					Wprowadź tutaj nazwę zarejestrowanej osoby prawnej							
Numer dokumentu: P39					Tytuł dokumentu: **Polityka skoordynowanego ujawniania podatności**							
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	6.1.3	
ISO/IEC 27002:2022	5.7, 8.8, 8.9, 8.28, 8.29	
NIST SP 800-53 Rev.5	RA-5, SI-2, PM-15, CA-8, SR-6	
RODO	Art. 32(1)(d)	
Dyrektywa NIS2	Art. 21(2)(e)	
Rozporządzenie DORA	Art. 11(1)(d)	
COBIT 2019	DSS05.01, DSS05.07, BAI09.02, MEA02.01	

1. Cel

1.1 Ustanowienie formalnego procesu przyjmowania, obsługi i ujawniania informacji o podatnościach wpływających na systemy lub usługi organizacji, zgodnie z wymogami art. 21 ust. 2 lit. e Dyrektywy NIS2 w zakresie obsługi podatności i ich ujawniania.

1.2 Zachęcanie zewnętrznych badaczy bezpieczeństwa, partnerów i użytkowników do odpowiedzialnego zgłaszania podatności (Coordinated Vulnerability Disclosure - CVD) oraz określenie sposobu, w jaki organizacja komunikuje informacje o podatnościach interesariuszom.

2. Zakres

2.1 Niniejsza polityka ma zastosowanie do wszystkich systemów sieciowych i informacyjnych będących własnością organizacji lub przez nią eksploatowanych oraz do wszelkich zidentyfikowanych podatności w tych systemach.

2.2 Obejmuje zespoły wewnętrzne (bezpieczeństwa informacji, IT, rozwoju oprogramowania) oraz wszystkie podmioty zewnętrzne zgłaszające podatności (np. badaczy, klientów, dostawców). Reguluje również komunikację z dostawcami produktów lub usług, jeżeli ich komponenty są powiązane z daną podatnością.

3. Cele

3.1 Wykrywanie i usuwanie podatności bezpieczeństwa w odpowiednim czasie, z wykorzystaniem zarówno ocen wewnętrznych, jak i zgłoszeń zewnętrznych.

3.2 Zapewnienie jasnych wytycznych dla podmiotów zewnętrznych zgłaszających podatności, aby mogły bezpiecznie i zgodnie z prawem przekazywać informacje o podatnościach, a organizacja mogła skutecznie reagować i wdrażać działania naprawcze.

3.3 Zapewnienie zgodności z wymaganiami Dyrektywy NIS2 oraz branżowymi dobrymi praktykami (ISO/IEC 29147 i 30111) w zakresie skoordynowanego ujawniania podatności, wzmacniając ogólny poziom bezpieczeństwa ekosystemu.

4. Role i odpowiedzialności

4.1 Zespół reagowania na podatności (VRT): wyznaczony zespół, kierowany przez Dyrektora ds. Bezpieczeństwa Informacji (CISO) lub osobę odpowiedzialną za zarządzanie podatnościami, który przyjmuje zgłoszenia podatności, prowadzi triage, ocenia ryzyko i wpływ oraz koordynuje remediację i publiczne ujawnienie.

4.2 Zespoły IT, bezpieczeństwa informacji oraz rozwoju oprogramowania: współpracują z VRT w celu walidacji zgłoszonych podatności, opracowania i testowania poprawek lub działań mitygujących oraz wdrożenia poprawek. W razie potrzeby przekazują szczegóły techniczne do komunikatów.

[... Sekcje 4.3–8 nie są uwzględnione w tej wersji zapoznawczej. Zakup pełny dokument, aby uzyskać dostęp do pełnej treści. ...]

9. Monitorowanie i audyt

9.1 VRT prowadzi rejestr ujawnień podatności obejmujący śledzenie każdego zgłoszenia od momentu przyjęcia do zamknięcia. Rejestr ten jest przeglądany co miesiąc w celu zapewnienia terminowej realizacji otwartych spraw. Pozycje przeterminowane podlegają eskalacji.

