{Nazwa systemu}

Kategoryzacja bezpieczeństwa: Wysoka

{Nazwa organizacji}

Plan awaryjny systemu informatycznego (ISCP)

Wersja [Wstaw #]

[Data]

Opracowane przez

[Nazwa organizacji]

[Adres]

Spis treści

[Zatwierdzenie planu 4](#_Toc40855997)

[1 Wstęp 5](#_Toc40855998)

[1.1 Tło 5](#_Toc40855999)

[1.2 Zakres 5](#_Toc40856000)

[1.3 Założenia 6](#_Toc40856001)

[2 Koncepcja operacji 6](#_Toc40856002)

[2.1 Opis systemu 7](#_Toc40856003)

[2.2 Przegląd trzech faz 7](#_Toc40856004)

[2.3 Role i odpowiedzialność 8](#_Toc40856005)

[3 Aktywacja i powiadamianie 8](#_Toc40856006)

[3.1 Kryteria aktywacji i procedury 9](#_Toc40856007)

[3.2 Powiadamianie 9](#_Toc40856008)

[3.3 Ocena awarii 9](#_Toc40856009)

[4 Odzyskiwanie 10](#_Toc40856010)

[4.1 Sekwencja czynności odzyskiwania 10](#_Toc40856011)

[4.2 Procedury odzyskiwania 10](#_Toc40856012)

[4.3 Powiadomienia o eskalacji odzyskiwania / świadomość sytuacyjna 11](#_Toc40856013)

[5 Odtwarzanie 11](#_Toc40856014)

[5.1 Przetwarzanie równoległe 11](#_Toc40856015)

[5.2 Testowanie poprawności danych 11](#_Toc40856016)

[5.3 Testowanie poprawności funkcjonalnej 12](#_Toc40856017)

[5.4 Deklaracja odzyskania systemu 12](#_Toc40856018)

[5.5 Powiadomienia (użytkowników) 12](#_Toc40856019)

[5.6 Czyszczenie 12](#_Toc40856020)

[*5.7* Przechowywanie danych poza siedzibą 13](#_Toc40856021)

[*5.8* Kopia zapasowa danych 13](#_Toc40856022)

[5.9 Dokumentowanie zdarzenia 13](#_Toc40856023)

[5.10 Dezaktywacja 14](#_Toc40856024)

[Sugerowane dodatki 14](#_Toc40856025)

[DODATEK A – LISTA KONTAKTOWA PERSONELU 15](#_Toc40856026)

[DODATEK B – LISTA KONTAKTÓW DO DOSTAWCÓW 17](#_Toc40856027)

[DODATEK C – SZCZEGÓŁOWE PROCEDURY ODZYSKIWANIA 17](#_Toc40856028)

[DODATEK D – PROCEDURY ALTERNATYWNE 17](#_Toc40856029)

[DODATEK E – PLAN TESTOWANIA POPRAWNOŚCI SYSTEMU 17](#_Toc40856030)

[DODATEK F – ALTERNATYWNE MIEJSCE PRZECHOWYWANIA DANYCH, ZAPASOWE MIEJSCE PRACY I ŚRODKI TELEKOMUNIKACJI 19](#_Toc40856031)

[DODATEK G – SCHEMATY (SYSTEM I URZĄDZENIA WEJŚCIA/WYJŚCIA) 20](#_Toc40856032)

[DODATEK H – INWENTARYZACJA SPRZĘTU I OPROGRAMOWANIA 20](#_Toc40856033)

[DODATEK I – TABELA POŁĄCZEŃ 20](#_Toc40856034)

[DODATEK J – HARMONOGRAM TESTÓW I UTRZYMANIA 21](#_Toc40856035)

[DODATEK K – POWIĄZANE PLANY I PROCEDURY 22](#_Toc40856036)

[DODATEK L – ANALIZA WPŁYWU NA DZIAŁALNOŚĆ (BIA) 22](#_Toc40856037)

[DODATEK M – STRONA ZMIANY DOKUMENTU 23](#_Toc40856038)

# Zatwierdzenie planu

Na drugiej stronie Planu awaryjnego systemu informatycznego (ISCP) należy zamieścić oświadczenie zgodnie z polityką stosowaną w organizacji w zakresie planowania awaryjnego, tak aby potwierdzić, że ISCP jest kompletny i został odpowiednio przetestowany. Oświadczenie powinno zostać zatwierdzone i podpisane przez właściwy organ organizacji. Oświadczenie powinno również potwierdzać, że wyznaczony organ jest odpowiedzialny za dalsze utrzymanie i testowanie ISCP. Należy wyznaczyć miejsce do podpisania przez wyznaczony organ wraz z innymi stosownymi podpisami zatwierdzającymi. Przykładowy zapis oświadczenia:

*Data …………………………………………*

*Jako organ wyznaczony dla {nazwa systemu}, niniejszym zaświadczam, że plan awaryjny systemu informatycznego (ISCP) jest kompletny oraz, że informacje zawarte w tym ISCP dokładne odzwierciedlają aplikacje, sprzęt, oprogramowanie i komponenty telekomunikacyjne {nazwa systemu}. Dodatkowo poświadczam, że dokument ten określa krytyczność systemu w związku z misją {nazwa organizacji} oraz, że zidentyfikowane strategie odzyskiwania zapewnią możliwość odzyskania funkcjonalności systemu w najbardziej dogodny i opłacalny sposób, zachowując jego poziomem krytyczności.*

*Ponadto potwierdzam, że niniejszy ISCP dla {nazwa systemu} będzie testowany co najmniej raz w roku. Plan był ostatnio testowany {wstaw datę przeprowadzonych testów}; materiały na temat przeprowadzonego testu, szkolenia i ćwiczeń (TT&E) z nim związanych, można znaleźć w {załącznik lub protokół z wynikami TT&E}. Ten dokument będzie modyfikowany w miarę wprowadzania zmian i pozostanie aktualizowany o kolejne wersje kontrolne, zgodnie z polityką planowania awaryjnego {nazwa organizacji}.*

*………………………………………………………….*

*{Imię i Nazwisko właściciela systemu}*

*{Stanowisko właściciela systemu}*

# Wstęp

Systemy informatyczne są niezbędne do realizacji procesów biznesowych {*nazwa organizacji*}; dlatego bardzo ważne jest, aby usługi świadczone przez {*nazwa systemu*} mogły funkcjonować skutecznie bez nadmiernych zakłóceń. Niniejszy plan awaryjny systemu informacyjnego (ISCP) ustanawia kompleksowe procedury szybkiego i skutecznego odtworzenia systemu {*nazwa systemu*} po zakłóceniu usługi.

