					Wprowadź tutaj nazwę zarejestrowanej osoby prawnej							
Numer dokumentu: P32					Tytuł dokumentu: **Polityka ciągłości działania i odtwarzania po awarii**							
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	
ISO/IEC 27002:2022	Środki kontrolne 5.29, 5.30	
NIST SP 800-53 Rev.5	CP-1 do CP-11	
NIST SP 800-34 Rev.1	Planowanie awaryjne	Ramy
ISO 22301:2019		Wymagania dotyczące systemu zarządzania ciągłością działania
RODO	Artykuł 32	
Dyrektywa NIS2	Artykuł 21(2)(f)	
Rozporządzenie DORA	Artykuł 10	
COBIT 2019	DSS	

1. Cel

1.1. Niniejsza polityka określa obowiązkowe środki kontrolne i odpowiedzialności zapewniające organizacji zdolność do utrzymania lub odtworzenia krytycznych operacji biznesowych oraz wspierających je usług ICT w trakcie i po wystąpieniu incydentu zakłócającego działalność.

1.2. Jej celem jest ochrona życia, stabilności operacyjnej, zgodności z wymaganiami prawnymi, zobowiązań wobec klientów oraz reputacji organizacji poprzez uwzględnienie odporności w proaktywnym planowaniu i zwalidowanych zdolnościach odtworzeniowych.

1.3. Niniejsza polityka stanowi podstawę ram zarządzania ciągłością działania (BCM) i odtwarzaniem po awarii (DR) w organizacji, zapewniając zgodność z mającymi zastosowanie wymaganiami regulacyjnymi, umownymi i branżowymi.

2. Zakres

2.1. Niniejsza polityka ma zastosowanie do wszystkich jednostek organizacyjnych, systemów informatycznych, procesów biznesowych, personelu oraz usług stron trzecich sklasyfikowanych jako krytyczne lub niezbędne na podstawie wyników analizy wpływu na działalność biznesową (BIA).

2.2. Polityka obejmuje:

2.2.1. zakłócenia naturalne i spowodowane przez człowieka, w tym cyberataki, awarie infrastruktury, niedostępność centrów danych, pandemie oraz przerwy w świadczeniu usług przez dostawcę

2.2.2. planowanie, testowanie i ciągłe doskonalenie planów ciągłości działania (BCP) oraz planów odtwarzania po awarii (DRP)

2.2.3. role i odpowiedzialności w zakresie reagowania awaryjnego, koordynacji odtwarzania oraz eskalacji incydentów

2.3. Wszystkie osoby odpowiedzialne za ciągłość działania lub odtwarzanie, w tym IT, właściciele biznesowi, menedżerowie kryzysowi i dostawcy, podlegają postanowieniom niniejszej polityki.

3. Cele

3.1. Zapewnienie ciągłości operacji biznesowych i usług poprzez zdefiniowane i przetestowane procedury, przy jednoczesnej minimalizacji wpływu operacyjnego, reputacyjnego i prawnego.

3.2. Odtwarzanie usług ICT w ramach określonych docelowych czasów odtworzenia (RTO) oraz docelowych punktów odtworzenia (RPO), zgodnie z poziomami tolerancji ryzyka biznesowego.

3.3. Przypisanie właścicielstwa planowania, realizacji i nadzoru nad ciągłością działania oraz odtwarzaniem po awarii w całej organizacji.

3.4. Zapewnienie regularnego testowania, utrzymywania i doskonalenia zdolności w zakresie ciągłości działania na podstawie realistycznych scenariuszy oraz ustaleń audytowych.

3.5. Spełnienie wymagań zgodności wynikających z norm ISO, NIST, RODO, DORA i NIS2, przy wspieraniu należytej staranności w zakresie odporności operacyjnej i dostępności.

4. Role i odpowiedzialności

4.1. Kierownictwo wykonawcze

4.1.1. Zatwierdza Politykę ciągłości działania i odtwarzania po awarii oraz zapewnia jej zgodność ze strategicznymi kierunkami organizacji.

4.1.2. Przydziela budżet i zasoby wspierające ciągłość działania, reagowanie awaryjne oraz ćwiczenia odtworzeniowe.

4.2. Kierownik ds. ciągłości działania (BCM Lead)

4.2.1. Odpowiada za opracowanie i utrzymanie planów ciągłości działania (BCP) dla całej organizacji oraz koordynację testów ciągłości działania.

4.2.2. Utrzymuje harmonogram analizy wpływu na działalność biznesową (BIA), wspiera realizację szkoleń oraz zapewnia, że dokumentacja spełnia wymagania zgodności.

