					Wprowadź tutaj nazwę zarejestrowanej osoby prawnej							
Numer dokumentu: P15S					Tytuł dokumentu: **Polityka tworzenia kopii zapasowych i odtwarzania**							
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	Zabezpieczenia dotyczące tworzenia kopii zapasowych zgodne z wymaganiami SZBI
ISO/IEC 27002:2022	Środki bezpieczeństwa 5.29, 8	Dobre praktyki w zakresie tworzenia kopii zapasowych oraz integracja z planami ciągłości działania
NIST SP 800-53 Rev.5	CP-9, MP-6	Tworzenie kopii zapasowych oraz ochrona nośników
Dyrektywa NIS2 UE	Artykuł 21(2)(c)	Odporność i ciągłość działania zapewniane przez kopie zapasowe
Rozporządzenie DORA UE	Artykuł 10(1)	Ciągłość ICT – kopie zapasowe dla organizacji finansowych
COBIT 2019	BAI04.05, DSS04	Dokumentowanie i testowanie kopii zapasowych oraz procesy kontrolne
RODO	Artykuły 5(1)(f), 32(1)(c)	Integralność, dostępność oraz terminowe odtworzenie danych

1. Cel

1.1 Niniejsza polityka określa sposób realizacji i zarządzania procesem tworzenia kopii zapasowych w organizacji w celu zapewnienia ciągłości działania, ochrony przed utratą danych oraz umożliwienia terminowego odtworzenia po incydentach.

1.2 Ustanawia wiążące zasady dotyczące tworzenia, przechowywania i odtwarzania kopii zapasowych systemów i danych, w szczególności w MŚP bez złożonej infrastruktury IT.

1.3 Niniejsza polityka wspiera gotowość audytową oraz certyfikację ISO/IEC 27001 poprzez zapewnienie, że niezbędne zabezpieczenia dotyczące tworzenia kopii zapasowych są wdrożone, stosowane spójnie i regularnie przeglądane.

1.4 Zdolność organizacji do odtworzenia działania po awariach technicznych, przypadkowym usunięciu danych lub incydentach cyberbezpieczeństwa zależy od ścisłego przestrzegania niniejszej polityki.

2. Zakres

2.1 Niniejsza polityka ma zastosowanie do wszystkich systemów biznesowych i danych, w tym:

2.1.1 dokumentacji finansowej, informacji o klientach oraz danych kadrowych

2.1.2 komputerów stacjonarnych, laptopów, serwerów oraz aplikacji chmurowych wykorzystywanych w działalności operacyjnej

2.1.3 nośników kopii zapasowych, takich jak dyski USB, nośniki zewnętrzne lub kopie zapasowe w chmurze

2.2 Ma ona również zastosowanie do wszystkich osób odpowiedzialnych za realizację lub zarządzanie procesami tworzenia kopii zapasowych, w tym:

2.2.1 Dyrektora Generalnego (GM) lub wyznaczonej osoby odpowiedzialnej

2.2.2 zewnętrznych dostawców wsparcia IT lub konsultantów

2.2.3 wszystkich pracowników odpowiedzialnych za zapisywanie danych w zatwierdzonych lokalizacjach

3. Cele

3.1 Zapewnienie, że wszystkie krytyczne dane biznesowe i systemy są bezpiecznie objęte kopiami zapasowymi w odpowiednich odstępach czasu, zależnie od ryzyka i potrzeb operacyjnych.

3.2 Zapewnienie, że dane mogą zostać odtworzone terminowo i w sposób kompletny po zakłóceniach.

3.3 Zapobieganie nieuprawnionemu dostępowi, manipulacji lub utracie danych z kopii zapasowych poprzez skuteczne zabezpieczenia przechowywania.

3.4 Jednoznaczne przypisanie oraz egzekwowanie ról i odpowiedzialności za wdrażanie i testowanie procedur tworzenia kopii zapasowych.

3.5 Wspieranie zgodności z ISO/IEC 27001, RODO oraz innymi obowiązkami regulacyjnymi poprzez uporządkowane i udokumentowane praktyki tworzenia kopii zapasowych.