## Tło

Niniejszy ISCP ustanawia procedury odtworzenia {*nazwa systemu*} po zakłóceniu. Ustalono następujące cele planu odtworzenia:

1. Maksymalizację skuteczności operacji awaryjnych poprzez ustalony plan, który składa się z następujących faz:

* Faza aktywacji i powiadomienia w celu aktywacji planu i ustalenia zakresu szkód;
* Faza odzyskiwania w celu przywrócenia operacji {*nazwa systemu*}; i
* Faza odtworzenia w celu upewnienia się, że {*nazwa systemu*} został sprawdzony podczas testów i że normalne operacje zostaną wznowione.

1. Identyfikację działania, zasobów i procedur w celu spełnienia wymagań przetwarzania {*nazwa systemu*} podczas długotrwałych przerw w normalnych operacjach.
2. Przypisanie obowiązków wyznaczonemu personelowi {*nazwa organizacji*} i zapewnienie wskazówek dotyczących odzyskiwania {*nazwa systemu*} podczas długotrwałych przerw w normalnych operacjach.
3. Zapewnienia koordynacji z innymi pracownikami odpowiedzialnymi za strategie planowania awaryjnego {*nazwa organizacji*} oraz zapewnienia koordynacji z zewnętrznymi punktami kontaktowymi i dostawcami powiązanymi z {*nazwa systemu*} oraz wykonania tego planu.

## Zakres

Niniejszy ISCP został opracowany dla {*nazwa systemu*}, który został sklasyfikowany jako system o wysokim wpływie zakłócenia, zgodnie z NSC 199. Procedury w tym ISCP dotyczą systemów o wysokim wpływie zakłócenia i mają na celu odzyskanie {*nazwa systemu*} w ciągu {*ilość godzin RTO*}. Plan ten nie dotyczy wymiany lub zakupu nowego sprzętu w przypadku krótkotrwałych zakłóceń trwających krócej niż { *ilość godzin RTO*} lub utraty danych w obiekcie zasadniczym lub na poziomie pulpitu użytkownika. Ponieważ {*nazwa systemu*} jest systemem o wysokim wpływie, alternatywne miejsce przechowywania danych i alternatywne miejsce przetwarzania nie są wymagane.

## Założenia

Przy opracowywaniu tego ISCP zastosowano następujące założenia:

* {*Nazwa systemu*} został ustanowiony jako system o wysokim poziomie wpływu, zgodnie z NSC 199.
* W systemie są wymagane alternatywne miejsca przetwarzania i alternatywne miejsce przechowywania danych.
* Bieżące kopie zapasowe oprogramowania systemowego i danych są nienaruszone i dostępne w zewnętrznym magazynie w {*adres*}.
* W alternatywnym miejscu pracy {*adres*} dostępne są alternatywne urządzenia i są one dostępne, jeśli są potrzebne do przeniesienia {*nazwa systemu*}.
* {*Nazwa systemu*} może nie działać w ciągu {*ilość godzin RTO*}.
* Kluczowy personel {*nazwa systemu*} został zidentyfikowany i przeszkolony w zakresie swoich ról w zakresie reagowania kryzysowego i odzyskiwania i jest dostępny, aby aktywować Plan awaryjny {*nazwa systemu*}.
* Dodatkowe założenia – w stosownych przypadkach.

ISCP {nazwa systemu} nie ma zastosowania w następujących sytuacjach:

* **Ogólnego odzyskiwania i ciągłość operacji biznesowych**. Plan ciągłości działania (BCP) i plan kontynuacji operacji (COOP) dotyczą ciągłości operacji biznesowych.
* **Awaryjnej ewakuacji personelu**. Plan awaryjny dla zasobów ludzkich (OEP) dotyczy ewakuacji pracowników.
* Wszelkie dodatkowe ograniczenia i powiązane plany należy dodać do tej listy.

# Koncepcja operacji

Sekcja Koncepcja operacji zawiera szczegółowe informacje na temat {*nazwa systemu*}, przegląd trzech faz ISCP (aktywacja i powiadomienie, odzyskiwanie oraz odtwarzanie), a także opis ról i obowiązków personelu {*nazwa organizacji*} podczas aktywacji procedury awaryjnej.

## Opis systemu

*UWAGA: Informacje dla tej sekcji powinny być dostępne z Planu bezpieczeństwa systemu (ang. System Security Plan - SSP) i można je skopiować z SSP lub odnieść się do odpowiedniej sekcji w SSP i dołączyć najnowszą wersję SSP do tego planu awaryjnego. Należy podać ogólny opis architektury systemu i funkcjonalności. Wskaż środowisko operacyjne, lokalizację fizyczną, ogólną lokalizację użytkowników oraz opis współpracy z zewnętrznymi organizacjami / systemami. Dołącz informacje dotyczące wszelkich innych zagadnień technicznych, które są ważne dla celów odzyskiwania, takich jak procedury tworzenia kopii zapasowych.*

## Przegląd trzech faz

Niniejszy ISCP został opracowany w celu odzyskania i odtworzenia {*nazwa systemu*} przy użyciu trójfazowego podejścia. Takie podejście zapewnia, że wysiłki związane z odzyskaniem i odtwarzaniem systemu są wykonywane metodycznie, aby zmaksymalizować skuteczność wysiłków związanych z odzyskaniem i odtwarzaniem oraz zminimalizować czas przestoju systemu z powodu zakłócenia. Trzy fazy odzyskiwania systemu to:

**Faza aktywacji i powiadomienia** - aktywacja ISCP następuje po zakłóceniu lub awarii, które mogą spowodować przestój systemu wykraczający poza ustalone dla tego systemu RTO. Awaria może spowodować poważne uszkodzenie obiektu, w którym mieści się system, poważne uszkodzenie lub utratę sprzętu lub inne uszkodzenia, które zwykle powodują długoterminową utratę zdolności przetwarzania informacji.

