.1.1 Odzwierciedlenia zmian w wymaganiach regulacyjnych (np. RODO, NIS2, DORA)

9.1.2 Uwzględnienia nowych lub pojawiających się zagrożeń i technik ataków

9.1.3 Aktualizacji treści i wymagań w związku ze zmianami platform, dostawców lub metod wytwarzania

9.2 Przeglądy doraźne muszą być również przeprowadzane, gdy:

9.2.1 Wprowadzane są nowe aplikacje

9.2.2 Istniejące aplikacje przechodzą istotne aktualizacje lub integracje

9.2.3 Wystąpi incydent lub naruszenie związane z aplikacją

9.2.4 Zidentyfikowane zostaną nowe ryzyka na podstawie zewnętrznych komunikatów lub alertów branżowych

9.3 Wszystkie aktualizacje niniejszej polityki muszą być:

9.3.1 Zatwierdzone przez Dyrektora Generalnego

9.3.2 Udokumentowane wraz z historią wersji i przyczyną zmiany

9.3.3 Zakomunikowane wszystkim pracownikom, programistom i dostawcom zaangażowanym w zarządzanie aplikacjami

9.3.4 Bezpiecznie przechowywane na potrzeby audytu i wykazania zgodności

10. Powiązane polityki i zależności

10.1 Niniejsza polityka jest bezpośrednio wspierana przez poniższe polityki bezpieczeństwa dostosowane do SME oraz przyczynia się do ich stosowania:

10.1.1 P2S – Polityka ról i odpowiedzialności w ramach ładu zarządczego: określa odpowiedzialność za zatwierdzanie aplikacji, stosowanie polityki i zarządzanie dostawcami.

10.1.2 P4S – Polityka kontroli dostępu: zapewnia, że dostęp do aplikacji jest zgodny z zasadą najmniejszych uprawnień i zasadami kontroli sesji.

10.1.3 P8S – Polityka świadomości i szkoleń w zakresie bezpieczeństwa informacji: zapewnia, że użytkownicy i programiści są szkoleni w zakresie rozpoznawania i zgłaszania zagrożeń związanych z aplikacjami.

10.1.4 P17S – Polityka ochrony danych i prywatności: określa zabezpieczenia prywatności danych, które muszą być stosowane przez każdą aplikację przetwarzającą dane osobowe.

10.1.5 P14S – Polityka retencji i utylizacji danych: reguluje sposób przechowywania, archiwizacji i bezpiecznego niszczenia logów, kopii zapasowych i danych wrażliwych generowanych przez aplikacje.

10.1.6 P30S – Polityka reagowania na incydenty: określa kroki identyfikowania, zgłaszania i powstrzymywania zdarzeń bezpieczeństwa informacji związanych z aplikacjami.

10.2 Łącznie polityki te zapewniają pełną integrację bezpieczeństwa aplikacji z Systemem Zarządzania Bezpieczeństwem Informacji (SZBI) organizacji oraz możliwość wykazania zgodności podczas audytu.

11. Normy referencyjne i ramy odniesienia

11.1 ISO/IEC 27001

11.1.1 Klauzula 8.1 – wymaga, aby organizacje ustanowiły zabezpieczenia operacyjne służące postępowaniu z ryzykami bezpieczeństwa informacji, w tym ryzykami związanymi z aplikacjami i systemami programowymi.

11.2 ISO/IEC 27002

11.2.1 Środek kontrolny 8.25 – zaleca wdrożenie praktyk bezpiecznego projektowania, rozwoju i przeglądu kodu we wszystkich aplikacjach, w tym dostarczanych przez dostawców.

11.2.2 Środek kontrolny 8.26 – zaleca formalne testowanie zabezpieczeń aplikacji, w szczególności w obszarach obejmujących kontrolę dostępu, walidację danych wejściowych i obsługę sesji.

11.3 NIST SP 800-53 Rev.5

11.3.1 SA-11 – określa wymagania dotyczące testowania przez programistów, analizy kodu i dynamicznego skanowania aplikacji przed wdrożeniem.

11.3.2 SI-10 – dotyczy wykrywania i zapobiegania typowym błędom oprogramowania, ze szczególnym uwzględnieniem świadomości programistów i zabezpieczeń technicznych.

11.4 RODO (2016/679)

11.4.1 Artykuł 25 – „ochrona danych w fazie projektowania i domyślna ochrona danych" wymaga wbudowania prywatności i bezpieczeństwa w podstawowe założenia projektowe aplikacji przetwarzających dane osobowe.

11.5 Dyrektywa UE NIS2 (2022/2555)

11.5.1 Artykuł 21(2)(a) i (e) – wymaga od podmiotów kluczowych i ważnych wdrożenia środków technicznych w celu zabezpieczenia aplikacji i wykrywania ryzyk związanych z oprogramowaniem.

11.6 Rozporządzenie DORA (2022/2554)

11.6.1 Artykuł 9(2)(c), 10(2)(c) – wymaga od SME z sektora finansowego wdrożenia zabezpieczeń na poziomie aplikacji oraz prowadzenia regularnych ocen w celu utrzymania cyfrowej odporności operacyjnej.

11.7 COBIT 2019

11.7.1 BAI03 – „Manage Solutions Identification and Build" wskazuje sposób rozwoju lub pozyskiwania bezpiecznego oprogramowania zgodnego z ryzykiem, wymaganiami zgodności i potrzebami biznesowymi, nawet w środowiskach SME o ograniczonych zasobach.