					Wprowadź tutaj nazwę zarejestrowanej osoby prawnej							
Numer dokumentu: P06					Tytuł dokumentu: **Polityka zarządzania ryzykiem**							
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**

Zgodność z normami i regulacjami, tam gdzie ma to zastosowanie

Norma/regulacja	Klauzula/artykuł	Komentarz
ISO/IEC 27001:2022	Klauzule 6.1, 8.32, 10	Podstawowe wymagania dotyczące identyfikacji ryzyka i zarządzania ryzykiem, integracja z zarządzaniem zmianą, ciągłe doskonalenie
ISO/IEC 27005:2024	Pełna metodyka cyklu życia ryzyka	Pełny proces zarządzania ryzykiem zgodny z normą
ISO 31000:2018	Zasady i ramy zarządzania ryzykiem	Zasady zarządzania ryzykiem przyjęte w ramach postępowania
NIST SP 800-30 Rev.1	SP 800-30, SP 800-39	Wytyczne i struktura dla ocen ryzyka, warstwowy nadzór nad ryzykiem
RODO	Artykuły 24, 25, 32	Procesy i mechanizmy kontrolne dotyczące ryzyk związanych z ochroną danych
Dyrektywa NIS2	Artykuł 21(2)(a–d)	Obowiązki w zakresie oceny ryzyka i bezpieczeństwa
Rozporządzenie DORA	Artykuły 5, 6	Zarządzanie ryzykiem ICT i odporność operacyjna
COBIT 2019	APO12, MEA	Struktura zarządzania ryzykiem i nadzór

1. Cel

1.1 Niniejsza polityka ustanawia jednolite i sformalizowane ramy identyfikacji, analizy, oceny, postępowania z ryzykiem, monitorowania oraz przeglądu ryzyk bezpieczeństwa informacji w całej organizacji.

1.2 Zapewnia spójne stosowanie zasad opartych na ryzyku, które chronią poufność, integralność i dostępność (CIA) aktywów informacyjnych, zgodnie z klauzulą 6.1 normy ISO/IEC 27001:2022 oraz ISO 31000:2018.

1.3 Polityka włącza zarządzanie ryzykiem bezpieczeństwa informacji do procesów decyzyjnych organizacji w celu realizacji wewnętrznych celów strategicznych oraz spełnienia zewnętrznych wymagań regulacyjnych.

2. Zakres

2.1 Niniejsza polityka ma zastosowanie do wszystkich jednostek organizacyjnych, procesów biznesowych, systemów, personelu oraz relacji ze stronami trzecimi związanych z przetwarzaniem, rozwojem, przechowywaniem lub zarządzaniem aktywami informacyjnymi.

2.2 Zakres obejmuje aktywa fizyczne, cyfrowe oraz aktywa utrzymywane w chmurze, w tym dane ustrukturyzowane i nieustrukturyzowane, aplikacje, infrastrukturę, sieci i usługi.

2.3 Obejmuje ryzyka bezpieczeństwa informacji na poziomie strategicznym, operacyjnym, projektowym i technicznym oraz jest obowiązkowa dla wszystkich pracowników, kontraktorów i dostawców usług zaangażowanych w działania w ramach Systemu Zarządzania Bezpieczeństwem Informacji (SZBI).

2.4 Zarządzanie ryzykiem musi być stosowane w następujących scenariuszach:

2.4.1 wdrożenie nowego projektu lub systemu

2.4.1.1 znaczące zmiany (np. architektura, własność, procesy)

2.4.1.2 wdrożenie dostawcy i umowy ze stronami trzecimi

2.4.1.3 reagowanie na incydenty i przeglądy po incydencie

2.4.1.4 okresowe przeglądy ryzyka w organizacji lub audyty

3. Cele

3.1 Ustanowienie i operacyjne wdrożenie powtarzalnego, obejmującego całą organizację procesu zarządzania ryzykiem opartego na metodykach ISO/IEC 27005 i ISO 31000.

3.2 Zapewnienie, że ryzyka są identyfikowane, analizowane, oceniane i poddawane postępowaniu z wykorzystaniem ustrukturyzowanych i możliwych do prześledzenia metod, w tym poprzez przypisanie właścicieli ryzyka i powiązań ze środkami kontroli.

3.3 Utrzymanie scentralizowanego rejestru ryzyk oraz planu postępowania z ryzykiem, objętych kontrolą wersji, odzwierciedlających bieżący status ryzyka, pokrycie środkami kontroli oraz postęp działań ograniczających ryzyko.

