					Wprowadź tutaj nazwę zarejestrowanej osoby prawnej							
Numer dokumentu: P19S					Tytuł dokumentu: **Polityka zarządzania podatnościami i wdrażania poprawek**							
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 8.8, 8.9	
NIST SP 800-53 Rev.5	RA-5, SI-2, CM-2	
Dyrektywa NIS2	Artykuły 21(2)(d), 21(2)(e)	
Rozporządzenie DORA	Artykuły 8(1), 10(2)	
COBIT 2019	DSS05.02, APO12	
RODO	Artykuł 32(1)(b)	

1. Cel

1.1 Niniejsza polityka określa sposób identyfikowania, oceny i ograniczania podatności w systemach, aplikacjach i infrastrukturze organizacji.

1.2 Jej celem jest ograniczenie ryzyka cyberbezpieczeństwa poprzez terminowe wdrażanie poprawek oraz stosowanie opartych na ryzyku działań naprawczych, odpowiednich dla małych i średnich przedsiębiorstw (MŚP).

1.3 Niniejsza polityka wspiera zgodność z wymaganiami certyfikacyjnymi ISO/IEC 27001:2022 oraz pomaga spełniać obowiązki regulacyjne wynikające z RODO, NIS2 i DORA poprzez wymaganie proaktywnego zarządzania podatnościami technicznymi.

1.4 Organizacja uznaje, że systemy bez wdrożonych poprawek stanowią istotne zagrożenie dla bezpieczeństwa informacji i muszą być traktowane systematycznie i bez zbędnej zwłoki.

2. Zakres

2.1 Niniejsza polityka ma zastosowanie do:

2.1.1 wszystkich serwerów, stacji roboczych, laptopów, urządzeń mobilnych, urządzeń sieciowych i platform hostowanych w chmurze wykorzystywanych przez organizację,

2.1.2 wszystkich systemów operacyjnych, oprogramowania firm trzecich, wtyczek i aplikacji wykorzystywanych w działalności biznesowej,

2.1.3 wewnętrznego personelu IT lub dostawców usług zewnętrznych odpowiedzialnych za utrzymanie systemów, aktualizacje lub monitorowanie,

2.1.4 wszelkiego oprogramowania wytwarzanego na zamówienie lub oprogramowania wbudowanego utrzymywanego przez organizację lub w jej imieniu.

2.2 Polityka obejmuje zarówno infrastrukturę zarządzaną bezpośrednio przez organizację, jak i systemy administrowane przez zakontraktowanych dostawców lub dostawców hostingu.

3. Cele

3.1 Terminowa i spójna identyfikacja oraz ocena znanych podatności we wszystkich aktywach IT

3.2 Wdrażanie poprawek i aktualizacji oprogramowania na podstawie ich krytyczności oraz ryzyka dla działalności organizacji lub danych osobowych

3.3 Zapobieganie wykorzystaniu słabości technicznych, które mogłyby prowadzić do zakłócenia świadczenia usług, naruszenia bezpieczeństwa danych lub niezgodności z wymaganiami prawnymi

3.4 Utrzymywanie dokładnej dokumentacji dotyczącej wdrożonych poprawek, nierozwiązanych problemów oraz odstępstw w celu zapewnienia gotowości audytowej

3.5 Stosowanie narzędzi i procesów odpowiednich do wielkości organizacji i złożoności operacyjnej bez obniżania skuteczności

3.6 Wspieranie zgodności z wymaganiami prawnymi i regulacyjnymi, w tym z art. 32 RODO oraz środkiem kontrolnym 8 załącznika A normy ISO

4. Role i odpowiedzialności

4.1 Dyrektor Generalny (GM)

4.1.1 Ponosi ogólną odpowiedzialność za zapewnienie realizacji działań związanych z zarządzaniem podatnościami i wdrażaniem poprawek

4.1.2 Zatwierdza odstępstwa od wymagań w przypadkach, gdy poprawki nie mogą zostać wdrożone, oraz dokonuje przeglądu powiązanych strategii ograniczania ryzyka

4.1.3 Dokonuje przeglądu raportów statusowych dotyczących wdrażania poprawek oraz zapewnia dostępność zasobów niezbędnych do realizacji obowiązków w tym zakresie

4.2 Dostawca wsparcia IT / wewnętrzny administrator IT

4.2.1 Monitoruje systemy pod kątem podatności i dostępnych poprawek z wykorzystaniem alertów dostawców, komunikatów o zagrożeniach i powiadomień systemowych

