					Wprowadź tutaj nazwę zarejestrowanej osoby prawnej							
Numer dokumentu: P32S					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	Klauzule 6.1, 6.3, 8	
ISO/IEC 27002:2022	Środki kontrolne 5.29, 5.30	
NIST SP 800-53 Rev.5	CP-2, CP-4, CP-6, CP-7	
RODO	Artykuły 32, 33	
Dyrektywa NIS2	Artykuł 21(2)(f)	
Rozporządzenie DORA	Artykuł 10	
COBIT 2019	DSS04	

1. Cel

1.1 Niniejsza polityka zapewnia, że organizacja może utrzymać ciągłość operacyjną oraz odtworzyć kluczowe usługi IT w trakcie i po wystąpieniu zdarzeń zakłócających, takich jak przerwy w zasilaniu, cyberataki, ataki ransomware lub awarie systemów.

1.2 Określa ona przejrzyste ramy planowania ciągłości działania i odtwarzania po awarii (BC/DR), dostosowane do potrzeb MŚP bez wydzielonych zespołów IT.

1.3 Polityka wspiera organizację w spełnianiu obowiązkowych wymagań wynikających z ISO/IEC 27001:2022, RODO, NIS2, DORA oraz COBIT 2019, a jednocześnie wzmacnia odporność operacyjną i zaufanie klientów.

2. Zakres

2.1 Niniejsza polityka ma zastosowanie do:

2.1.1 wszystkich systemów i usług krytycznych dla działalności biznesowej (np. poczty elektronicznej, pamięci masowej w chmurze, platform fakturowania, rejestrów klientów)

2.1.2 wszystkich pracowników oraz zewnętrznych dostawców usług IT odpowiedzialnych za gotowość BC/DR i realizację działań w tym zakresie

2.1.3 wszystkich rodzajów zakłóceń, w tym incydentów cyberbezpieczeństwa, awarii sprzętu, utraty zasilania, zalania oraz braku dostępu do biura

2.2 Polityka obejmuje:

2.2.1 zarządzanie kopiami zapasowymi

2.2.2 planowanie ciągłości działania (BCP)

2.2.3 działania związane z odtwarzaniem po awarii

2.2.4 szkolenia personelu i testowanie

2.2.5 procedury reagowania prawnego i regulacyjnego

3. Cele

3.1 Ochronę zdolności organizacji do świadczenia kluczowych usług mimo nieplanowanych zakłóceń.

3.2 Zapewnienie terminowego odtworzenia systemów i danych przy użyciu zdefiniowanych celów czasu odtworzenia (RTO).

3.3 Umożliwienie całemu personelowi stosowania procedur ciągłości działania w sytuacjach kryzysowych przy minimalnym ryzyku nieporozumień.

3.4 Utrzymanie zgodności z przepisami dotyczącymi ochrony danych i odporności operacyjnej, w tym z art. 32 RODO i art. 21 NIS2.

3.5 Ustanowienie praktycznej i testowalnej strategii ciągłości działania i odtwarzania, odpowiedniej dla MŚP.

4. Role i odpowiedzialności

4.1 Dyrektor Generalny (GM)

4.1.1 Odpowiada za proces BC/DR oraz za niniejszą politykę.

4.1.2 Zatwierdza plan ciągłości działania (BCP).

4.1.3 Koordynuje reagowanie na incydenty oraz komunikację wewnętrzną podczas zakłóceń.

4.1.4 Dokonuje wymaganych zgłoszeń regulacyjnych (np. zgłoszeń naruszeń na podstawie RODO).

4.2 Dostawca usług IT / Administrator systemów

4.2.1 Utrzymuje i testuje kopie zapasowe.

4.2.2 Realizuje procedury odtwarzania po awarii po ich uruchomieniu.

4.2.3 Dokumentuje wszystkie działania odtworzeniowe oraz zdarzenia związane z przywracaniem systemów.

4.2.4 Niezwłocznie zgłasza krytyczne incydenty IT do GM.

[... 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 i planu

9.1.1 Dyrektor Generalny (GM) musi zapewnić formalny przegląd niniejszej polityki oraz powiązanego z nią planu ciągłości działania (BCP) co najmniej raz w roku.

9.1.2 Przegląd musi obejmować:

9.1.2.1 ocenę nowych lub pojawiających się ryzyk

9.1.2.2 ponowną walidację RTO/RPO

9.1.2.3 weryfikację informacji o dostawcach i danych kontaktowych

9.1.2.4 dostosowanie do zmian w systemach IT, obowiązkach prawnych lub działalności operacyjnej

9.2 Aktualizacje uruchamiane zdarzeniem

9.2.1 Niniejsza polityka musi być również aktualizowana w odpowiedzi na:

9.2.1.1 poważne incydenty lub zakłócenia, w szczególności jeżeli cele nie zostały osiągnięte

9.2.1.2 nowe obowiązki prawne lub regulacyjne (np. zmiany w DORA)

9.2.1.3 zmiany w systemach krytycznych, platformach chmurowych lub personelu

9.2.1.4 ustalenia wynikające z corocznych testów BCP/DR

9.3 Proces kontroli zmian

9.3.1 Wszystkie zmiany muszą być zatwierdzane przez GM.

9.3.2 Należy prowadzić rejestr historii wersji, obejmujący datę, opis zmiany oraz osobę zatwierdzającą.

9.3.3 Zaktualizowana polityka musi zostać ponownie przekazana całemu właściwemu personelowi, w tym dostawcy usług IT oraz kierownikom działów.