3.4 Dostosowanie decyzji dotyczących ryzyka do udokumentowanego apetytu na ryzyko i poziomów tolerancji ryzyka oraz umożliwienie świadomych decyzji w ramach ładu organizacyjnego dotyczących akceptacji, ograniczania, transferu lub unikania ryzyka.

3.5 Ciągłe monitorowanie trendów ryzyka i zapewnienie skuteczności działań związanych z postępowaniem z ryzykiem, przy jednoczesnym umożliwieniu proaktywnego dostosowania do zmian zagrożeń lub zmian biznesowych.

4. Role i odpowiedzialności

4.1 Kierownictwo wykonawcze / Rada Dyrektorów

4.1.1 Zatwierdza ramy zarządzania ryzykiem i określa dopuszczalny apetyt na ryzyko oraz progi tolerancji ryzyka.

4.1.2 Zatwierdza strategie postępowania z ryzykiem dla ryzyk rezydualnych przekraczających tolerancję.

4.1.3 Przydziela zasoby i sprawuje nadzór nad skutecznym działaniem programu zarządzania ryzykiem.

4.2 Menedżer Systemu Zarządzania Bezpieczeństwem Informacji / Menedżer Ryzyka

4.2.1 Odpowiada za niniejszą politykę i utrzymuje jej zgodność z normami ISO/IEC 27001 i ISO/IEC 27005.

4.2.2 Kieruje procesem oceny ryzyka w organizacji oraz utrzymuje rejestr ryzyk i plan postępowania z ryzykiem.

4.2.3 Zapewnia okresowe przeglądy oraz eskalację kluczowych ryzyk do kierownictwa wykonawczego lub komitetu sterującego SZBI.

[... 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 i powiązane z nią ramy muszą podlegać corocznemu przeglądowi lub częściej:

9.1.1 po istotnym zdarzeniu ryzyka lub incydencie bezpieczeństwa

9.1.2 po znaczącej zmianie organizacyjnej lub technicznej

9.1.3 w odpowiedzi na ustalenia audytowe lub nowe wymagania regulacyjne

9.2 Menedżer Systemu Zarządzania Bezpieczeństwem Informacji, Menedżer Ryzyka oraz zespół ds. zgodności wspólnie odpowiadają za:

9.2.1 inicjowanie cyklu przeglądu

9.2.2 gromadzenie informacji wejściowych od jednostek biznesowych

9.2.3 aktualizację procedur i progów w razie potrzeby

9.3 Wszystkie zmiany muszą być:

9.3.1 objęte kontrolą wersji i rejestrowane

9.3.2 zatwierdzane przez kierownictwo wykonawcze

9.3.3 komunikowane interesariuszom

9.3.4 przechowywane w repozytorium audytowym przez co najmniej 5 lat

10. Powiązane polityki i zależności

10.1 Niniejsza polityka pozostaje współzależna z następującymi politykami bezpieczeństwa informacji:

10.1.1 P1 – Polityka bezpieczeństwa informacji: ustanawia ogólny model ładu bezpieczeństwa, w ramach którego funkcjonuje niniejsza polityka ryzyka.

10.1.2 P2 – Polityka ról i odpowiedzialności w ramach ładu organizacyjnego: definiuje właścicieli odpowiedzialnych za rozliczalność oraz poziomy ładu organizacyjnego, do których odwołuje się macierz eskalacji ryzyka.

10.1.3 P5 – Polityka zarządzania zmianą: inicjuje ponowną ocenę ryzyka dla zmian infrastrukturalnych i organizacyjnych.

10.1.4 P13 – Polityka klasyfikacji i etykietowania danych: wspiera ocenę wpływu na etapie identyfikacji ryzyka.

10.1.5 P33 – Polityka audytu i monitorowania zgodności: weryfikuje przestrzeganie polityki, w tym kompletność rejestru ryzyk i dowody realizacji działań związanych z postępowaniem z ryzykiem.

11. Normy i ramy odniesienia

11.1 Niniejsza polityka jest bezpośrednio dostosowana do następujących norm i ram, aby zapewnić zgodność z międzynarodowymi dobrymi praktykami oraz oczekiwaniami regulacyjnymi w zakresie zarządzania ryzykiem bezpieczeństwa informacji:

11.2 ISO/IEC 27001:

11.2.1 Klauzula 6.1: określa wymagania dotyczące identyfikacji ryzyk i szans, w tym pełnego cyklu życia ocen ryzyka bezpieczeństwa informacji oraz postępowania z ryzykiem. Niniejsza polityka operacjonalizuje klauzule 6.1.2 i 6.1.3 poprzez ustrukturyzowane ramy nakładające obowiązek udokumentowanej identyfikacji, analizy, oceny, postępowania z ryzykiem oraz protokołów akceptacji ryzyka rezydualnego.