4.2.2 Wdraża aktualizacje systemów operacyjnych, oprogramowania układowego i aplikacji w określonych terminach

4.2.3 Prowadzi formalny rejestr poprawek i dokumentuje nierozwiązane lub odroczone aktualizacje

4.2.4 Przeprowadza testy i planuje wdrożenie aktualizacji krytycznych w sposób minimalizujący zakłócenia operacyjne

[... 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 Coroczny przegląd

9.1.1 Niniejsza polityka musi być poddawana przeglądowi co najmniej raz w roku przez Dyrektora Generalnego, z udziałem Dostawcy wsparcia IT oraz Koordynatora ds. prywatności

9.2 Przesłanki przeglądu

9.2.1 Przeglądy doraźne muszą być przeprowadzane, jeżeli:

9.2.1.1 istotna podatność lub exploit wpływa na systemy objęte zakresem,

9.2.1.2 występują istotne zmiany systemowe lub programowe,

9.2.1.3 audyt identyfikuje luki w procesach wdrażania poprawek,

9.2.1.4 zostanie odnotowany incydent lub naruszenie związane z wdrażaniem poprawek.

9.3 Kontrola wersji polityki

9.3.1 Wszystkie aktualizacje muszą być rejestrowane w rejestrze wersji wraz z podsumowaniem zmian

9.3.2 Zmiany muszą być komunikowane personelowi, którego dotyczą

9.3.3 Nieaktualne wersje muszą być archiwizowane z ograniczonym dostępem

10. Powiązane polityki i zależności

10.1 Niniejsza polityka wspiera kilka innych polityk SME i jest z nimi powiązana:

10.1.1 P12S – Polityka zarządzania aktywami: określa właścicieli systemów i klasyfikację, zapewniając ujęcie i zinwentaryzowanie wszystkich aktywów wymagających wdrażania poprawek

10.1.2 P14S – Polityka retencji danych i utylizacji: zapewnia, że systemy przeznaczone do wycofania z eksploatacji są bezpiecznie aktualizowane lub wymazywane, ograniczając ekspozycję na podatności

10.1.3 P17S – Polityka ochrony danych i prywatności: nadaje priorytet działaniom naprawczym dotyczącym podatności w systemach przetwarzających dane osobowe w celu zapewnienia zgodności z przepisami o ochronie prywatności

10.1.4 P22S – Polityka rejestrowania i monitorowania: wspiera wykrywanie systemów bez wdrożonych poprawek lub podejrzanych zachowań, które mogą sygnalizować wykorzystywanie podatności

10.1.5 P30S – Polityka reagowania na incydenty: określa procedury reagowania na podatności prowadzące do incydentów bezpieczeństwa, w tym ścieżki eskalacji i obowiązki sprawozdawcze

11. Normy i ramy odniesienia

11.1 ISO/IEC 27001

11.1.1 Klauzula 8.1 – wymaga wdrożenia środków kontrolnych służących ograniczaniu ryzyka operacyjnego, w tym zarządzania podatnościami

11.2 ISO/IEC 27002

11.2.1 Środek kontrolny 8.8 – określa procesy skanowania i usuwania znanych słabości w systemach

11.2.2 Środek kontrolny 8.9 – podkreśla znaczenie bezpiecznej konfiguracji, walidacji poprawek i kontroli zmian w celu uniknięcia nowych ekspozycji podczas aktualizacji

11.3 NIST SP 800-53 Rev.5

11.3.1 RA-5 – wymaga identyfikacji podatności i działań naprawczych w określonych terminach

11.3.2 SI-2 – wymaga niezwłocznego wdrażania poprawek i aktualizacji zależnie od ich krytyczności

11.3.3 CM-2 – reguluje konfiguracje bazowe systemów i dokumentowanie aktualizacji w celu zapewnienia spójnych zabezpieczeń

11.4 RODO

11.4.1 Artykuł 32(1)(b) – wymaga, aby organizacje wdrażały odpowiednie środki techniczne, w tym poprawki, w celu zapewnienia bezpieczeństwa przetwarzania

11.5 Dyrektywa UE NIS2

11.5.1 Artykuł 21(2)(d) – wymaga obsługi podatności poprzez systematyczne skanowanie i działania naprawcze

11.5.2 Artykuł 21(2)(e) – nakłada obowiązek bezpiecznej konfiguracji i zarządzania poprawkami w celu zapewnienia odporności ICT

11.6 Rozporządzenie DORA

11.6.1 Artykuł 8(1) – wymaga wykrywania i ograniczania ryzyk ICT, w tym podatności technicznych

11.6.2 Artykuł 10(2) – zobowiązuje podmioty finansowe do usuwania słabości wpływających na systemy i operacje ICT

11.7 COBIT 2019

11.7.1 DSS05.02 – wymaga postępowania ze znanymi podatnościami technicznymi w celu utrzymania bezpiecznych operacji

11.7.2 APO12.01 – wiąże zarządzanie ryzykiem z proaktywnym monitorowaniem i korygowaniem słabości systemowych