					Wprowadź tutaj nazwę zarejestrowanej osoby prawnej							
Numer dokumentu: P30					Tytuł dokumentu: **Polityka reagowania na incydenty**							
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 8.1, Klauzula 9	Ustrukturyzowane procesy zarządzania ryzykiem i reagowania na incydenty
ISO/IEC 27002:2022	Zabezpieczenia 5.25–5.27	Role, zgłaszanie, reagowanie i doskonalenie w obszarze incydentów
NIST SP 800-53 Rev.5	IR-1 do IR-9	Kompleksowy cykl życia reagowania na incydenty
RODO	Art. 33 ust. 1, 33 ust. 3 lit. a–d, 34 ust. 1, 34 ust. 2 lit. a–c	Terminy zgłaszania naruszeń, raportowanie oraz komunikacja z osobami, których dane dotyczą
Dyrektywa NIS2	Art. 23 ust. 1–4	Zgłoszenia do właściwego organu krajowego i ustrukturyzowane raportowanie
Rozporządzenie DORA	Art. 17 ust. 1–3	Zgłaszanie poważnych incydentów związanych z ICT przez podmioty finansowe
COBIT 2019	DSS02, DSS04, MEA	Definiowanie, monitorowanie i ocena zarządzania incydentami, ciągłością działania i mechanizmami oceny

1. Cel

1.1 Niniejsza polityka ustanawia formalne ramy identyfikacji, zgłaszania, analizy, powstrzymywania, reagowania, odtwarzania oraz oceny poincydentalnej w odniesieniu do incydentów bezpieczeństwa informacji wpływających na organizację.

1.2 Zapewnia terminową, skoordynowaną i skuteczną reakcję w celu ograniczenia zakłóceń operacyjnych, strat finansowych, szkód reputacyjnych oraz niezgodności regulacyjnych.

1.3 Polityka wspiera również ciągłe doskonalenie poziomu cyberodporności organizacji poprzez wykorzystanie wniosków z incydentów oraz integrację ustaleń poincydentalnych z ładem organizacyjnym, narzędziami i programami szkoleniowymi.

2. Zakres

2.1 Niniejsza polityka ma zastosowanie do:

2.1.1 całego personelu, w tym pracowników, wykonawców, konsultantów i dostawców usług zewnętrznych

2.1.2 wszystkich systemów informatycznych, aplikacji, infrastruktury, sieci i danych — niezależnie od tego, czy są utrzymywane lokalnie, w chmurze obliczeniowej czy w modelu hybrydowym

2.1.3 wszystkich rodzajów incydentów bezpieczeństwa, w tym między innymi:

2.1.3.1 nieuprawnionego dostępu lub eskalacji uprawnień

2.1.3.2 ataków z użyciem złośliwego oprogramowania i ransomware

2.1.3.3 ataków odmowy usługi (DoS/DDoS)

2.1.3.4 utraty danych, wycieków danych lub eksfiltracji danych

2.1.3.5 niewłaściwych działań pracowników lub naruszeń polityk

2.1.3.6 naruszeń bezpieczeństwa fizycznego wpływających na aktywa cyfrowe

2.2 Polityka obejmuje wykrywanie, triage, dochodzenie, eskalację, powstrzymywanie, postępowanie z materiałem dowodowym, powiadamianie, odtwarzanie oraz analizę przyczyny źródłowej.

3. Cele

3.1 Ustanowienie powtarzalnej i skalowalnej zdolności reagowania na incydenty, umożliwiającej szybkie wykrywanie, klasyfikację i ograniczanie skutków incydentów bezpieczeństwa.

3.2 Ograniczenie wpływu zdarzeń bezpieczeństwa informacji na działalność biznesową poprzez ustrukturyzowane procedury powstrzymywania, usuwania zagrożenia i odtwarzania systemów.

3.3 Zapewnienie, że zgłaszanie incydentów i reagowanie na nie są zgodne z wymaganiami prawnymi, regulacyjnymi i umownymi — w szczególności w zakresie terminów zgłaszania naruszeń oraz postępowania z materiałem dowodowym.

3.4 Wspieranie przejrzystości i rozliczalności poprzez właściwe rejestrowanie, dokumentowanie oraz monitorowanie wskaźników dla wszystkich incydentów bezpieczeństwa.

3.5 Promowanie ciągłego doskonalenia poprzez przeglądy poincydentalne, działania korygujące i szkolenia interesariuszy.

4. Role i odpowiedzialności

4.1 Dyrektor ds. Bezpieczeństwa Informacji (CISO)

4.1.1 Odpowiada za ramy reagowania na incydenty, zapewnia stosowanie polityki oraz nadzoruje koordynację obsługi incydentów w całej organizacji.

4.1.2 Pełni rolę głównego punktu kontaktowego wobec organów regulacyjnych, najwyższego kierownictwa i zewnętrznych doradców prawnych podczas poważnych incydentów.

4.2 Koordynator reagowania na incydenty

4.2.1 Koordynuje międzyfunkcyjne zespoły reagowania, zarządza przebiegiem prac oraz monitoruje status powstrzymywania i odtwarzania.