Po aktywacji ISCP właściciele systemu i użytkownicy są powiadamiani o możliwym długoterminowym wyłączeniu oraz przeprowadzana jest dokładna ocena awarii systemu. Informacje z oceny awarii są przedstawiane właścicielom systemu i mogą być wykorzystane do modyfikacji procedur odzyskiwania specyficznych dla danej przyczyny awarii.

**Faza odzyskiwania** - faza odzyskiwania zawiera szczegółowe informacje na temat działań i procedur odzyskiwania systemu, którego dotyczy problem. Działania i procedury są napisane na poziomie, który pozwala odpowiednio wykwalifikowanemu technikowi odzyskać system bez ścisłej wiedzy o tym systemie. Ta faza obejmuje procedury powiadamiania i eskalacji działań w celu przekazania statusu przywracania właścicielom systemu i użytkownikom.

**Faza** **odtwarzania** - Faza odtwarzania określa działania podejmowane w celu przetestowania i potwierdzenia zdolności i funkcjonalności systemu w pierwotnej lub nowej lokalizacji. Faza ta składa się z dwóch głównych działań: sprawdzania poprawności odtworzenia i dezaktywacji planu:

* Podczas sprawdzania poprawności, system jest testowany i sprawdzany czy osiągnął zdolność do działania tak, jak w stanie normalnym. Procedury sprawdzania poprawności mogą obejmować testowanie funkcjonalności lub regresji, równoczesne przetwarzanie i/lub sprawdzanie poprawności danych. System zostaje przez właściciela uznany za odtworzony i zdolny do normalnego działania po pomyślnym zakończeniu testów walidacyjnych.
* Dezaktywacja obejmuje działania mające na celu powiadomienie użytkowników o stanie operacyjnym systemu. Faza ta obejmuje także dokumentowanie wysiłków związanych z odzyskiwaniem, finalizację dziennika aktywności, włączenie wyciągniętych wniosków do aktualizacji planu i przygotowanie zasobów na możliwe przyszłe zdarzenia.

## Role i odpowiedzialność

ISCP ustanawia kilka ról związanych z obsługą odzyskiwania i odtwarzania {*nazwa systemu*}. Osoby lub zespoły przypisane do ról ISCP zostały przeszkolone w zakresie reagowania na zdarzenie awaryjne mające wpływ na {*nazwa systemu*}.

*Opisz każdy zespół i rolę odpowiedzialną za wykonywanie lub wspieranie odzyskiwania i odtwarzania systemu. Zależnie od przypadku, uwzględnij obowiązki dla każdego zespołu/roli, role kierownicze i koordynację z innymi zespołami ds. odzyskiwania i odtwarzania. Jako minimum należy ustanowić rolę właściciela systemu lub punktu kontaktowego jednostki biznesowej, koordynatora odzyskiwania oraz technicznego punktu kontaktowego odzyskiwania.*

*Role kierownicze powinny obejmować kierownika ISCP, który ponosi ogólną odpowiedzialność za zarządzanie planem, oraz koordynatora ISCP, który jest odpowiedzialny za nadzorowanie postępów w zakresie odzyskiwania i odtwarzania, inicjowanie wszelkich niezbędnych eskalacji lub komunikacji informującej o postępie prac w ISCP oraz ustanowienie koordynacji z innymi zespołami ds. odzyskiwania i odtwarzania.*

# Aktywacja i powiadamianie

Faza aktywacji i powiadomienia określa wstępne działania podejmowane po wykryciu zakłócenia {*nazwa systemu*} lub gdy wydaje się, że przestój systemu jest nieuchronny. Faza ta obejmuje działania mające na celu powiadomienie personelu ds. odzyskiwania, przeprowadzenie oceny awarii i aktywację ISCP. Po zakończeniu fazy aktywacji i powiadomienia {*nazwa systemu*}, personel ISCP będzie przygotowany do przeprowadzenia działań naprawczych.

## Kryteria aktywacji i procedury

ISCP {*nazwa systemu*} może zostać aktywowany, jeśli zostanie spełnione co najmniej jedno z następujących kryteriów:

1. Rodzaj awarii wskazuje, że {*nazwa systemu*} będzie wyłączona na więcej niż {*godziny RTO*};
2. Infrastruktura budowlana lokalizacji {*nazwa systemu*} jest uszkodzona i może nie być dostępna w ciągu {*godzin RTO*};
3. *Inne kryteria, stosownie do przypadku*.

Jeśli jedno lub więcej z powyższych kryteriów jest spełnione, następujące osoby lub role mogą aktywować ISCP:

*Ustal jedną lub więcej ról, które mogą aktywować plan na podstawie kryteriów aktywacji. Upoważnione osoby mogą obejmować właściciela systemu / firmy lub operacyjny punkt kontaktowy (PoC) ustanowiony w celu wsparcia systemu.*

## Powiadamianie

Pierwszym krokiem po aktywacji ISCP {*nazwa systemu*} jest powiadomienie odpowiedniego personelu odpowiedzialnego za realizację zadań biznesowych organizacji i personelu wsparcia systemu. Informacje kontaktowe do odpowiednich PoC znajdują się w {*Nazwa listy kontaktów w załączniku*}.

