					Wprowadź tutaj nazwę zarejestrowanej osoby prawnej							
Numer dokumentu: P19					Tytuł dokumentu: **Polityka zarządzania podatnościami i poprawkami**							
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	Systematyczne postępowanie z podatnościami technicznymi; bieżące zapewnienie skuteczności zabezpieczeń.
ISO/IEC 27002:2022	Zabezpieczenia 8.8, 8.9, 5	Wytyczne wdrożeniowe dotyczące wdrażania poprawek, skanowania podatności, integralności oprogramowania, bezpiecznej konfiguracji oraz inwentaryzacji aktywów.
NIST SP 800-53 Rev.5	RA-5, SI-2, CM-2, CM-6	Wymagane jest częste skanowanie, usuwanie błędów oraz zarządzanie konfiguracją.
EU GDPR	Artykuł 32, Motyw 49	Środki techniczne zapewniające niezwłoczne wdrażanie poprawek, obsługę podatności oraz ciągłość bezpieczeństwa.
EU NIS2	Artykuł 21(2)(d)	Wykrywanie podatności, reagowanie na nie i ich ograniczanie w celu utrzymania wysokiego poziomu cyberhigieny.
EU DORA	Artykuły 8, 10(2)(f)	Terminowa remediacja podatności ICT; ciągłe oceny ukierunkowane na zagrożenia.
COBIT 2019	DSS05.02, DSS01.03, MEA	Skanowanie, śledzenie i ograniczanie znanych słabości technicznych; monitorowanie pod kątem wykorzystania; audyt skuteczności, w tym statusu poprawek.

1. Cel

1.1 Niniejsza polityka określa obowiązkowe wymagania organizacji dotyczące identyfikowania, klasyfikowania, usuwania oraz monitorowania podatności technicznych i błędów oprogramowania we wszystkich systemach informacyjnych i aktywach objętych zakresem Systemu Zarządzania Bezpieczeństwem Informacji (SZBI).

1.2 Zapewnia ona, że wszystkie znane podatności są oceniane i obsługiwane terminowo oraz w sposób oparty na ryzyku, poprzez skoordynowane wdrażanie poprawek, zmiany konfiguracji lub kompensacyjne zabezpieczenia, zgodnie z potrzebami biznesowymi i obowiązkami zgodności.

1.3 Niniejsza polityka wspiera zgodność z ISO/IEC 27001, Załącznik A, zabezpieczenie 8.8 oraz wytycznymi ISO/IEC 27002, a także uwzględnia wymagania regulacyjne wynikające z artykułu 8 DORA, artykułu 21 NIS2, artykułu 32 RODO oraz obszarów DSS i APO w COBIT 2019.

2. Zakres

2.1 Niniejsza polityka ma zastosowanie do wszystkich systemów informacyjnych, aktywów i środowisk, które przechowują, przetwarzają lub przesyłają dane podlegające nadzorowi SZBI, w tym do:

2.1.1 systemów operacyjnych, aplikacji, urządzeń sieciowych, oprogramowania układowego, platform chmurowych, interfejsów API oraz oprogramowania stron trzecich.

2.1.2 systemów w środowiskach deweloperskich, testowych, produkcyjnych, kopii zapasowych oraz odtwarzania po awarii.

2.1.3 punktów końcowych, serwerów, urządzeń Internetu rzeczy (IoT), infrastruktury wirtualizacyjnej oraz kontenerów.

2.2 Jest ona wiążąca dla:

2.2.1 personelu wewnętrznego: administratorów IT, inżynierów systemowych, programistów aplikacji, analityków bezpieczeństwa oraz zespołów infrastruktury.

2.2.2 stron zewnętrznych: wykonawców, dostawców usług zarządzanych (MSP), dostawców oprogramowania oraz integratorów ponoszących odpowiedzialność techniczną za aktywa objęte zakresem.

