					Wprowadź tutaj nazwę zarejestrowanej osoby prawnej							
Numer dokumentu: P06S					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**

Nota prawna (prawa autorskie i ograniczenia użytkowania)

(C) 2025 Clarysec LLC. All rights reserved.

Niniejszy dokument stanowi własność intelektualną spółki Clarysec LLC. Żadna część tego dokumentu nie może być kopiowana, ponownie wykorzystywana, rozpowszechniana ani modyfikowana do celów komercyjnych lub wdrożeniowych bez uprzedniej wyraźnej pisemnej zgody.
Nieuprawnione użycie jest surowo zabronione i może skutkować podjęciem kroków prawnych.
W sprawach licencjonowania prosimy o kontakt: info@clarysec.com

Zgodność z normami i regulacjami

Norma/regulacja	Klauzula/artykuł	Komentarz
ISO/IEC 27001:2022	Klauzule 6.1, 6.1.3	
ISO/IEC 27002:2022	5.4, 5.25	
NIST SP 800-53 Rev. 5	RA-1 do RA-7, PM-9	
Dyrektywa NIS2	Artykuł 21 ust. 2 lit. a–d	
Rozporządzenie DORA	Artykuł 5	
COBIT 2019	APO12, MEA01	

1. Cel

1.1 Niniejsza polityka określa sposób, w jaki organizacja identyfikuje, ocenia i zarządza ryzykiem związanym z bezpieczeństwem informacji, działalnością operacyjną, technologią oraz usługami stron trzecich.

1.2 Zapewnia, że zarządzanie ryzykiem stanowi aktywny element planowania, realizacji projektów, wyboru dostawców oraz reagowania na incydenty, zgodnie z ISO 27001, ISO 31000 oraz wymaganiami regulacyjnymi.

1.3 Polityka wspiera podejmowanie świadomych decyzji, ochronę aktywów informacyjnych oraz odporność kluczowych operacji biznesowych.

2. Zakres

2.1 Niniejsza polityka ma zastosowanie do:

2.1.1 wszystkich działów, systemów i użytkowników w organizacji;

2.1.2 wszystkich informacji, usług i aktywów zarządzanych wewnętrznie lub za pośrednictwem stron trzecich;

2.1.3 działań związanych z ryzykiem, w tym przeglądów projektów, modernizacji systemów, outsourcingu oraz zgodności regulacyjnej.

2.2 Obejmuje wszystkie rodzaje ryzyka, w tym:

2.2.1 zagrożenia cyberbezpieczeństwa i podatności systemów;

2.2.2 zakłócenia operacyjne i niedostępność usług;

2.2.3 ryzyko prawne, regulacyjne lub reputacyjne;

2.2.4 ryzyko związane ze stronami trzecimi i łańcuchem dostaw.

2.3 Pracownicy, współpracownicy oraz dostawcy usług muszą stosować się do niniejszej polityki podczas identyfikowania lub zgłaszania ryzyka.

3. Cele

3.1 Zintegrować proste i powtarzalne procedury oceny ryzyka z bieżącą działalnością biznesową.

3.2 Identyfikować i priorytetyzować ryzyka, które mogą wpływać na poufność, integralność, dostępność (CIA) lub zgodność z prawem.

3.3 Przypisać właściciela oraz określić działania w ramach postępowania z ryzykiem dla wszystkich istotnych ryzyk.

3.4 Utrzymywać dokładny i aktualny rejestr ryzyka w celu zapewnienia gotowości do audytu oraz możliwości śledzenia ryzyka.

3.5 Zapewnić udział kierownictwa w zatwierdzaniu tolerancji ryzyka oraz głównych planów postępowania z ryzykiem.

4. Role i obowiązki

4.1 Dyrektor Generalny

4.1.1 Określa apetyt na ryzyko organizacji i zatwierdza ramy zarządzania ryzykiem.

4.1.2 Zatwierdza kluczowe decyzje dotyczące postępowania z ryzykiem oraz alokacji zasobów.

4.1.3 Dokonuje kwartalnego przeglądu najważniejszych ryzyk wraz z Koordynatorem ds. ryzyka.

4.2 Koordynator ds. ryzyka (lub właściciel SZBI)

4.2.1 Koordynuje oceny ryzyka i utrzymuje rejestr ryzyka.

4.2.2 Zapewnia udokumentowanie oceny ryzyka, przypisania właściciela oraz działań w ramach postępowania z ryzykiem.

4.2.3 Organizuje co najmniej jeden formalny przegląd ryzyka rocznie.

[... 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 polityki

9.1.1 Niniejsza polityka musi być przeglądana co najmniej raz w roku przez Dyrektora Generalnego oraz Koordynatora ds. ryzyka w celu zapewnienia jej adekwatności i kompletności.