[... 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 corocznemu przeglądowi przez Kierownika ds. ciągłości działania oraz Dyrektora ds. bezpieczeństwa informacji (CISO), aby zapewnić zgodność z:

9.1.1. zmianami w operacjach biznesowych, systemach krytycznych lub infrastrukturze

9.1.2. wnioskami z incydentów, audytów, ćwiczeń typu tabletop lub testów DR

9.1.3. zaktualizowanymi obowiązkami regulacyjnymi lub umownymi (np. DORA, RODO, wymaganiami klientów dotyczącymi RTO/RPO)

9.1.4. zmianami apetytu na ryzyko organizacji lub strategii ciągłości działania

9.2. Przeglądy muszą obejmować:

9.2.1. walidację aktualności planów i danych kontaktowych

9.2.2. ponowną ocenę RTO, RPO oraz poziomów odtwarzania

9.2.3. ocenę zdolności usług kopii zapasowych i DR

9.2.4. informacje zwrotne od interesariuszy, którzy realizowali ostatnie plany odtworzeniowe lub testy

9.3. Wszystkie zmiany polityki muszą być:

9.3.1. objęte kontrolą wersji wraz z udokumentowanym uzasadnieniem i akceptacją interesariuszy

9.3.2. zakomunikowane kluczowemu personelowi i zespołom z uwzględnieniem zaktualizowanych odpowiedzialności

9.3.3. odzwierciedlone w zaktualizowanych szkoleniach, materiałach uświadamiających i procedurach operacyjnych

9.4. Tymczasowe aktualizacje awaryjne muszą zostać wydane, jeżeli wystąpi istotna zmiana organizacyjna, wymóg prawny lub krytyczne ustalenie powodujące, że aktualne plany lub polityka stają się niewykonalne.

10. Powiązane polityki i zależności

10.1. Niniejsza polityka jest stosowana łącznie z następującymi kluczowymi dokumentami:

10.1.1. P1 – Polityka bezpieczeństwa informacji: ustanawia wymóg prowadzenia odpornych operacji opartych na ryzyku w każdych warunkach.

10.1.2. P5 – Polityka zarządzania zmianą: zapewnia, że wszelkie zmiany konfiguracji lub infrastruktury związane z odtwarzaniem przebiegają zgodnie z udokumentowanymi i zatwierdzonymi ścieżkami.

10.1.3. P14 – Polityka retencji i utylizacji danych: reguluje cykl życia nośników kopii zapasowych oraz odtworzonych danych wykorzystywanych w działaniach ciągłościowych.

10.1.4. P15 – Polityka tworzenia kopii zapasowych i odtwarzania: wymusza środki kontrolne dotyczące częstotliwości tworzenia kopii zapasowych, bezpieczeństwa i weryfikacji odtworzenia.

10.1.5. P18 – Polityka zabezpieczeń kryptograficznych: zapewnia, że procesy odtwarzania spełniają standardy szyfrowania i poufności.

10.1.6. P22 – Polityka logowania i monitorowania: wspiera wykrywanie i eskalację zdarzeń wpływających na ciągłość działania.

10.1.7. P30 – Polityka reagowania na incydenty: określa procesy powstrzymania, eskalacji i analizy przyczyny źródłowej zgodne z wyzwalaczami ciągłości działania.

10.1.8. P33 – Polityka monitorowania audytu i zgodności: weryfikuje integralność i skuteczność praktyk ciągłości działania i odtwarzania w systemach i procesach.

11. Normy i ramy odniesienia

11.1. Niniejsza polityka jest zgodna z międzynarodowo uznanymi normami dotyczącymi ciągłości działania i odtwarzania po awarii, wspierając możliwość prześledzenia audytowego, odporność i zgodność z prawem.

11.2. ISO/IEC 27002

11.2.1. Załącznik A, środek kontrolny 5.29 – Bezpieczeństwo informacji podczas zakłóceń: wymaga utrzymania środków kontrolnych bezpieczeństwa w warunkach zakłóceń.

11.2.2. Załącznik A, środek kontrolny 5.30 – Gotowość ICT na potrzeby ciągłości działania: wymaga przygotowania, testowania i walidacji zdolności odtworzeniowych ICT.

11.3. ISO 22301:2019 – Systemy zarządzania ciągłością działania

11.3.1. Zapewnia ramy ustanawiania, wdrożenia i utrzymania praktyk BCM zgodnych z celami organizacji i progami ryzyka.

11.4. NIST SP 800-34 Rev.1 – Przewodnik planowania awaryjnego

11.4.1. Określa dobre praktyki dla planów awaryjnych systemów IT, w tym opracowanie strategii ciągłości działania, analizę wpływu oraz testowanie planów.

11.5. RODO (2016/679)

11.5.1. Artykuł 32 – Bezpieczeństwo przetwarzania: wymaga odporności systemów i usług przetwarzania oraz terminowego odtworzenia dostępności i dostępu do danych osobowych po incydencie.

11.6. Dyrektywa UE NIS2 (2022/2555)

11.6.1. Artykuł 21(2)(f): wymaga środków dotyczących ciągłości działania i zarządzania kryzysowego wspierających bezpieczeństwo sieci i systemów informacyjnych.

11.7. Rozporządzenie DORA (2022/2554)

11.7.1. Artykuł 10 – Ciągłość działania ICT: wymaga od podmiotów finansowych opracowania i testowania planów ciągłości działania ICT, w tym opartych na ryzyku parametrów RTO/RPO oraz zdolności przełączenia awaryjnego.

11.8. COBIT 2019

11.8.1. DSS04 – Zarządzanie ciągłością działania: obejmuje wszystkie aspekty planowania ciągłości działania, w tym identyfikację zagrożeń, analizę wpływu, strategię odtworzeniową i regularne testowanie.