					Wprowadź tutaj nazwę zarejestrowanej osoby prawnej							
Numer dokumentu: P05					Tytuł dokumentu: **Polityka zarządzania zmianami**							
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

Dostosowanie do norm i regulacji

Standard/regulacja	Klauzula/artykuł	Komentarz
ISO/IEC 27001:2022	Klauzule 6.1, 5	Obejmuje działania związane z ryzykiem, kontrolą dostępu i zarządzaniem zmianami
ISO/IEC 27002:2022	Środek kontrolny 8	Wdraża ustrukturyzowany proces zarządzania zmianami
NIST SP 800-53 Rev.5	CM-2 do CM-14	Środki kontrolne zarządzania konfiguracją
RODO	Artykuły 32(1)(b–d), 25; motyw 78	Techniczne i organizacyjne środki bezpieczeństwa dla systemów i danych w trakcie zmian
Dyrektywa NIS2	Artykuł 21(2)(a, b, d, e)	Nakłada wymóg zarządzania ryzykiem zmian w obszarze ICT
Rozporządzenie DORA	Artykuły 5, 8, 12	Reguluje ryzyko operacyjne i ICT oraz zgłaszanie incydentów
COBIT 2019	BAI06, BAI02, BAI03, DSS01, MEA01, MEA03	Ustrukturyzowane zarządzanie zmianami IT w zakresie wydajności, zgodności i wymagań

1. Cel

1.1. Niniejsza polityka ustanawia formalne ramy inicjowania, oceny, zatwierdzania, wdrażania i przeglądu zmian w systemach informatycznych organizacji, infrastrukturze, aplikacjach i powiązanych procesach.

1.2. Zapewnia ona, że wszystkie zmiany są realizowane w sposób kontrolowany i zapewniający identyfikowalność audytową, przy jednoczesnym ograniczaniu ryzyka zakłóceń, naruszenia bezpieczeństwa lub braku zgodności regulacyjnej.

1.3. Wspiera ona wymagania normy ISO/IEC 27001:2022, Załącznik A, Środek kontrolny 8.32, poprzez egzekwowanie bezpiecznych, udokumentowanych i opartych na ryzyku praktyk zarządzania zmianami.

1.4. Polityka zapewnia również identyfikowalność decyzji dotyczących zmian oraz wspiera odporność operacyjną podczas planowanych zmian i zmian awaryjnych.

2. Zakres

2.1. Niniejsza polityka ma zastosowanie do wszystkich zmian wpływających na systemy, dane i środowiska objęte zakresem SZBI, w tym:

2.1.1. infrastrukturę IT (infrastrukturę lokalną, chmurę obliczeniową, środowiska hybrydowe)

2.1.2. środowiska produkcyjne, przedprodukcyjne oraz środowisko odtwarzania po awarii

2.1.3. aplikacje biznesowe, usługi, interfejsy API i integracje

2.1.4. ustawienia konfiguracyjne, wdrażanie poprawek, wydania oprogramowania i migracje systemów

2.1.5. poprawki awaryjne oraz zmiany projektowe lub planowane

2.2. Obejmuje ona zmiany inicjowane przez:

2.2.1. personel wewnętrzny (operacje IT, programistów, właścicieli systemów)

2.2.2. zewnętrznych dostawców, dostawców usług zarządzanych (MSP) oraz wykonawców

2.2.3. zespoły projektowe podczas wdrożeń systemów, aktualizacji lub przejść usługowych

2.3. Niniejsza polityka nie ma zastosowania do:

2.3.1. tymczasowych środowisk testowych i rozwojowych bez dostępu do danych produkcyjnych

2.3.2. osobistych konfiguracji użytkowników (objętych Polityką dopuszczalnego użytkowania)

2.3.3. zmian w systemach znajdujących się poza zakresem kontroli organizacji, o ile nie wpływają one na zintegrowane aktywa lub obowiązki w zakresie zgodności

3. Cele

3.1. Zapewnienie, że wszystkie zmiany przed realizacją podlegają przeglądowi, zatwierdzeniu, testowaniu i udokumentowaniu.

3.2. Utrzymanie dostępności systemów, integralności danych i ciągłości usług w trakcie i po realizacji zmian.

3.3. Wymaganie stosowania zdefiniowanej klasyfikacji zmian, planów wycofania oraz ocen ryzyka dla wszystkich typów zmian.

3.4. Umożliwienie przejrzystego podejmowania decyzji i eskalacji poprzez ustrukturyzowany ład organizacyjny.

3.5. Wspieranie gotowości do audytu poprzez identyfikowalne zapisy zmian i przeglądy po wdrożeniu.

3.6. Egzekwowanie rozdzielenia obowiązków oraz ograniczanie ryzyka nieuprawnionych lub kolidujących zmian w systemach krytycznych.