W przypadku {*nazwa systemu*} stosowana jest następująca metoda i procedura powiadomień:

*Opisz ustanowione procedury powiadomień. Procedury powiadomień powinny obejmować to, kto dokonuje pierwszych powiadomień, kolejność, w jakiej powiadamiany jest personel (np. właściciel systemu, techniczny PoC, koordynator ISCP, PoC jednostki biznesowej lub jednostki użytkownika oraz PoC zespołu odzyskiwania) oraz sposób powiadomienia (np. wysyłanie wiadomości e-mail, drzewo połączeń, automatyczny system powiadomień itp.).*

## Ocena awarii

Po powiadomieniu o aktywacji ISCP konieczna jest dokładna ocena awarii w celu ustalenia zakresu zakłócenia, wszelkich szkód i oczekiwanego czasu naprawy. Tę ocenę awarii przeprowadza {*nazwa zespołu odzyskiwania*}. Wyniki oceny są przekazywane koordynatorowi ISCP, aby pomóc w koordynowaniu odzyskiwania {*nazwa systemu*}.

*Zarys szczegółowych procedur w celu ustalenia, jak ustalić przyczynę awarii; identyfikacja możliwości dodatkowego zakłócenia lub uszkodzenia; ocena dotkniętych obszarów fizycznych; oraz określenie stanu infrastruktury fizycznej, funkcjonalności sprzętu IT i innych zasobów. Procedury powinny obejmować opis komponentów, które będą musiały zostać wymienione oraz szacowany czas przywrócenia usługi do normalnej pracy.*

# Odzyskiwanie

Faza odzyskiwania zapewnia formalne operacje odzyskiwania, które rozpoczynają się po aktywacji ISCP, ocenie skutków wyłączeń (jeśli to możliwe), powiadomieniu personelu i zmobilizowaniu odpowiednich zespołów. Działania w fazie odzyskiwania koncentrują się na wdrażaniu strategii odzyskiwania w celu przywrócenia możliwości systemu, naprawy uszkodzeń i wznowienia możliwości operacyjnych w pierwotnej lub alternatywnej lokalizacji. Po zakończeniu fazy odzyskiwania system {*nazwa systemu*} będzie funkcjonalny i będzie mógł wykonywać funkcje określone w sekcji 2.1 niniejszego planu.

## Sekwencja czynności odzyskiwania

Podczas odzyskiwania {*nazwa systemu*} występują następujące działania:

*{Zmodyfikuj poniższą listę odpowiednio do wybranej strategii odzyskiwania systemu}*.

1. Zidentyfikuj lokalizację odzyskiwania (jeśli nie w pierwotnej lokalizacji organizacji);
2. Zidentyfikuj zasoby wymagane do przeprowadzenia procedur odzyskiwania;
3. Pobierz kopię zapasową i nośnik instalacyjny systemu;
4. Odzyskaj sprzęt i system operacyjny (jeśli jest wymagany);
5. Odzyskaj system z kopii zapasowej i nośnika instalacyjnego systemu.

## Procedury odzyskiwania

Poniżej przedstawiono procedury odzyskiwania {*nazwa systemu*} w pierwotnej lub alternatywnej lokalizacji. Aby utrzymać efektywny wysiłek odzyskiwania, procedury odzyskiwania są określone dla każdego zespołu i powinny być wykonywane w przedstawionej kolejności.

*Podaj ogólne procedury odzyskiwania systemu z nośnika kopii zapasowej. Jeśli alternatywna lokalizacja (zapasowe miejsce pracy) jest częścią strategii odzyskiwania, dołącz procedury odzyskiwania w tej lokalizacji. Szczegółowe procedury powinny się znaleźć w załączniku. Jeżeli w załączniku podano określone procedury, w tej sekcji należy zawrzeć odniesienie do tego dodatku. Powinny zostać zidentyfikowane zespoły lub osoby odpowiedzialne za każdą procedurę.*

## Powiadomienia o eskalacji odzyskiwania / świadomość sytuacyjna

*Zapewnij odpowiednie procedury dotyczące powiadomień o eskalacji podczas odzyskiwania. Powiadomienia podczas odzyskiwania obejmują eskalację problemu do kierownictwa i kształtowanie świadomości o statusie dla właścicieli systemów i użytkowników. Powinny zostać zidentyfikowane zespoły lub osoby odpowiedzialne za każdą procedurę eskalacji / podnoszenia świadomości.*

# Odtwarzanie

Odtwarzanie to proces, w którym czynności odzyskiwania są zakończone i wznawiane są normalne operacje systemowe. Jeśli pierwotnego obiektu podstawowego miejsca pracy nie można odzyskać, w celu spełnienia wymagań przetwarzania systemu, działania na tym etapie można również zastosować do przygotowania nowej stałej lokalizacji. Należy ustalić, czy system przeszedł znaczącą zmianę i będzie wymagał ponownej oceny i ponownej autoryzacji. Faza składa się z dwóch głównych działań: zatwierdzenia pomyślnego odtworzenia i dezaktywacji planu.

## Przetwarzanie równoległe

*Zasadniczo systemy o wysokim poziomie wpływu zakłócenia nie muszą stosować przetwarzania równoległego jako metody zapewnienia ciągłości działania. Jeśli jednak zastosowano taką metodę, należy tutaj wprowadzić opis jej procedur. Procedury powinny obejmować czas równoczesnego przetwarzania, sposób przetwarzania informacji w obu równoległych systemach oraz sposób sprawdzania poprawności informacji w odzyskanym systemie.*

*W przypadku systemów o wysokim wpływie zakłócenia, ale bez prowadzenia równoczesnego przetwarzania, tę sekcję można usunąć, albo zastosować następujące stwierdzenia:*

Podczas równoległego przetwarzania system funkcjonuje jednocześnie w dwóch oddzielnych lokalizacjach, dopóki nie nastąpi pewność, że odzyskany system działa poprawnie.

