| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Wprowadź tutaj nazwę zarejestrowanej osoby prawnej | | | | | | | |
| Numer dokumentu:<br>P15 | | | | | Tytuł dokumentu:<br>**Polityka tworzenia kopii zapasowych i odtwarzania** | | | | | | | |
| Wersja:<br>1.0 | | Data wejścia w życie:<br>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 6.1.3, 8.1 | Postępowanie z ryzykiem, planowanie oraz operacyjne zabezpieczenia w zakresie kopii zapasowych |
| ISO/IEC 27002:2022 | Zabezpieczenia 8.13, 5.28, 5.29 | Zarządzanie kopiami zapasowymi, bezpieczna utylizacja oraz odporność |
| NIST SP 800-53 Rev.5 | CP-9, CP-10, SI-12, MP-6 | Wymagania dotyczące kopii zapasowych systemów, odzyskiwania oraz sanityzacji nośników |
| RODO | Artykuł 32, Motyw 49 | Odtwarzanie i dostępność danych osobowych, ciągłość działania |
| NIS2 | Artykuł 21(2)(c-e) | Zabezpieczenia w zakresie kopii zapasowych i ciągłości działania na potrzeby odporności |
| DORA | Artykuły 10, 11 | Wymagania sektora finansowego dotyczące kopii zapasowych, odzyskiwania i testowania |
| COBIT 2019 | DSS01, DSS04, MEA03 | Operacje tworzenia kopii zapasowych, ciągłość działania oraz monitorowanie zgodności |

**1. Cel**

1.1 Celem niniejszej polityki jest określenie obowiązkowych wymagań dotyczących tworzenia kopii zapasowych i odtwarzania danych, systemów oraz aplikacji w celu wspierania odporności operacyjnej, integralności danych i ciągłości działania.

**1.2 Polityka ustanawia ustandaryzowane ramy w celu:**

1.2.1 Ochrony danych organizacji przed utratą wskutek usunięcia, uszkodzenia, awarii lub cyberataków

1.2.2 Określenia wymagań dotyczących odzyskiwania poprzez jednoznaczne parametry RTO (Recovery Time Objective) i RPO (Recovery Point Objective)

1.2.3 Integracji operacji tworzenia kopii zapasowych z szerszym SZBI oraz planami ciągłości działania i planami odtwarzania po awarii (BCP/DRP)

1.2.4 Zapewnienia zgodności z mającymi zastosowanie przepisami prawa i regulacjami sektorowymi w zakresie dostępności i odtwarzalności

1.3 Polityka wdraża zabezpieczenia normy ISO/IEC 27001:2022 odnoszące się do bezpiecznej utylizacji danych (5.28), odporności (5.29) oraz kopii zapasowych informacji (8.13), a także odwołuje się do dobrych praktyk określonych w ISO/IEC 27002:2022, NIST SP 800-53 Rev.5, RODO, DORA i NIS2.

**2. Zakres**

**2.1 Niniejsza polityka ma zastosowanie do:**

2.1.1 Wszystkich systemów krytycznych dla działalności i systemów operacyjnych objętych zakresem SZBI

2.1.2 Wszystkich ustrukturyzowanych i nieustrukturyzowanych danych biznesowych, w tym baz danych, plików, wiadomości e-mail i konfiguracji

2.1.3 Wszystkich środowisk — infrastruktury lokalnej, chmury obliczeniowej, środowisk hybrydowych oraz zdalnych lub zewnętrznych lokalizacji przechowywania

2.1.4 Całego personelu odpowiedzialnego za zarządzanie, realizację, weryfikację lub odtwarzanie procesów tworzenia kopii zapasowych

**2.2 Polityka ma również zastosowanie do:**

2.2.1 Nośników i infrastruktury kopii zapasowych, w tym fizycznych taśm, urządzeń wirtualnych, migawek dyskowych oraz rozwiązań do tworzenia kopii zapasowych opartych na chmurze obliczeniowej

2.2.2 Dostawców zewnętrznych zakontraktowanych do hostowania, zarządzania lub przetwarzania kopii zapasowych organizacji

2.2.3 Kopii zapasowych dzienników, konfiguracji, ścieżek audytu oraz dokumentacji operacyjnej krytycznej dla ciągłości działania

2.3 Systemy wyraźnie wyłączone z tworzenia kopii zapasowych muszą zostać udokumentowane, poddane ocenie ryzyka oraz formalnie zaakceptowane przez Menedżera Systemu Zarządzania Bezpieczeństwem Informacji oraz właściciela systemu.

**3. Cele**

3.1 Zapewnienie, że dla wszystkich systemów krytycznych i danych tworzone są wiarygodne kopie zapasowe z odpowiednią częstotliwością, redundancją i zabezpieczeniami.

3.2 Zapewnienie mechanizmów odtwarzania spełniających zdefiniowane wymagania RTO i RPO, zgodnie z wynikami analiz wpływu na biznes.