9.2 Funkcja audytu wewnętrznego lub zgodności, albo niezależny asesor bezpieczeństwa, dokonuje corocznego przeglądu skuteczności procesu obsługi podatności — np. sprawdzając, czy próbki przypadków podatności były obsługiwane zgodnie z polityką (potwierdzone, usunięte, ujawnione w odpowiednim czasie). Weryfikuje również, czy publicznie dostępny kanał zgłaszania działa prawidłowo (np. czy wiadomości testowe są odbierane i obsługiwane).

9.3 Wskaźniki dotyczące podatności (liczba według wagi, czasy remediacji itp.) są zestawiane kwartalnie i przedstawiane komitetowi ds. ładu cyberbezpieczeństwa w celu uwzględnienia przy aktualizacji oceny ryzyka.

10. Przegląd i utrzymanie

10.1 Niniejsza polityka podlega przeglądowi co najmniej raz w roku. Dodatkowo każda istotna zmiana w środowisku IT organizacji (np. uruchomienie nowej usługi dostępnej z Internetu) lub istotne zmiany regulacyjne (np. nowe przepisy UE dotyczące ujawniania podatności produktów) skutkują przeglądem pozaplanowym.

10.2 Aktualizacje polityki uwzględniają informacje zwrotne od podmiotów zewnętrznych zgłaszających podatności oraz wnioski z wewnętrznych analiz po incydencie. Istotne zmiany są zatwierdzane przez CISO, komunikowane całemu personelowi oraz publikowane w internetowym repozytorium polityk bezpieczeństwa organizacji w celu zapewnienia przejrzystości.

11. Powiązane polityki i zależności

11.1 P01 – P01 Polityka bezpieczeństwa informacji. Mandat zarządczy dla obsługi i ujawniania podatności.

11.2 P19 – Polityka zarządzania podatnościami i poprawkami. Wewnętrzny proces remediacji powiązany z przyjmowaniem zgłoszeń CVD.

11.3 P24 – Polityka bezpiecznego rozwoju oprogramowania. Zasila proces SDLC poprawkami i działaniami wzmacniającymi na podstawie zgłoszonych problemów.

11.4 P25 – Polityka wymagań bezpieczeństwa aplikacji. Zapewnia, że produkty mają wymagania bezpieczeństwa uwzględniające potrzeby związane z ujawnianiem podatności.

11.5 P30 – Polityka reagowania na incydenty (P30). Obejmuje przypadki aktywnego wykorzystania ujawnionych podatności.

11.6 P31 – Polityka zabezpieczania materiału dowodowego i informatyki śledczej. Zapewnia zabezpieczenie artefaktów związanych ze zgłoszonymi lub wykorzystanymi błędami.

11.7 P26 – Polityka bezpieczeństwa dostawców i stron trzecich. Koordynuje ujawnienia dotyczące komponentów dostawców.

11.8 P37 – Polityka zgodności prawnej i regulacyjnej. Reguluje powiadomienia, treść klauzuli bezpiecznej przystani i publikację.

12. Odniesienia

12.1 Dyrektywa NIS2 (UE 2022/2555), art. 21 ust. 2 lit. e (bezpieczeństwo w rozwoju oraz obsługa i ujawnianie podatności)

12.2 Rozporządzenie wykonawcze Komisji (UE) 2024/2690, załącznik, sekcja 6.10 (wymagania techniczne dotyczące procesów obsługi i ujawniania podatności)

12.3 Wytyczne techniczne ENISA dotyczące środków zarządzania ryzykiem cyberbezpieczeństwa – sekcja dotycząca obsługi i ujawniania podatności

12.4 ISO/IEC 27001:2022 / ISO/IEC 27002:2022 (środek kontrolny A.5.7 dotyczący informacji o zagrożeniach i ujawniania podatności; środek kontrolny A.8.28 dotyczący bezpiecznego rozwoju oprogramowania)

12.5 ISO/IEC 29147:2018 (wytyczne dotyczące ujawniania podatności) oraz ISO/IEC 30111:2019 (wytyczne dotyczące procesów obsługi podatności)