2.3 Polityka obejmuje pełny cykl życia zarządzania podatnościami i poprawkami, w tym:

2.3.1 skanowanie i wykrywanie

2.3.2 klasyfikację ryzyka i priorytetyzację

2.3.3 pozyskiwanie, testowanie, wdrażanie i planowanie wycofania zmian

2.3.4 obsługę odstępstw i planowanie kompensacyjnych zabezpieczeń

2.3.5 rejestrowanie, raportowanie oraz zapewnienie ścieżki audytowej

3. Cele

3.1 Zapewnienie, że wszystkie znane podatności są identyfikowane, oceniane i usuwane w sposób minimalizujący ekspozycję na ryzyko oraz zgodny z priorytetami operacyjnymi.

3.2 Ustanowienie spójnych, obowiązujących w całej organizacji procesów w zakresie skanowania podatności, klasyfikacji poziomu istotności (np. CVSS) oraz zarządzania poprawkami, w tym obsługi awaryjnej i planowania wycofania zmian.

3.3 Umożliwienie zarządzania bezpieczną konfiguracją poprzez zgodność z konfiguracjami bazowymi utwardzania, praktykami zarządzania zmianą oraz informacjami o zagrożeniach w czasie rzeczywistym.

3.4 Zapewnienie mierzalnej zgodności z zabezpieczeniami wynikającymi z regulacji i norm w zakresie integralności systemów, higieny poprawek oraz terminowego usuwania błędów.

3.5 Określenie odpowiedzialności i rozliczalności poszczególnych ról w pełnym cyklu życia zarządzania podatnościami, tak aby wszyscy interesariusze działali zgodnie z określonymi umowami o poziomie usług (SLA) i raportowanymi wskaźnikami kontrolnymi.

3.6 Zapewnienie gotowości do audytu i zwiększenie odporności na nowe zagrożenia, w tym podatności zero-day, aktywnie wykorzystywane łańcuchy exploitów oraz istotne publiczne ujawnienia dostawców.

4. Role i odpowiedzialności

4.1 Dyrektor ds. bezpieczeństwa informacji (CISO)

4.1.1 Odpowiada za niniejszą politykę i zapewnia jej integrację w ramach SZBI.

4.1.2 Określa profil ryzyka organizacji i zapewnia zgodność z oczekiwaniami regulacyjnymi oraz kontrolnymi.

4.2 Osoba odpowiedzialna za zarządzanie podatnościami / Kierownik operacji bezpieczeństwa

4.2.1 Nadzoruje kompleksowe działania w zakresie zarządzania podatnościami i poprawkami.

4.2.2 Koordynuje harmonogramy skanowania, modele priorytetyzacji oraz terminy remediacji.

4.2.3 Utrzymuje Rejestr podatności i współpracuje przy ocenie kompensacyjnych zabezpieczeń.

[... 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 podlega przeglądowi co najmniej raz w roku lub w przypadku:

9.1.1 istotnych zmian regulacyjnych (np. zmian w DORA, NIS2)

9.1.2 zmian w ramach priorytetyzacji podatności (np. aktualizacji CVSS)

9.1.3 istotnych zmian w środowisku IT (np. migracji do chmury, istotnych zmian EDR)

9.1.4 istotnych naruszeń lub zewnętrznych komunikatów wymagających wzmocnienia polityki

9.2 Przeglądy są prowadzone przez CISO we współpracy z operacjami bezpieczeństwa, zarządzaniem ryzykiem oraz kierownictwem infrastruktury.

9.3 Aktualizacje polityki muszą być:

9.3.1 udokumentowane w rejestrze kontroli dokumentów SZBI

9.3.2 poddane przeglądowi i zatwierdzone przez kierownictwo wykonawcze

9.3.3 zakomunikowane wszystkim zainteresowanym stronom, w tym podmiotom przetwarzającym danych stron trzecich

9.4 Wersje historyczne muszą być bezpiecznie przechowywane do celów audytowych i rozliczalności.

10. Powiązane polityki i zależności

10.1 P1 - P01 Polityka bezpieczeństwa informacji. Określa nadrzędne zobowiązanie do ochrony systemów i danych, obejmujące proaktywne zarządzanie podatnościami oraz zapewnienie integralności oprogramowania.

10.2 P5 - P05 Polityka zarządzania zmianą. Reguluje wszystkie wdrożenia poprawek i zmiany konfiguracji, wymagając dokumentowania, testowania, zatwierdzania oraz procedur wycofania zmian wspierających procesy remediacji podatności.