11.2.2 Klauzula 8.32: integracja podejścia opartego na ryzyku z procesami zarządzania zmianą zapewnia, że wszystkie znaczące zmiany organizacyjne uruchamiają formalne ponowne oceny ryzyka.

11.2.3 Klauzula 10: ciągłe doskonalenie jest realizowane poprzez regularne przeglądy polityki, analizę trendów ryzyka oraz aktualizacje SoA wynikające z wniosków płynących z analizy ryzyka.

11.3 ISO/IEC 27005:

11.3.1 Zapewnia wyspecjalizowane i szczegółowe wytyczne dotyczące zarządzania ryzykiem bezpieczeństwa informacji. Niniejsza polityka wdraża pełny model procesu ryzyka według ISO/IEC 27005: ustanowienie kontekstu, identyfikacja ryzyka, analiza ryzyka, ocena ryzyka, postępowanie z ryzykiem, akceptacja ryzyka, komunikowanie ryzyka, monitorowanie i przegląd ryzyka.

11.4 ISO 31000:

11.4.1 Niniejsza polityka integruje zasady ISO 31000, takie jak zaangażowanie kierownictwa, integracja z procesami decyzyjnymi oraz ciągłe doskonalenie. Zapewnia to osadzenie zarządzania ryzykiem w kulturze i działalności organizacji.

11.5 NIST SP 800-30 Rev.1:

11.5.1 Jest zgodna z przewodnikiem NIST dotyczącym prowadzenia ocen ryzyka, w tym identyfikacji zagrożeń, analizy podatności, szacowania prawdopodobieństwa i określania skutków. Struktura niniejszej polityki odzwierciedla kroki oceny ryzyka zdefiniowane przez NIST i dostosowuje je zarówno do procesów technicznych, jak i biznesowych.

11.6 NIST SP 800-39:

11.6.1 Wspiera nadzór nad ryzykiem na poziomie organizacji, podkreślając warstwowe zarządzanie ryzykiem na poziomie organizacji, misji/procesów biznesowych i systemów informacyjnych. Polityka zapewnia jednoznaczne określenie właścicieli ryzyka na wszystkich poziomach oraz uwzględnia strategie postępowania z ryzykiem na poziomie organizacji.

11.7 RODO:

11.7.1 Artykuł 24: wymaga wdrożenia odpowiednich środków technicznych i organizacyjnych w celu zapewnienia właściwego zarządzania ryzykami związanymi z ochroną danych — co realizuje niniejsza polityka poprzez ustrukturyzowany proces ryzyka.

11.7.2 Artykuł 25: „ochrona danych w fazie projektowania i domyślna ochrona danych” jest zgodna z włączaniem postępowania z ryzykiem do projektowania systemów i procesów.

11.7.3 Artykuł 32: nakłada obowiązek podejścia opartego na ryzyku do środków bezpieczeństwa — realizowanego poprzez ocenę ryzyka opartą na skutkach oraz dobór środków kontroli.

11.8 Dyrektywa NIS2:

11.8.1 Artykuł 21(2)(a–d): wymaga od podmiotów prowadzenia ocen ryzyka, wdrażania polityk w zakresie analizy ryzyka oraz zapewnienia proporcjonalnych środków bezpieczeństwa. Niniejsza polityka spełnia te obowiązki poprzez ciągłe stosowanie pełnego cyklu życia ryzyka i udokumentowany ład organizacyjny.

11.9 Rozporządzenie DORA:

11.9.1 Artykuł 5: wymaga udokumentowanych ram zarządzania ryzykiem ICT — w pełni objętych architekturą niniejszej polityki, w tym mapowaniem do SoA i KRI.

11.9.2 Artykuł 6: wymaga integracji zarządzania ryzykiem ze strategiami odporności operacyjnej, co jest realizowane poprzez macierze eskalacji i śledzenie aktywów krytycznych.

11.10 COBIT 2019:

11.10.1 APO12 – Zarządzanie ryzykiem: bezpośrednio odpowiada ustanowionemu w organizacji ustrukturyzowanemu podejściu do zarządzania ryzykiem, przypisywaniu ról, śledzeniu działań związanych z postępowaniem z ryzykiem oraz zapewnieniu rozliczalności na poziomie Rady Dyrektorów.

11.10.2 MEA01 – Monitorowanie, ocena i analiza wydajności oraz zgodności: odzwierciedlone w ukierunkowaniu niniejszej polityki na analizę trendów, monitorowanie KRI oraz włączanie informacji zwrotnej z audytu do pętli ciągłego doskonalenia.