4. Role i odpowiedzialności

4.1. Kierownictwo wykonawcze

4.1.1. Zatwierdza P05 Politykę zarządzania zmianami i zapewnia jej zgodność z celami strategicznymi oraz obowiązkami regulacyjnymi.

4.1.2. Zatwierdza programy zmian o wysokim wpływie lub międzyfunkcyjne w ramach nadzoru w obszarze ładu organizacyjnego.

4.1.3. Przydziela niezbędne zasoby i budżet na narzędzia kontroli zmian oraz szkolenia personelu.

4.2. Komitet Doradczy ds. Zmian (CAB)

4.2.1. Dokonuje przeglądu i autoryzuje zmiany standardowe oraz zmiany istotne, zapewniając odpowiednią ocenę ryzyka, wpływu i zależności.

4.2.2. Waliduje plany wycofania zmian, wyniki testów, komunikację z interesariuszami oraz harmonogramowanie.

4.2.3. W jego skład wchodzą właściciele systemów, przedstawiciele bezpieczeństwa, operacji IT, biznesu oraz zgodności.

4.2.4. Może delegować decyzje dotyczące zmian niskiego ryzyka lub zmian awaryjnych na udokumentowanych zasadach.

[... 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. Czynniki uruchamiające przegląd i częstotliwość

9.1.1. Niniejsza polityka musi być poddawana przeglądowi co najmniej raz w roku lub w przypadku:

9.1.1.1. istotnych zmian w IT lub infrastrukturze

9.1.1.2. istotnych incydentów związanych z nieudanymi lub nieuprawnionymi zmianami

9.1.1.3. zmian regulacyjnych lub nowych obowiązków prawnych związanych ze zmianami

9.1.1.4. wdrożenia nowych narzędzi lub platform CMS

9.2. Proces przeglądu Polityki zarządzania zmianami

9.2.1. Menedżer zmian prowadzi proces przeglądu we współpracy z:

9.2.1.1. IT, bezpieczeństwem i operacjami

9.2.1.2. audytem wewnętrznym i zarządzaniem ryzykiem

9.2.1.3. przedstawicielami CAB

9.2.2. Aktualizacje muszą zostać poddane przeglądowi i zatwierdzone przez kierownictwo wykonawcze oraz Komitet Sterujący SZBI.

9.2.3. Ponownie wydane wersje muszą być rejestrowane w Rejestrze dokumentów i komunikowane stronom, których dotyczą, wraz z ponownym potwierdzeniem zapoznania się, jeżeli jest wymagane.

9.3. Nadzór nad dokumentem i wersjonowanie

9.3.1. Wszystkie wersje muszą zawierać:

9.3.1.1. identyfikator polityki, tytuł i poziom klasyfikacji

9.3.1.2. właściciela oraz historię zmian

9.3.1.3. rejestr zmian i datę wejścia w życie

9.3.1.4. organ zatwierdzający

9.3.2. Wersje archiwalne muszą być przechowywane zgodnie z Polityką retencji dokumentów (minimum 3 lata).

10. Powiązane polityki i zależności

10.1. Niniejsza polityka jest bezpośrednio powiązana z następującymi politykami i wspiera stosowanie ich postanowień:

10.1.1. P1 – Polityka bezpieczeństwa informacji: ustanawia wymóg formalnych środków bezpieczeństwa i rozliczalności na poziomie procesów, w tym ładu organizacyjnego w obszarze zarządzania zmianami.

10.1.2. P2 – Polityka ról i odpowiedzialności w ramach ładu organizacyjnego: określa uprawnienia do zatwierdzania i rozdzielenie obowiązków istotne dla autoryzacji zmian i nadzoru nad nimi.

10.1.3. P4 – Polityka kontroli dostępu: zapewnia, że uprawnienia dostępu dla osób wdrażających zmiany i osób dokonujących przeglądu są zgodne z zasadą najmniejszych uprawnień.

10.1.4. P6 – Polityka zarządzania ryzykiem: zapewnia, że wszystkie zmiany podlegają właściwej ocenie ryzyka i strategiom jego ograniczania.

10.1.5. P33 – Polityka monitorowania, audytu i zgodności: reguluje walidację i przegląd audytowy zapisów zarządzania zmianami oraz naruszeń.

10.2. Polityki te łącznie umożliwiają defensywny, identyfikowalny i bezpieczny cykl życia zarządzania zmianami w ramach SZBI.

11. Normy i ramy odniesienia

11.1. ISO/IEC 27001:2022

11.1.1. Klauzula 6.1 – Działania dotyczące ryzyk i szans: niniejsza polityka wspiera identyfikację, ocenę i kontrolę ryzyk związanych ze zmianami.