10.3 P6 - Polityka zarządzania ryzykiem. Wspiera klasyfikację i postępowanie z nieusuniętymi podatnościami poprzez ustrukturyzowane oceny ryzyka, analizę wpływu oraz procedury akceptacji ryzyka rezydualnego.

10.4 P12 - Polityka zarządzania aktywami. Zapewnia prawidłową inwentaryzację i klasyfikację systemów, umożliwiając spójne skanowanie podatności, przypisanie właścicieli oraz pokrycie poprawkami w całym cyklu życia.

10.5 P22 - Polityka rejestrowania i monitorowania. Określa wymagania dotyczące wykrywania zdarzeń oraz generowania zapisów audytowych. Niniejsza polityka wspiera widoczność działań związanych z wdrażaniem poprawek, nieuprawnionych zmian oraz prób wykorzystania znanych podatności.

10.6 P30 - Polityka reagowania na incydenty (P30). Określa protokoły eskalacji i strategie powstrzymania dla wykorzystanych podatności, postępowań wyjaśniających dotyczących naruszeń oraz działań korygujących zgodnych z zabezpieczeniami niniejszej polityki.

11. Normy i ramy odniesienia

11.1 ISO/IEC 27001: Klauzula 8.1 - Planowanie i nadzór operacyjny: wymaga systematycznego postępowania z podatnościami technicznymi w celu zapewnienia bieżącej skuteczności zabezpieczeń.

11.2 ISO/IEC 27002:2022 - Zabezpieczenia 8.8, 8.9, 5: zawiera wytyczne wdrożeniowe dotyczące wdrażania poprawek, skanowania podatności, integralności oprogramowania oraz integracji z bezpieczną konfiguracją i inwentaryzacją aktywów.

11.3 NIST SP 800-53 Rev.5: RA-5 - Monitorowanie i skanowanie podatności: wymaga częstego skanowania i śledzenia remediacji. SI-2 - Usuwanie błędów: wymaga niezwłocznej oceny i

ograniczania błędów przy użyciu dostępnych poprawek lub innych działań. CM-2 / CM-6 - Konfiguracje bazowe i zabezpieczenia zarządzania konfiguracją: ustanawia podstawę bezpiecznych konfiguracji systemów powiązanych z egzekwowaniem poprawek.

11.4 EU GDPR (2016/679): Artykuł 32 - Bezpieczeństwo przetwarzania: wymaga wdrożenia odpowiednich środków technicznych, takich jak niezwłoczne wdrażanie poprawek i obsługa podatności, aby zapewnić poufność i odporność systemów. Motyw 49: zachęca podmioty do wdrażania zabezpieczeń zapobiegawczych przeciwko znanym zagrożeniom w celu wsparcia bezpieczeństwa i ciągłości działania.

11.5 Dyrektywa NIS2 UE (2022/2555): Artykuł 21(2)(d): nakłada na podmioty kluczowe i ważne obowiązek wykrywania podatności systemowych, reagowania na nie i ich ograniczania oraz utrzymywania wysokiego poziomu cyberhigieny.

11.6 EU DORA (2022/2554): Artykuł 8 - zarządzanie ryzykiem ICT: wymaga identyfikacji i terminowej remediacji podatności w technologiach informacyjno-komunikacyjnych wykorzystywanych w systemach finansowych. Artykuł 10(2)(f): podkreśla znaczenie ciągłych ocen podatności ukierunkowanych na zagrożenia oraz wdrażania poprawek jako elementu odporności operacyjnej.

11.7 COBIT 2019: DSS05.02 - Zarządzanie podatnościami bezpieczeństwa: nakazuje organizacjom skanowanie, śledzenie i ograniczanie znanych słabości technicznych. DSS01.03 - Monitorowanie infrastruktury: zapewnia monitorowanie systemów pod kątem oznak wykorzystania lub słabości. MEA03 - Monitorowanie, ocena i ocena zgodności: wymaga regularnego audytowania skuteczności zabezpieczeń, w tym statusu poprawek i obsługi odstępstw.