{*Nazwa systemu*} nie posiada przetwarzania równoległego jako sposobu sprawdzania poprawności. Po przetestowaniu i zatwierdzeniu odzyskanego systemu zostanie on wprowadzony do normalnej pracy.

## Testowanie poprawności danych

Testowanie poprawności danych to proces testowania i sprawdzania odzyskanych danych w celu upewnienia się, że pliki danych lub bazy danych zostały całkowicie odzyskane w stałej lokalizacji. Aby ustalić, czy dane są kompletne i aktualne w stosunku do ostatniej dostępnej kopii zapasowej, zostaną zastosowane następujące procedury:

*Zapewnij procedury testowania i sprawdzania poprawności danych, aby upewnić się, że dane są poprawne i aktualne. Ta sekcja może być połączona z sekcją Testowanie poprawności funkcjonalnej, jeżeli procedury testują zarówno funkcjonalność, jak i poprawność danych. Powinny zostać zidentyfikowane zespoły lub osoby odpowiedzialne za każdą procedurę. Przykładem testu poprawności danych dla systemu o wysokim poziomie wpływu byłoby sprawdzenie, czy ostatnia znana kompletna transakcja została zaktualizowana w bazie danych. Szczegółowe procedury testowania danych można znaleźć w załączniku E, Plan testów poprawności systemu.*

## Testowanie poprawności funkcjonalnej

Testowanie poprawności funkcjonalniej to proces sprawdzania, czy funkcje {*nazwa systemu*} zostały przetestowane i czy system jest gotowy do powrotu do normalnej pracy.

*Przeprowadź testy funkcjonalnie i/lub procedury sprawdzania poprawności systemu, aby upewnić się, że system działa poprawnie. Tę sekcję można połączyć z sekcją Testowanie poprawności danych, jeśli procedury sprawdzają zarówno funkcjonalność, jak i poprawność danych. Powinny zostać zidentyfikowane zespoły lub osoby odpowiedzialne za każdą procedurę. Przykładem testu funkcjonalnego dla systemu o wysokim poziomie wpływie może być zalogowanie się do systemu i uruchomienie raportu lub wykonanie transakcji, aby sprawdzić, czy system działa poprawnie. Szczegółowe procedury testowania funkcjonalności można znaleźć w dodatku E, Plan testów poprawności systemu.*

## Deklaracja odzyskania systemu

Po pomyślnym zakończeniu testowaniu poprawności {*właściciel systemu*} oficjalnie ogłosi zakończenie odzyskiwania i stwierdzi, że {*nazwa systemu*} działa poprawnie. Biznesowe i techniczne PoC {*nazwa systemu*} zostaną powiadomione o deklaracji przez koordynatora ISCP.

## Powiadomienia (użytkowników)

Po powrocie do normalnych operacji systemowych użytkownicy {*nazwa systemu*} zostaną powiadomieni przez {*rola*} *przy użyciu wcześniej określonych procedur powiadamiania (np. e‑mail, wiadomości rozgłoszeniowe, połączenia telefoniczne itp.)*.

## Czyszczenie

Czyszczenie to proces demontażu tymczasowych (zapasowych) miejsc pracy wykorzystywanych do celów odzyskiwania, uzupełniania zużytych materiałów eksploatacyjnych, zwracania instrukcji lub innej dokumentacji do ich pierwotnych lokalizacji oraz przygotowania systemu na ewentualne przyszłe zdarzenia awaryjne.

*Podaj wszelkie specyficzne procedury czyszczenia systemu, w tym preferowane lokalizacje instrukcji i dokumentów oraz przywrócenia kopii zapasowej lub nośnika instalacyjnego do pierwotnej lokalizacji.*

## Przechowywanie danych poza siedzibą

Ważne jest, aby wszystkie nośniki kopii zapasowych i instalacyjnych użyte podczas odzyskiwania zostały zwrócone do lokalizacji przechowywania danych poza siedzibą organizacji. Należy wykonać następujące procedury, aby zwrócić nośnik kopii zapasowej i instalacyjny do lokalizacji przechowywania danych poza siedzibą organizacji.

*Podaj procedury zwracania pobranego nośnika kopii zapasowej lub instalacyjnego do lokalizacji przechowywania danych poza siedzibą organizacji. Może to obejmować prawidłowe rejestrowanie i pakowanie nośników kopii zapasowych i instalacyjnych, przygotowanie do transportu i sprawdzanie, czy nośnik jest bezpiecznie przechowywany w lokalizacji poza siedzibą firmy.*

## Kopia zapasowa danych

Po odzyskaniu systemu, tak szybko jak tylko będzie to uzasadnione, należy wykonać pełną kopię zapasową systemu i zapisać tę kopię na potrzeby przyszłych działań związanych z odzyskiwaniem. Pełna kopia zapasowa jest następnie przechowywana z wraz innymi kopiami zapasowymi systemu. Procedury przeprowadzania pełnej kopii zapasowej systemu to:

*Ustal odpowiednie procedury zapewniające wykonanie w rozsądnym czasie pełnej kopii zapasowej systemu, najlepiej w następnym zaplanowanym okresie tworzenia kopii zapasowej.*

## Dokumentowanie zdarzenia

Ważne jest, aby wszystkie zdarzenia związane z odzyskiwaniem były dobrze udokumentowane, w tym podjęte działania i problemy napotkane podczas wysiłków związanych z odzyskiwaniem i odtwarzaniem oraz wyciągnięte wnioski na temat uruchomienia i aktualizacji niniejszego ISCP. Obowiązkiem każdego zespołu lub osoby działającego w ramach ISCP jest udokumentowanie swoich działań związanych z odzyskiwaniem i odtwarzaniem oraz przekazanie tej dokumentacji koordynatorowi ISCP.