9.4 Dokumentowanie wniosków

9.4.1 Po testach lub rzeczywistych zakłóceniach udokumentowane wnioski muszą być wykorzystywane przy kolejnych aktualizacjach.

9.4.2 Przeglądy te muszą również obejmować oceny wyników dostawców oraz sprawdzenie adekwatności reakcji.

10. Powiązane polityki i zależności

10.1 Niniejsza polityka jest ściśle powiązana z następującymi politykami SME:

10.1.1 P1S – P01 Polityka bezpieczeństwa informacji: określa nadrzędne cele bezpieczeństwa, które muszą wspierać praktyki ciągłości działania i odtwarzania.

10.1.2 P4S – Polityka kontroli dostępu: umożliwia awaryjne cofnięcie dostępu lub przywrócenie dostępu użytkowników w scenariuszach zakłócenia działalności.

10.1.3 P6S – Polityka zarządzania ryzykiem: stanowi podstawę identyfikacji, oceny i priorytetyzacji ryzyk związanych z ciągłością działania.

10.1.4 P8S – Polityka świadomości i szkoleń w zakresie bezpieczeństwa informacji: zapewnia przygotowanie pracowników do działania podczas zakłóceń i zrozumienie BCP.

10.1.5 P15S – Polityka tworzenia kopii zapasowych i odtwarzania: określa szczegółowe procedury techniczne służące ochronie dostępności danych i ich odzyskiwaniu.

10.1.6 P17S – Polityka ochrony danych i prywatności: zapewnia, że planowanie ciągłości działania uwzględnia ochronę danych osobowych i pozostaje zgodne z RODO w trakcie i po incydentach.

10.1.7 P22S – Polityka logowania i monitorowania: wspiera wykrywanie zdarzeń mogących uruchomić procesy BC/DR oraz zapewnia ślady audytowe po zakłóceniu.

10.1.8 P30S – Polityka reagowania na incydenty: bezpośrednio poprzedza uruchomienie procesu odtwarzania w przypadku incydentów cyberbezpieczeństwa lub incydentów operacyjnych.

10.1.9 P31S – Polityka gromadzenia materiału dowodowego i kryminalistyki cyfrowej: zapewnia zabezpieczenie dowodów cyfrowych podczas scenariuszy ciągłości działania na potrzeby zgodności, ubezpieczenia lub dochodzenia.

10.2 Polityki te tworzą spójne, zapewniające gotowość do audytu ramy odporności, rozliczalności i ciągłości kontroli we wszystkich działaniach SME.

11. Normy i ramy odniesienia

11.1 ISO/IEC 27001:

11.1.1 Klauzula 6.1 – wymaga planowania i postępowania opartego na ryzyku, w tym w zakresie ciągłości działania i odtwarzania.

11.1.2 Klauzula 6.3 – podkreśla potrzebę ciągłego doskonalenia po wystąpieniu zakłóceń.

11.1.3 Klauzula 8.1 – nakłada obowiązek stosowania środków kontroli operacyjnej, w tym udokumentowanych środków ciągłości działania.

11.2 ISO/IEC 27002:

11.2.1 Środek kontrolny 5.29 – wymaga ustanowienia i utrzymywania rozwiązań w zakresie ciągłości działania.

11.2.2 Środek kontrolny 5.30 – wymaga testowania i przeglądu tych rozwiązań.

11.3 NIST SP 800-53 Rev.5:

11.3.1 CP-2 – definiuje wymagania dotyczące planowania awaryjnego.

11.3.2 CP-4 – nakłada obowiązek szkoleń z zakresu planowania awaryjnego dla personelu organizacji.

11.3.3 CP-6 – obejmuje wymagania dotyczące alternatywnej lokalizacji przechowywania.

11.3.4 CP-7 – określa wymagania dotyczące alternatywnej lokalizacji przetwarzania.

11.4 RODO:

11.4.1 Artykuł 32 – wymaga stosowania środków zapewniających ciągłą dostępność i odporność systemów oraz usług przetwarzania.

11.4.2 Artykuł 33 – uruchamia obowiązki zgłoszenia naruszenia w przypadkach, gdy nieskuteczność ciągłości działania prowadzi do naruszenia ochrony danych osobowych.

11.5 Dyrektywa UE NIS2 (2022/2555):

11.5.1 Artykuł 21(2)(f) – wymaga planowania ciągłości działania i zdolności zarządzania kryzysowego jako warunku gotowości na ryzyko cybernetyczne.

11.6 Rozporządzenie UE DORA (2022/2554):

11.6.1 Artykuł 10 – nakłada obowiązek wdrożenia testowania cyfrowej odporności operacyjnej oraz zdolności odtworzeniowych, w szczególności dla MŚP z sektora finansowego.

11.7 COBIT 2019:

11.7.1 DSS04 – Zarządzanie ciągłością: zawiera wytyczne w zakresie ładu korporacyjnego dla utrzymywania i walidacji odporności operacyjnej, w tym w zakresie odpowiedzialności, testowania, integracji dostawców i przeglądów po zdarzeniu.