4.2.2 Inicjuje i prowadzi przegląd poincydentalny (PIR) oraz zapewnia, że działania korygujące są rejestrowane i wdrażane.

[... 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 co najmniej raz w roku i aktualizowana w razie potrzeby w celu uwzględnienia:

9.1.1 zmian w krajobrazie zagrożeń, typach incydentów lub wektorach ataku

9.1.2 wniosków z poważnych incydentów, sytuacji bliskich incydentowi lub ustaleń regulacyjnych

9.1.3 aktualizacji obowiązujących przepisów prawa i regulacji (np. RODO, DORA, NIS2)

9.1.4 informacji zwrotnych z ćwiczeń reagowania na incydenty i przeglądów poincydentalnych

9.2 CISO odpowiada za inicjowanie i koordynowanie procesu przeglądu, w konsultacji z:

9.2.1.1 doradcą prawnym i IOD

9.2.1.2 SOC i operacjami IT

9.2.1.3 zespołami ds. ciągłości działania i zarządzania ryzykiem

9.2.1.4 najwyższym kierownictwem

9.3 Zmiany polityki muszą być:

9.3.1 dokumentowane w repozytorium objętym kontrolą wersji

9.3.2 komunikowane wszystkim zespołom objętym wpływem oraz uwzględniane w szkoleniach uświadamiających

9.3.3 walidowane poprzez ćwiczenia typu tabletop lub praktyczne ćwiczenia reagowania na incydenty w ciągu trzech miesięcy od zatwierdzenia

9.4 Pilne aktualizacje wynikające z nowych zagrożeń, ustaleń audytowych lub nowo ustanowionych obowiązków prawnych muszą być wdrażane niezwłocznie i odnotowywane w historii zmian polityki.

10. Powiązane polityki i zależności

10.1 Niniejsza polityka jest wspierana przez następujące polityki organizacyjne i od nich zależna:

10.1.1 P1 – Polityka bezpieczeństwa informacji: określa nadrzędny wymóg prowadzenia działań operacyjnych w oparciu o ryzyko oraz utrzymywania gotowości do reagowania na incydenty.

10.1.2 P5 – Polityka zarządzania zmianą: zapewnia, że działania związane z powstrzymywaniem i odtwarzaniem obejmujące infrastrukturę lub usługi są realizowane zgodnie z formalnymi procedurami.

10.1.3 P13 – Polityka klasyfikacji i oznaczania informacji: wspiera klasyfikację istotności incydentów na podstawie wrażliwości danych.

10.1.4 P15 – Polityka tworzenia kopii zapasowych i odtwarzania: umożliwia odtworzenie po ransomware lub atakach destrukcyjnych przy zachowaniu integralności.

10.1.5 P18 – Polityka zabezpieczeń kryptograficznych: określa środki szyfrowania ograniczające wpływ incydentów i ryzyko ujawnienia danych.

10.1.6 P22 – Polityka logowania i monitorowania: zapewnia podstawową widoczność zdarzeń, alertowanie oraz przechowywanie logów wymagane do skutecznego wykrywania i informatyki śledczej.

10.1.7 P29 – Polityka danych testowych i środowisk testowych: zapewnia, że incydenty wpływające na środowiska nieprodukcyjne są również obsługiwane w sposób ustrukturyzowany i bezpieczny.

10.1.8 P33 – Polityka monitorowania audytu i zgodności: potwierdza gotowość do reagowania na incydenty i skuteczność reakcji poprzez ustrukturyzowane audyty oraz oceny zgodności.

11. Normy i ramy odniesienia

11.1 ISO/IEC 27001: Klauzula 8.1 – Planowanie operacyjne i nadzór: ustrukturyzowane procesy zarządzania ryzykiem i planowania reagowania na incydenty.

11.2 ISO/IEC 27002:2022 – Zabezpieczenia 5.25–5.27: odpowiedzialności w zakresie zarządzania incydentami, zgłaszania, reagowania, komunikacji i doskonalenia.

11.3 NIST SP 800-53 Rev.5: IR-1 do IR-9, AU-6, PL-2: kompleksowe wymagania dotyczące cyklu życia reagowania na incydenty, audytu i planowania bezpieczeństwa.

11.4 RODO: Art. 33/34: obowiązki sprawozdawcze wobec organów nadzorczych oraz wymagania dotyczące powiadamiania osób, których dane dotyczą (z określonymi wyjątkami).

11.5 Dyrektywa UE NIS2 (2022/2555): Art. 23: obowiązkowe raportowanie do właściwych organów krajowych, wraz z obowiązkami raportowania pośredniego i końcowego.

11.6 Rozporządzenie DORA (2022/2554): Art. 17: wymagania dotyczące zgłaszania incydentów ICT właściwym organom przez instytucje finansowe.

11.7 COBIT 2019: DSS02, DSS04, MEA01: zarządzanie incydentami usług i ciągłością działania oraz monitorowanie efektywności i zgodności.