3.3 Utrzymywanie pełnej dokumentacji procedur tworzenia kopii zapasowych, harmonogramów retencji, ról i technologii.

3.4 Walidacja skuteczności operacji tworzenia kopii zapasowych poprzez systematyczne testy odtwarzania, rejestrowanie awarii oraz monitorowanie działań naprawczych.

3.5 Ochrona danych kopii zapasowych przed nieuprawnionym dostępem, modyfikacją lub zniszczeniem przez cały ich cykl życia.

**3.6 Zapewnienie zgodności z:**

3.6.1 Wymaganiami operacyjnymi i wymaganiami ciągłości działania normy ISO/IEC 27001

3.6.2 Rodzinami CP i MP normy NIST SP 800-53 w zakresie kopii zapasowych i sanityzacji

3.6.3 Artykułem 32 i Motywem 49 RODO w zakresie przywracania dostępu do danych osobowych

3.6.4 Artykułem 10 DORA i Artykułem 21 NIS2 w zakresie ciągłości działania i odporności ICT

3.7 Zapewnienie, że usługi tworzenia kopii zapasowych świadczone przez strony trzecie spełniają umowne i regulacyjne obowiązki bezpieczeństwa, w tym w zakresie szyfrowania, utylizacji i protokołów powiadamiania.

**4. Role i odpowiedzialności**

**4.1 Kierownictwo wykonawcze**

4.1.1 Zatwierdza niniejszą politykę i zapewnia, że systemy krytyczne dla działalności są odpowiednio chronione z wykorzystaniem zatwierdzonych praktyk tworzenia kopii zapasowych i odtwarzania.

4.1.2 Odpowiada za zapewnienie odpowiednich zasobów dla operacji tworzenia kopii zapasowych oraz za ich okresowy przegląd pod kątem zgodności regulacyjnej.

**4.2 Dyrektor ds. Bezpieczeństwa Informacji (CISO)**

4.2.1 Jest właścicielem niniejszej polityki i zapewnia jej spójność z szerszymi ramami bezpieczeństwa informacji, zarządzania ryzykiem i ciągłości działania.

4.2.2 Nadzoruje integrację procedur tworzenia kopii zapasowych z BCP/DRP, reagowaniem na incydenty oraz planowaniem odporności.

4.2.3 Dokonuje przeglądu odstępstw dotyczących kopii zapasowych i ocenia propozycje akceptacji ryzyka dla wyłączeń systemów krytycznych.

[ ... 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 podlega przeglądowi co najmniej raz w roku lub wcześniej, jeżeli zostanie to wywołane przez:**

9.1.1 Zmiany strategii ciągłości działania lub odtwarzania po awarii

9.1.2 Nowe obowiązki regulacyjne lub prawne wpływające na częstotliwość tworzenia kopii zapasowych lub retencję danych

9.1.3 Zmiany architektury systemów, narzędzi do tworzenia kopii zapasowych lub dostawców usług

9.1.4 Istotne incydenty lub ustalenia audytowe związane z utratą danych lub niepowodzeniami odzyskiwania

**9.2 Przegląd jest koordynowany przez CISO we współpracy z:**

9.2.1 Zespołem ds. Infrastruktury i Operacji IT

9.2.2 Audytem wewnętrznym

9.2.3 Inspektorem Ochrony Danych

9.2.4 Zespołami ciągłości działania i odtwarzania po awarii

**9.3 Harmonogramy kopii zapasowych, wykazy systemów objętych zakresem, dokumentacja odtwarzania oraz rejestry odstępstw podlegają równoległemu przeglądowi w celu zapewnienia:**

9.3.1 Prawidłowości pokrycia kopiami zapasowymi dla wszystkich aktywów krytycznych

9.3.2 Zgodności z wymaganiami RTO/RPO i okresami retencji

9.3.3 Kompletności dzienników testowych i raportów incydentów

9.3.4 Usunięcia wcześniej zidentyfikowanych luk w zabezpieczeniach

**9.4 Wszystkie aktualizacje muszą:**

9.4.1 Być objęte kontrolą wersji i przechowywane w repozytorium dokumentów SZBI

9.4.2 Zawierać podsumowanie zmian i uzasadnienie

9.4.3 Być zatwierdzone przez kierownictwo wykonawcze

9.4.4 Być zakomunikowane całemu personelowi technicznemu i biznesowemu, którego dotyczą

**10. Powiązane polityki i zależności**

**10.1 Niniejsza polityka bezpośrednio wspiera i pozostaje powiązana z następującymi dokumentami:**

10.1.1 P6 - Polityka zarządzania ryzykiem: Określa priorytetyzację ochrony kopii zapasowych dla systemów i usług w oparciu o ryzyko.

10.1.2 P12 - Polityka zarządzania aktywami: Zapewnia, że systemy kwalifikujące się do objęcia kopiami zapasowymi są ujęte w inwentarzu oraz powiązane ze śledzeniem cyklu życia i klasyfikacją.

