					Wprowadź tutaj nazwę zarejestrowanej osoby prawnej							
Numer dokumentu: P05S					Tytuł dokumentu: **Polityka zarządzania zmianą**							
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, tam gdzie ma to zastosowanie

Norma/regulacja	Klauzula/artykuł	Komentarz
ISO/IEC 27001:2022	Klauzula 6.1, 8	
ISO/IEC 27002:2022	Środek kontrolny 8	
NIST SP 800-53 Rev. 5	CM-2 do CM-5, CM-11	
Dyrektywa NIS2	Artykuł 21(2)(b)	
Rozporządzenie DORA	Artykuły 6(9), 8(4)(b)	
COBIT 2019	BAI06, DSS01	

1. Cel

1.1 Niniejsza polityka zapewnia, że wszystkie zmiany w systemach IT, konfiguracjach, aplikacjach biznesowych i usługach chmurowych są planowane, poddawane ocenie ryzyka, testowane i zatwierdzane przed wdrożeniem.

1.2 Celem polityki jest ograniczenie zakłóceń operacyjnych, ryzyk bezpieczeństwa oraz niedostępności usług poprzez ustanowienie uproszczonego, ale egzekwowalnego procesu, który ma zastosowanie również w małych przedsiębiorstwach o ograniczonych zasobach.

1.3 Niniejsza polityka wspiera certyfikację ISO/IEC 27001:2022 poprzez sformalizowanie sposobu zarządzania i dokumentowania zmian technicznych oraz operacyjnych.

2. Zakres

2.1 Niniejsza polityka ma zastosowanie do:

2.1.1 pracowników i kierowników działów zgłaszających lub realizujących zmiany

2.1.2 zewnętrznych dostawców usług IT zarządzających systemami lub oprogramowaniem

2.1.3 Dyrektora Generalnego, który ponosi ogólną odpowiedzialność za zatwierdzanie zmian

2.2 Polityka obejmuje zmiany dotyczące:

2.2.1 oprogramowania (aktualizacje, poprawki, nowe aplikacje)

2.2.2 sprzętu (wymiany, modernizacje)

2.2.3 konfiguracji sieci i reguł zapory sieciowej

2.2.4 usług chmurowych, uprawnień dostępu użytkowników oraz integracji z dostawcami

2.2.5 zmian w krytycznych procesach biznesowych obejmujących systemy informatyczne

2.3 Zakres niniejszej polityki obejmuje zarówno zmiany planowane, jak i zmiany awaryjne.

3. Cele

3.1 Zapewnienie, że wszystkie zmiany w systemach IT i systemach biznesowych są autoryzowane, dokumentowane oraz odwracalne w przypadku wystąpienia problemów.

3.2 Zapobieganie nieplanowanym przestojom, utracie danych i incydentom bezpieczeństwa spowodowanym niekontrolowanymi zmianami.

3.3 Określenie prostych i powtarzalnych procedur zgłaszania, zatwierdzania, testowania i wycofywania zmian.

3.4 Utrzymanie dziennika zmian zapewniającego ścieżkę audytu oraz wspierającego rozliczalność operacyjną i zgodność z wymaganiami regulacyjnymi.

3.5 Umożliwienie podejmowania decyzji w oparciu o ryzyko w odniesieniu do zmian istotnych lub wrażliwych.

4. Role i odpowiedzialności

4.1 Dyrektor Generalny

4.1.1 Posiada ostateczną odpowiedzialność za wszystkie istotne zmiany.

4.1.2 Dokonuje przeglądu i zatwierdza zmiany niestandardowe, krytyczne lub wysokiego ryzyka.

4.1.3 Dokonuje kwartalnego przeglądu dziennika zmian lub przeglądu po istotnych incydentach.

4.2 IT lub zewnętrzny dostawca usług IT

4.2.1 Wdraża zmiany, w tym aktualizacje konfiguracji, wdrażanie poprawek i migracje systemów.

4.2.2 Prowadzi podstawowy dziennik zmian zawierający daty, rodzaje zmian, wyniki oraz osoby zatwierdzające.

4.2.3 Testuje zmiany przed wdrożeniem i w razie potrzeby stosuje procedury wycofania.

4.2.4 Informuje użytkowników, których dotyczą zmiany, przed wdrożeniem istotnych zmian i po ich wdrożeniu.

[... 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

9.1.1 Niniejsza polityka musi być poddawana corocznemu przeglądowi przez Dyrektora Generalnego lub wyznaczoną osobę kontaktową IT w celu zapewnienia zgodności z aktualnymi systemami, sposobem pracy i wymaganiami regulacyjnymi.