*Podaj szczegółowe informacje na temat rodzajów informacji, które każdy członek zespołu ISCP jest zobowiązany dostarczyć lub zebrać w celu aktualizacji ISCP o wyciągnięte wnioski. Rodzaje dokumentacji, które należy wygenerować i zebrać po aktywacji awaryjnej, obejmują:*

* *Dzienniki aktywności (w tym wykonane kroki odzyskiwania i przez kogo, czas zainicjowania i ukończenia kroków oraz wszelkie problemy lub wątpliwości napotkane podczas wykonywania działań);*
* *Wyniki testów funkcjonalności i testów danych;*
* *Udokumentowanie wyciągniętych wniosków;*
* *Raporty z działania.*

*Procedury dokumentacji zdarzeń powinny szczegółowo określać odpowiedzialność za rozwój, zbieranie, zatwierdzanie i utrzymywanie.*

## Dezaktywacja

Po zakończeniu wszystkich działań i zaktualizowaniu dokumentacji {*właściciel systemu*} formalnie dezaktywuje działanie ISCP w zakresie odzyskiwania i odtwarzania. Powiadomienie o tej deklaracji zostanie dostarczone do wszystkich PoC biznesowych i technicznych.

# Sugerowane dodatki

Sugerowane są następujące dodatki do planu ISCP:

# DODATEK A – LISTA KONTAKTOWA PERSONELU

| **{nazwa systemu} kluczowy personel ISCP** | | |
| --- | --- | --- |
| **Kluczowy personel** | **Informacja o kontakcie** | |
| **Kierownik ISCP** | Tel. praca | *Wstaw numer* |
| *Wstaw imię, nazwisko i stanowisko* | Tel. dom | *Wstaw numer* |
| *Wstaw dokładny adres* | Tel. kom. | *Wstaw numer* |
| Email | *Wstaw adres email* |
| **Zastępca Kierownika ISCP** | Tel. praca | *Wstaw numer* |
| *Wstaw imię, nazwisko i stanowisko* | Tel. dom | *Wstaw numer* |
| *Wstaw dokładny adres* | Tel. kom. | *Wstaw numer* |
| Email | *Wstaw adres email* |
| **Koordynator ISCP** | Tel. praca | *Wstaw numer* |
| *Wstaw imię, nazwisko i stanowisko* | Tel. dom | *Wstaw numer* |
| *Wstaw dokładny adres* | Tel. kom. | *Wstaw numer* |
| Email | *Wstaw adres email* |
| **Zastępca Koordynatora ISCP** | Tel. praca | *Wstaw numer* |
| *Wstaw imię, nazwisko i stanowisko* | Tel. dom | *Wstaw numer* |
| *Wstaw dokładny adres* | Tel. kom. | *Wstaw numer* |
| Email | *Wstaw adres email* |
| **Kierownik Zespołu {Nazwa Zespołu 1}** | Tel. praca | *Wstaw numer* |
| *Wstaw imię, nazwisko i stanowisko* | Tel. dom | *Wstaw numer* |
| *Wstaw dokładny adres* | Tel. kom. | *Wstaw numer* |
| Email | *Wstaw adres email* |
| **Członek Zespołu {Nazwa Zespołu 1}** | Tel. praca | *Wstaw numer* |
| *Wstaw imię, nazwisko i stanowisko* | Tel. dom | *Wstaw numer* |
| *Wstaw dokładny adres* | Tel. kom. | *Wstaw numer* |
| Email | *Wstaw adres email* |
| **Członek Zespołu {Nazwa Zespołu 1}** | Tel. praca | *Wstaw numer* |
| *Wstaw imię, nazwisko i stanowisko* | Tel. dom | *Wstaw numer* |
| *Wstaw dokładny adres* | Tel. kom. | *Wstaw numer* |
| Email | *Wstaw adres email* |
| **Kierownik Zespołu {Nazwa Zespołu 2}** | Tel. praca | *Wstaw numer* |
| *Wstaw imię, nazwisko i stanowisko* | Tel. dom | *Wstaw numer* |
| *Wstaw dokładny adres* | Tel. kom. | *Wstaw numer* |
|  | Email | *Wstaw adres email* |
| **Członek Zespołu {Nazwa Zespołu 2}** | Tel. praca | *Wstaw numer* |
| *Wstaw imię, nazwisko i stanowisko* | Tel. dom | *Wstaw numer* |
| *Wstaw dokładny adres* | Tel. kom. | *Wstaw numer* |
|  | Email | *Wstaw adres email* |
| **Członek Zespołu {Nazwa Zespołu 2}** | Tel. praca | *Wstaw numer* |
| *Wstaw imię, nazwisko i stanowisko* | Tel. dom | *Wstaw numer* |
| *Wstaw dokładny adres* | Tel. kom. | *Wstaw numer* |
|  | Email | *Wstaw adres email* |

# DODATEK B – LISTA KONTAKTÓW DO DOSTAWCÓW

*W tym dodatku powinny być zawarte informacje kontaktowe dotyczące wszystkich kluczowych dostawców usług serwisowych lub wsparcia. Należy podać informacje kontaktowe, takie jak numery telefonów alarmowych, nazwiska kontaktowe, numery umów oraz reakcje umowne i lokalne godziny pracy.*

# DODATEK C – SZCZEGÓŁOWE PROCEDURY ODZYSKIWANIA

*Niniejszy dodatek zawiera szczegółowe procedury odzyskiwania systemu, które mogą obejmować takie elementy, jak:*

* *Kroki odzyskiwania na poziomie pojedynczych czynności;*
* *Instrukcje instalacji systemu z taśmy, płyty CD lub innego nośnika;*
* *Wymagane ustawienia lub zmiany konfiguracji;*
* *Odzyskiwanie danych z nośnika danych i dzienników audytu;*
* *Inne procedury odzyskiwania systemu, zależnie od przypadku.*

*Jeżeli system jest całkowicie zależny od innego systemu do odzyskiwania i odtwarzania (np. system mainframe), dostarczone informacje powinny obejmować dane kontaktowe i lokalizacje szczegółowych procedur odzyskiwania dla systemu wspierającego.*

# DODATEK D – PROCEDURY ALTERNATYWNE

*W dodatku tym należy zidentyfikować wszelkie dostępne alternatywne ręczne lub techniczne procedury przetwarzania, które pozwolą jednostce biznesowej na dalsze przetwarzanie informacji, które normalnie byłyby wykonywane przez system, którego dotyczy problem. Przykłady alternatywnych procesów obejmują ręczne przetwarzanie formularzy, wprowadzanie danych do stacji roboczych w celu przechowywania danych do momentu ich przesłania i przetworzenia lub kolejkowanie danych wejściowych*.