9.2 Przesłanki aktualizacji

9.2.1 Wcześniejszy przegląd i aktualizacja muszą nastąpić, jeżeli:

9.2.1.1 istotny incydent lub ustalenie audytowe ujawni luki w zarządzaniu ryzykiem;

9.2.1.2 zostaną wprowadzone nowe jednostki biznesowe, technologie lub partnerstwa;

9.2.1.3 zmianie ulegnie wymaganie regulacyjne lub umowne.

9.3 Kontrola wersji

9.3.1 Wszystkie aktualizacje niniejszej polityki muszą podlegać kontroli wersji i zawierać następujące metadane:

9.3.1.1 numer wersji i datę wejścia w życie;

9.3.1.2 podsumowanie zmian;

9.3.1.3 osobę zatwierdzającą (Dyrektor Generalny);

9.3.1.4 zarchiwizowane poprzednie wersje do celów audytowych.

9.4 Komunikacja i świadomość

9.4.1 Zaktualizowane wersje polityki oraz główne plany postępowania z ryzykiem muszą zostać przekazane właściwym członkom personelu. Coroczne szkolenie przypominające musi obejmować podstawowe zasady świadomości ryzyka.

10. Powiązane polityki i zależności

10.1 Niniejsza polityka funkcjonuje w powiązaniu z innymi dokumentami, aby zapewnić kompleksowy ład bezpieczeństwa:

10.1.1 P2S – Polityka ról i odpowiedzialności w ramach ładu zarządczego: określa, kto odpowiada za własność ryzyka i podejmowanie decyzji.

10.1.2 P5S – P05 Polityka zarządzania zmianą: wymaga przeprowadzenia oceny ryzyka przed wdrożeniem zmian technicznych lub procesowych.

10.1.3 P17S – Polityka ochrony danych i prywatności: dotyczy ryzyka regulacyjnego związanego z przetwarzaniem danych osobowych.

10.1.4 P30S – Polityka reagowania na incydenty (P30): zapewnia ciągłość postępowania z ryzykiem w trakcie i po wystąpieniu incydentów bezpieczeństwa.

10.1.5 P33S – Polityka ciągłości działania: identyfikuje ryzyko rezydualne i środki odtworzeniowe dla usług krytycznych.

11. Normy odniesienia i ramy postępowania

11.1 ISO/IEC 27001:

11.1.1 Klauzula 6.1 – ustanawia formalny proces zarządzania ryzykiem oraz planowanie postępowania z ryzykiem.

11.1.2 Klauzula 6.1.3 – wymaga od organizacji utrzymywania udokumentowanych planów postępowania z ryzykiem oraz zatwierdzeń.

11.2 ISO/IEC 27002:

11.2.1 Środki kontrolne 5.4, 5.25 – zawierają wytyczne wdrożeniowe dotyczące własności ryzyka, priorytetyzacji oraz zarządzania w całym cyklu życia.

11.3 NIST SP 800-53 Rev. 5:

11.3.1 RA-1 do RA-7 – definiują ocenę ryzyka, strategie reagowania, dokumentowanie oraz mechanizmy przeglądu.

11.4 PM-9 – wymaga spójnego nadzoru nad ryzykiem organizacyjnym na poziomie kierownictwa.

11.5 Dyrektywa NIS2

11.5.1 Artykuł 21 ust. 2 lit. a–d – nakłada obowiązek stosowania ocen ryzyka, działań ograniczających ryzyko oraz zabezpieczeń z zakresu ładu zarządczego wobec podmiotów kluczowych i ważnych.

11.6 Rozporządzenie DORA

11.6.1 Artykuł 5 – wymaga od podmiotów regulowanych ustanowienia i utrzymywania ram zarządzania ryzykiem ICT, w tym identyfikacji, klasyfikacji i reagowania.

11.7 COBIT 2019

11.7.1 APO12 – Zarządzanie ryzykiem: integruje ryzyko z planowaniem strategicznym i operacyjnym.

11.7.2 MEA01 – Monitorowanie, ocena i analiza: zapewnia skuteczność i zgodność procesów oraz działań związanych z ryzykiem.