4. Role i odpowiedzialności

4.1 Dyrektor Generalny (GM)

4.1.1 Zatwierdza niniejszą politykę i zapewnia jej stosowanie.

4.1.2 Przydziela zasoby i wyznacza odpowiedzialność za działania związane z tworzeniem kopii zapasowych i odtwarzaniem.

4.1.3 Dokonuje przeglądu niepowodzeń wykonywania kopii zapasowych, incydentów lub odstępstw od polityki.

4.1.4 Prowadzi coroczne przeglądy polityki i zapewnia gotowość audytową.

4.2 Dostawca wsparcia IT (jeżeli dotyczy)

4.2.1 Wdraża i zarządza rozwiązaniami do tworzenia kopii zapasowych (lokalnymi lub chmurowymi).

4.2.2 Monitoruje prawidłowość wykonywania kopii zapasowych i planuje testy odtworzeniowe.

4.2.3 Zgłasza niepowodzenia i incydenty bezpośrednio do GM.

4.2.4 Zapewnia szyfrowanie, ograniczenia dostępu oraz właściwe postępowanie z nośnikami kopii zapasowych.

[... 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 przeglądowi co najmniej raz w roku przez GM. Przesłanki do przeglądu doraźnego obejmują:

9.1.1 istotne zmiany w systemach lub metodach przechowywania

9.1.2 wdrożenie nowych platform chmurowych lub systemów IT

9.1.3 zmiany prawne lub regulacyjne wpływające na odtwarzanie danych

9.1.4 ustalenia z audytów lub incydentów

9.2 GM odpowiada za zainicjowanie przeglądu, zatwierdzenie zmian i przekazanie aktualizacji.

9.3 Wersje polityki muszą być śledzone i archiwizowane. Wersje wycofane z użycia muszą mieć ograniczony dostęp, aby zapobiec niejasnościom podczas audytów lub zdarzeń związanych z odtworzeniem działalności.

10. Powiązane polityki i zależności

10.1 Niniejsza polityka jest spójna z następującymi politykami SME i od nich zależy:

10.1.1 P14S – Polityka retencji i utylizacji danych: określa, jak długo dane z kopii zapasowych powinny być przechowywane i bezpiecznie usuwane.

10.1.2 P13S – Polityka klasyfikacji i oznaczania danych: pomaga ustalić priorytet danych, które muszą być objęte kopiami zapasowymi, na podstawie poziomów klasyfikacji.

10.1.3 P30S – Polityka reagowania na incydenty: obejmuje procedury na wypadek niepowodzenia wykonywania kopii zapasowych lub konieczności odtworzenia danych po naruszeniu lub niedostępności.

10.1.4 P2S – Polityka ról i odpowiedzialności w ramach ładu zarządczego: przypisuje jednoznaczne uprawnienia do nadzoru nad kopiami zapasowymi i stosowania polityki.

10.1.5 P17S – Polityka ochrony danych i prywatności: zapewnia, że postępowanie z danymi osobowymi w kopiach zapasowych jest zgodne z wymogami prawnymi i przepisami dotyczącymi prywatności.

11. Normy i ramy odniesienia

11.1 ISO/IEC 27001

11.1.1 Klauzula 8.1: planowanie operacyjne i nadzór nad systemami tworzenia kopii zapasowych jako część SZBI

11.2 ISO/IEC 27002

11.2.1 Środek bezpieczeństwa 8.13: określa dobre praktyki w zakresie harmonogramowania, monitorowania i odtwarzania kopii zapasowych

11.2.2 Załącznik A, środek bezpieczeństwa 5.29: integracja kopii zapasowych z ciągłością działania i gotowością do odtworzenia

11.3 NIST SP 800-53 Rev.

11.3.1 CP-9 (Contingency Planning): definiuje uporządkowane strategie tworzenia kopii zapasowych na potrzeby odporności biznesowej

11.3.2 MP-6 (Media Protection): wymaga bezpiecznego postępowania z nośnikami kopii zapasowych i ich niszczenia

11.4 RODO

11.4.1 Artykuł 5(1)(f): nakłada wymóg zapewnienia integralności i dostępności danych osobowych

11.4.2 Artykuł 32(1)(c): wymaga zdolności do terminowego przywrócenia dostępu do danych osobowych

11.5 Dyrektywa NIS2 UE

11.5.1 Artykuł 21(2)(c): wymaga tworzenia kopii zapasowych i odtwarzania jako części planowania odporności i ciągłości działania

11.6 Rozporządzenie DORA UE

11.6.1 Artykuł 10(1): organizacje sektora finansowego muszą zapewniać kopie zapasowe jako część środków ciągłości ICT

11.7 COBIT 2019

11.7.1 BAI04.05: wymaga udokumentowanych strategii tworzenia kopii zapasowych

11.7.2 DSS04.07: podkreśla rutynowe testowanie i nadzór nad procesami tworzenia kopii zapasowych oraz odtwarzania danych