# DODATEK E – PLAN TESTOWANIA POPRAWNOŚCI SYSTEMU

*Ten dodatek zawiera procedury akceptacji systemu, które są wykonywane po odzyskaniu systemu i przed oddaniem go do pełnego działania i zwróceniu użytkownikom. Plan testów sprawdzania poprawności systemu może obejmować testowanie danych oraz regresję lub testy funkcjonalności przeprowadzone przed wdrożeniem aktualizacji lub zmiany systemu.*

*Przykład planu testu sprawdzania poprawności systemu:*

Po odzyskaniu systemu zostaną wykonane następujące kroki w celu sprawdzenia poprawności danych i funkcjonalności systemu:

| **Procedura** | **Oczekiwane rezultaty** | **Aktualne rezultaty** | **Czy procedura przebiegła z powodzeniem?**  **Tak/Nie** | **Wykonywana przez** |
| --- | --- | --- | --- | --- |
| W wierszu komend wprowadź: **sysname** | Zostanie wyświetlony ekran logowania do systemu |  |  |  |
| Zaloguj się jako użytkownik **testuser**, używając hasła:  **testpass** | Zostanie wyświetlony ekran początkowy z menu głównym |  |  |  |
| Z menu wybierz **5- Generate Report** | Wyświetla się ekran generowania raportów |  |  |  |
| - Wybierz **Current Date Report**  - Wybierz **Weekly**  - Wybierz **To Screen** | Raport jest generowany na ekranie z uwzględnieniem ostatniej udanej transakcji |  |  |  |
| - Wybierz **Close** | Pokazuje ekran generowania raportów |  |  |  |
| - Wybierz **Return to Main Menu** | Zostanie wyświetlony ekran początkowy z menu głównym |  |  |  |
| - Wybierz **Log-Off** | Zostanie wyświetlony ekran logowania do systemu |  |  |  |
| W wierszu komend wprowadź: **sysname** | Zostanie wyświetlony ekran logowania do systemu |  |  |  |

# DODATEK F – ALTERNATYWNE MIEJSCE PRZECHOWYWANIA DANYCH, ZAPASOWE MIEJSCE PRACY I ŚRODKI TELEKOMUNIKACJI

*Załącznik zawiera informacje dotyczące alternatywnego miejsca przechowywania danych, zapasowego miejsca przetwarzania i alternatywnych środków telekomunikacji dla systemu. W przypadku systemów o wysokim poziomie wpływu, wymagane są alternatywne informacje o pamięci, lokalizacji i telekomunikacji, zgodnie z NSC 800-53. Informacje, które należy podać dla każdego obszaru, obejmują:*

*Alternatywne miejsce do przechowywania danych:*

* *Adres alternatywnego obiektu oraz odległość od obiektu podstawowego;*
* *Informację, czy alternatywne miejsce przechowywania danych jest własnością organizacji, czy jest własnością zewnętrznego dostawcy;*
* *Nazwa i punkty kontaktowe dla alternatywnego miejsca przechowywania danych;*
* *Harmonogram i procedury dostaw nośników przeznaczonych do przekazania do alternatywnego miejsca składowania;*
* *Procedury pobierania mediów z alternatywnego miejsca przechowywania danych;*
* *Nazwiska i dane kontaktowe osób upoważnionych do pobierania nośników;*
* *Wszelkie potencjalne problemy z dostępnością do alternatywnego miejsca przechowywania danych w przypadku powszechnego zakłócenia lub katastrofy;*
* *Kroki łagodzące, umożliwiające uzyskanie dostępu do alternatywnego miejsca przechowywania w przypadku powszechnego zakłócenia lub katastrofy;*
* *Rodzaje danych znajdujących się w alternatywnym miejscu przechowywania, w tym bazy danych, oprogramowanie aplikacyjne, systemy operacyjne i inne oprogramowanie systemowe o krytycznym znaczeniu;*
* *Inne odpowiednie informacje.*

*Alternatywne miejsce przetwarzania:*

* *Adres alternatywnego (zapasowego) miejsca przetwarzania oraz odległość od miejsca głównego;*
* *Informacja o tym, czy alternatywne miejsce przetwarzania jest własnością organizacji, czy jest własnością zewnętrznego dostawcy;*
* *Nazwa i punkty kontaktowe dla alternatywnego miejsca przetwarzania;*
* *Procedury uzyskiwania dostępu do alternatywnego miejsca przetwarzania i korzystania z niego oraz dostępu do funkcji bezpieczeństwa alternatywnego miejsca przetwarzania;*
* *Nazwiska i dane kontaktowe osób upoważnionych do dostępu do alternatywnego miejsca przetwarzania;*
* *Rodzaj alternatywnego miejsca przetwarzania i sprzęt dostępny w tym miejscu;*
* *Wszelkie potencjalne problemy z dostępnością do alternatywnego miejsca przetwarzania w przypadku powszechnego zakłócenia lub katastrofy;*
* *Kroki łagodzące, umożliwiające uzyskanie dostęp do alternatywnego miejsca przetwarzania w przypadku powszechnego zakłócenia lub katastrofy;*
* *Umowy SLA lub inne umowy dotyczące korzystania z alternatywnego miejsca przetwarzania, dostępnej powierzchni biurowej / wsparcia, czasów , itp.;*
* *Inne odpowiednie informacje.*