10.1.3 P13 - Polityka klasyfikacji i etykietowania danych: Określa, które kategorie danych wymagają tworzenia kopii zapasowych, w tym metadane etykietowania na potrzeby priorytetyzacji.

10.1.4 P14 - Polityka retencji i utylizacji danych: Koordynuje retencję kopii zapasowych z regulacyjnymi limitami przechowywania oraz właściwą utylizacją nośników po upływie ich okresu użytkowania.

10.1.5 P16 - Polityka maskowania danych i pseudonimizacji: Wspiera minimalizację danych podczas tworzenia kopii zapasowych wrażliwych zbiorów danych.

10.1.6 P30 - Polityka reagowania na incydenty: Uruchamiana w przypadku awarii kopii zapasowych, problemów z odtwarzaniem lub naruszenia repozytoriów danych kopii zapasowych.

10.2 Te wzajemnie powiązane polityki tworzą spójne ramy zapewniające, że nadzór nad kopiami zapasowymi jest osadzony w szerszym SZBI organizacji oraz strategii odporności operacyjnej.

## 11. Normy i ramy odniesienia

### 11.1 ISO/IEC 27001:

11.1.1 Klauzula 6.1.3 - plan postępowania z ryzykiem: Wspiera priorytetyzację kopii zapasowych i planowanie odtwarzania w oparciu o ryzyko.

11.1.2 Klauzula 8.1 - planowanie i nadzór operacyjny: Integruje zabezpieczenia odzyskiwania i ciągłości działania jako część zabezpieczeń operacyjnych.

11.1.3 Załącznik A, zabezpieczenie 5.28 - bezpieczna utylizacja lub ponowne użycie sprzętu: Odnosi się do bezpiecznej sanityzacji nośników kopii zapasowych.

11.1.4 Załącznik A, zabezpieczenie 5.29 - bezpieczeństwo informacji podczas zakłóceń: Zapewnia zdolność do odtwarzania podczas incydentów lub awarii.

11.1.5 Załącznik A, zabezpieczenie 8.13 - kopie zapasowe informacji: Realizowane bezpośrednio poprzez planowe, testowane i bezpieczne operacje tworzenia kopii zapasowych.

11.2 ISO/IEC 27002:2022 - Zabezpieczenia 8.13, 5.28, 5.29: Zabezpieczenia te wzmacniają wymaganie regularnego tworzenia kopii zapasowych, walidacji integralności oraz planowania odtwarzania we wszystkich środowiskach IT.

### 11.3 NIST SP 800-53 Rev.5:

11.3.1 CP-9 - kopia zapasowa systemu: Ustanawia kompleksowe procedury tworzenia kopii zapasowych, w tym przechowywanie poza lokalizacją podstawową i testy odtwarzania.

11.3.2 CP-10 - odzyskiwanie i odtwarzanie systemu: Wymaga zwalidowanych procedur pełnego lub częściowego odtwarzania zgodnych z celami odzyskiwania.

11.3.3 MP-6 - sanityzacja nośników: Zapewnia bezpieczne postępowanie z wycofanymi nośnikami kopii zapasowych.

11.3.4 SI-12 - procedury postępowania z informacjami: Wzmacnia odpowiedzialności związane z kopiami zapasowymi i odzyskiwaniem danych wrażliwych.

### 11.4 RODO (UE 2016/679):

11.4.1 Artykuł 32 - bezpieczeństwo przetwarzania: Nakłada wymóg zapewnienia zdolności odtwarzania oraz zabezpieczeń dostępności danych, w szczególności danych osobowych.

11.4.2 Motyw 49: Wspiera środki ciągłości działania i odtwarzania po awarii, w tym bezpieczne kopie zapasowe jako element odporności organizacyjnej.

### 11.5 Dyrektywa NIS2 (UE 2022/2555):

11.5.1 Artykuł 21(2)(c-e): Wymaga środków technicznych i organizacyjnych, w tym zabezpieczeń w zakresie kopii zapasowych i ciągłości działania, w celu zapewnienia odporności usług.

### 11.6 DORA (UE 2022/2554):

11.6.1 Artykuł 10 - ciągłość działania ICT: Wymaga od podmiotów finansowych pełnych kopii zapasowych danych, odzyskiwania i planowania ciągłości działania.

11.6.2 Artykuł 11 - testowanie planów ciągłości działania ICT: Podkreśla walidację zdolności odzyskiwania poprzez regularne testowanie.

**11.7 COBIT 2019:**

11.7.1 DSS01 - zarządzane operacje: Wspiera niezawodne świadczenie usług poprzez chronioną dostępność danych.

11.7.2 DSS04 - zarządzana ciągłość: Definiuje strategiczne i operacyjne zabezpieczenia ciągłości działania, w tym zweryfikowane kopie zapasowe.

11.7.3 MEA03 - monitorowanie, ocena i weryfikacja zgodności: Nakłada wymóg okresowego przeglądu zabezpieczeń ciągłości działania, w tym skuteczności kontroli kopii zapasowych.