11.1.2. Klauzula 5.15 – Kontrola dostępu: zapewnia, że dostęp w trakcie zmian jest kontrolowany i identyfikowalny.

11.1.3. Załącznik A, Środek kontrolny 8.32 – Zarządzanie zmianami: niniejsza polityka w pełni wdraża wymóg zarządzania zmianami w obiektach przetwarzania informacji i systemach w sposób planowy i kontrolowany.

11.2. ISO/IEC 27002:2022 – Środek kontrolny 8

11.2.1. Wzmacnia wdrożenie ustrukturyzowanego procesu zarządzania zmianami obejmującego klasyfikację zmian, zatwierdzanie, testowanie, wycofanie zmian i dokumentację.

11.3. NIST SP 800-53 Rev.5

11.3.1. Rodzina CM (CM-1 do CM-14): niniejsza polityka jest ściśle zgodna ze środkami kontrolnymi zarządzania konfiguracją, w tym konfiguracjami bazowymi (CM-2), kontrolą zmian konfiguracji (CM-3), analizą wpływu na bezpieczeństwo (CM-4) i ograniczeniami dostępu (CM-5).

11.3.2. Rodzina AU (AU-2, AU-6, AU-12): mechanizmy rejestrowania i audytu wskazane w niniejszej polityce wspierają identyfikowalność zdarzeń i przegląd zgodności dla działań związanych ze zmianami.

11.3.3. RA-3, RA-5: oceny ryzyka wywołane zmianami i skany podatności są wbudowane w proces oceny zmian.

11.3.4. PM-11 (Definicja misji/procesu biznesowego): zapewnia zachowanie ciągłości działania i celów operacyjnych podczas zmian.

11.4. RODO (2016/679)

11.4.1. Artykuł 32(1)(b–d): niniejsza polityka wspiera wymóg stosowania odpowiednich środków technicznych i organizacyjnych w celu zapewnienia bezpieczeństwa danych, w szczególności podczas zmian w systemach.

11.4.2. Artykuł 25 – Ochrona danych w fazie projektowania i domyślna ochrona danych: zapewnia, że zmiany wpływające na dane osobowe uwzględniają prywatność i bezpieczeństwo na etapie projektowania oraz wdrożenia.

11.4.3. Motyw 78: wymaga, aby administratorzy danych wdrażali mechanizmy, takie jak polityki kontroli zmian, zapewniające stałą poufność, integralność i odporność systemów przetwarzania.

11.5. Dyrektywa NIS2 (2022/2555)

11.5.1. Artykuł 21(2)(a, b, d, e): nakłada wymóg stosowania technicznych i organizacyjnych środków do zarządzania ryzykami ICT, w tym ryzykami wynikającymi ze zmian systemowych, aktualizacji oprogramowania i modyfikacji infrastruktury.

11.6. Rozporządzenie DORA (2022/2554)

11.6.1. Artykuł 5 – Ramy ładu organizacyjnego i kontroli wewnętrznej: niniejsza polityka egzekwuje zasady zarządzania ryzykiem operacyjnym związanym ze zmianami i aktualizacjami ICT.

11.6.2. Artykuł 8 – Ramy zarządzania ryzykiem ICT: nakłada wymóg, aby podmioty finansowe zarządzały wszystkimi zmianami wpływającymi na systemy ICT w ramach ustrukturyzowanych procesów zarządzania zmianami, co znajduje odzwierciedlenie w wymaganiach niniejszej polityki dotyczących klasyfikacji, testowania, wycofania zmian i dokumentacji.

11.6.3. Artykuł 12 – Zgłaszanie incydentów: zapewnia, że nieudane zmiany prowadzące do zakłóceń ICT są identyfikowalne, udokumentowane i zgłaszane tam, gdzie ma to zastosowanie.

11.7. COBIT 2019

11.7.1. BAI06 – Managed IT Changes: niniejsza polityka bezpośrednio realizuje cele BAI06 poprzez ustanowienie ustrukturyzowanych ścieżek pracy dla zatwierdzania zmian, oceny wpływu, komunikacji i testowania.

11.7.2. BAI02 – Managed Requirements Definition oraz BAI03 – Managed Solutions Identification and Build: zapewniają, że zmiany wynikające z potrzeb biznesowych są poddawane przeglądowi i wdrażane w sposób bezpieczny.

11.7.3. DSS01 – Managed Operations: wspiera zachowanie integralności systemów podczas realizacji zmian.

11.7.4. MEA01 oraz MEA03 – Monitor, Evaluate, and Assess Performance and Compliance: umożliwiają ciągły nadzór nad skutecznością i stosowaniem Polityki zarządzania zmianami.