*Środki telekomunikacji alternatywnej:*

* *Nazwa i dane kontaktowe alternatywnych dostawców usług telekomunikacyjnych;*
* *Zakontraktowana pojemność alternatywnych środków telekomunikacji;*
* *Umowy SLA lub inne umowy dotyczące wdrożenia alternatywnych zdolności telekomunikacyjnych;*
* *Nazwiska i dane kontaktowe osób upoważnionych do wdrożenia lub korzystania z alternatywnych środków telekomunikacyjnych;*
* *Inne odpowiednie informacje.*

# DODATEK G – SCHEMATY (SYSTEM I URZĄDZENIA WEJŚCIA/WYJŚCIA)

*UWAGA: Informacje w tym załączniku powinny pochodzić z Planu Bezpieczeństwa Systemu (SSP) i można je skopiować z SSP lub odnieść się do odpowiedniej sekcji w SSP i dołączyć najnowszą wersję SSP do tego planu awaryjnego. Uwzględnij architekturę systemu, urządzenia wejściowe / wyjściowe oraz inne schematy techniczne lub logiczne, które mogą być przydatne w odzyskiwaniu systemu. Schematy mogą także identyfikować informacje o połączeniach z innymi systemami.*

# DODATEK H – INWENTARYZACJA SPRZĘTU I OPROGRAMOWANIA

*Zapewnij inwentaryzację sprzętu i oprogramowania systemu. Informacje inwentarzowe powinny obejmować typ serwera lub sprzętu, na którym działa system, wymagania dotyczące procesorów i pamięci, wymagania dotyczące pamięci oraz wszelkie inne istotne szczegóły. Inwentaryzacja oprogramowania powinna identyfikować system operacyjny (w tym poziomy dodatku Service Pack lub wersji oraz wszelkie inne aplikacje niezbędne do obsługi systemu, takie jak oprogramowanie bazy danych).*

# DODATEK I – TABELA POŁĄCZEŃ

*UWAGA: Informacje w tym załączniku powinny być dostępne z Planu Bezpieczeństwa Systemu (SSP) i można je skopiować z SSP lub odnieść się do odpowiedniej sekcji w SSP i dołączyć najnowszą wersję SSP do tego planu awaryjnego. Dodatek zawiera informacje o innych systemach, które bezpośrednio łączą się lub wymieniają informacje z systemem. Informacje o połączeniu powinny obejmować rodzaj połączenia, przekazywane informacje i osobę kontaktową tego systemu.*

*Jeśli w systemie nie ma żadnych bezpośrednich połączeń, dodatek ten można usunąć lub zastosować następujące oświadczenie:*

*{Nazwa systemu}* nie łączy się bezpośrednio z żadnym innym systemem*.*

# DODATEK J – HARMONOGRAM TESTÓW I UTRZYMANIA

*Wszystkie ISCP powinny być przeglądane i testowane z częstotliwością określoną przez organizację (np. corocznie) lub za każdym razem, gdy nastąpi znacząca zmiana w systemie. Podaj informacje i harmonogram testowania systemu. W przypadku systemów o wysokim poziomie wpływu wystarczy coroczne ćwiczenie aplikacyjne. Ćwiczenie aplikacyjne powinno obejmować wszystkie punkty kontaktowe ISCP i powinno być prowadzone przez zewnętrznego lub bezstronnego obserwatora. Formalny plan testów jest opracowywany przed ćwiczeniem, w tym także opracowywane są pytania obejmujące kluczowe sekcje ISCP, w tym omówienie następujących elementów:*

* *Procedury powiadamiania;*
* *Odzyskiwanie systemu na alternatywnej platformie z nośnika kopii zapasowej;*
* *Łączność zewnętrzna i wewnętrzna;*
* *Procedury odtwarzania.*

*Wyniki testu są udokumentowane w raporcie, a wyciągnięte wnioski służą opracowaniu w celu aktualizacji informacji w ISCP.*

Oto przykład rocznego harmonogramu testów i konserwacji dla systemu o wysokim poziomie wpływu:

| **Procedura** | **Termin do** | **Osoba odpowiedzialna** | **Data planowana** | **Data odbycia** |
| --- | --- | --- | --- | --- |
| Wyznaczenie mediatora ćwiczenia | {data} | Koordynator ISCP |  |  |
| Opracowanie planu ćwiczenia | {data} | Mediator |  |  |
| Zaproszenie uczestników | {data} | Mediator |  |  |
| Odbycie ćwiczenia | {data} | Mediator, Koordynator ISCP,  PoC |  |  |
| Opracowanie wniosków z ćwiczenia | {data} | Koordynator ISCP |  |  |
| Uaktualnienie ISCP na podstawie wniosków z ćwiczenia | {data} | Koordynator ISCP |  |  |
| Zatwierdzenie i dystrybucja nowej wersji ISCP | {data} | Kierownik ISCP, Koordynator ISCP |  |  |

# DODATEK K – POWIĄZANE PLANY I PROCEDURY

*UWAGA: Informacje tej sekcji powinny być dostępne z Planu Bezpieczeństwa Systemu (SSP) i można je skopiować z SSP lub odnieść się do odpowiedniej sekcji w SSP i dołączyć najnowszą wersję SSP do tego planu awaryjnego. ISCP dla innych systemów, które łączą się ze sobą lub obsługują system, powinny zostać określone w tym dodatku. Należy odnotować najnowszą wersję ISCP, lokalizację ISCP i główny punkt kontaktowy (taki jak Koordynator ISCP).*

# DODATEK L – ANALIZA WPŁYWU NA DZIAŁALNOŚĆ (BIA)

*W tym załączniku powinny być ujęte wyniki analizy BIA.*

# DODATEK M – STRONA ZMIANY DOKUMENTU

Od ostatniego drukowania w planie wprowadzone zostały następujące zmiany:

|  |  |  |  |
| --- | --- | --- | --- |
| **Rejestr zmian** | | | |
| **Nr strony** | **Komentarz zmiany** | **Data zmiany** | **Podpis** |
|  |  |  |  |
|  |  |  |  |