9.2 Przeglądy doraźne

9.2.1 Przegląd musi zostać również uruchomiony w przypadku:

9.2.1.1 incydentów bezpieczeństwa spowodowanych niewłaściwą obsługą zmian

9.2.1.2 wdrożenia nowych systemów IT

9.2.1.3 zmian w odpowiednich normach, takich jak ISO, NIS2 lub DORA

9.3 Dokumentowanie aktualizacji

9.3.1 Zmiany w niniejszej polityce muszą podlegać kontroli wersji i być zatwierdzane przez Dyrektora Generalnego. Każda wersja musi zawierać datę, podsumowanie zmian oraz osobę zatwierdzającą.

9.4 Komunikowanie polityki

9.4.1 Wszelkie aktualizacje muszą być komunikowane wszystkim pracownikom i zewnętrznym dostawcom, których dotyczą. Dokumentacja musi zostać zaktualizowana we wszystkich miejscach odniesienia (np. portal pracowniczy, dyski współdzielone).

10. Powiązane polityki i zależności

10.1 Niniejsza polityka jest ściśle powiązana z następującymi politykami SME:

10.1.1 P2S – Polityka ról i odpowiedzialności w zakresie nadzoru: określa uprawnienia do zatwierdzania zmian.

10.1.2 P4S – Polityka kontroli dostępu: zapewnia, że modyfikacje uprawnień dostępowych wynikające ze zmian są dokumentowane i wdrażane prawidłowo.

10.1.3 P7S – Polityka wdrażania i zakończenia współpracy: koordynuje zmiany związane ze zmianą roli oraz nadawaniem dostępu.

10.1.4 P15S – Polityka tworzenia kopii zapasowych i odtwarzania: zapewnia możliwość wykonania działań wycofania i odtworzenia, jeśli zmiana zakończy się niepowodzeniem.

10.1.5 P30S – Polityka reagowania na incydenty: określa sposób traktowania nieudanych lub nieautoryzowanych zmian jako incydentów bezpieczeństwa.

11. Normy i ramy odniesienia

11.1 ISO/IEC 27001

11.1.1 Klauzula 6.1 – planowanie oparte na ryzyku musi obejmować działania związane ze zmianami.

11.1.2 Klauzula 8.1 – środki kontrolne operacyjne muszą być stosowane w sposób spójny do działań związanych ze zmianami, aby zapewnić integralność usług.

11.2 ISO/IEC 27002

11.2.1 Środek kontrolny 8.32 – zawiera wytyczne dotyczące bezpiecznych procesów zarządzania zmianą, w tym dokumentowania, testowania i zatwierdzania.

11.3 NIST SP 800-53 Rev. 5

11.3.1 CM-2 – konfiguracja bazowa systemów przed zmianą.

11.3.2 CM-3 – kontrola zmian konfiguracji.

11.3.3 CM-4 – analiza wpływu na bezpieczeństwo.

11.3.4 CM-5 – zatwierdzanie i dokumentowanie zmian.

11.3.5 CM-11 – audyt i monitorowanie zmian.

11.4 Dyrektywa NIS2

11.4.1 Artykuł 21(2)(b) – wymaga formalnych procedur dla technicznych i organizacyjnych środków bezpieczeństwa, w tym zarządzania zmianą.

11.5 Rozporządzenie DORA

11.5.1 Artykuły 6(9) i 8(4)(b) – wymagają od podmiotów finansowych utrzymywania zarządzania zmianą i konfiguracją dla systemów ICT.

11.6 COBIT 2019

11.6.1 BAI06 – Zarządzanie zmianami: podkreśla znaczenie planowania, oceny ryzyka i zdolności do wycofania zmian.

11.6.2 DSS01 – Zarządzanie operacjami: zapewnia integralność operacyjną podczas zmian technicznych i przejść między stanami operacyjnymi.