

POLITYKA CIĄGŁOŚCI DZIAŁANIA

1. Wstęp i cel dokumentu

Ciągłość działania Ministerstwa Aktywów Państwowych to zdolność organizacji do utrzymania realizacji kluczowych procesów na akceptowalnym, z góry określonym poziomie, nawet w sytuacjach wystąpienia poważnych zakłóceń lub kryzysów. Cel ten realizowany jest poprzez wdrożenie skutecznych procedur reagowania oraz systemowe odzyskiwanie zasobów i infrastruktury.

Zarządzanie ciągłością działania stanowi proces kompleksowy, obejmujący systematyczną identyfikację zagrożeń, analizę ich wpływu na funkcjonowanie urzędu oraz ciągłą ocenę ryzyka. Działania te budują odporność organizacji, zapewniając skuteczną reakcję na incydenty, zabezpieczenie realizacji zadań ustawowych oraz ochronę wizerunku Ministerstwa Aktywów Państwowych jako instytucji stabilnej i wiarygodnej, przygotowanej na sytuacje kryzysowe.

Niniejsza Polityka określa ramy operacyjne dla ustanowienia, utrzymania i ciągłego doskonalenia Systemu Zarządzania Ciągłością Działania w Ministerstwie Aktywów Państwowych, który realizowany jest z uwzględnieniem wymagań i wytycznych międzynarodowych norm PN-EN ISO 22301:2020 (Bezpieczeństwo i odporność – Systemy zarządzania ciągłością działania – Wymagania) oraz PN-EN ISO 22313:2020 (Bezpieczeństwo i odporność – Systemy zarządzania ciągłością działania – Wytyczne dotyczące stosowania ISO 22301).

Głównym zadaniem Systemu zarządzania ciągłością działania jest przygotowanie Ministerstwa Aktywów Państwowych do ochrony przed negatywnym wpływem zakłóceń, minimalizacja potencjalnych strat oraz sprawne przywracanie procesów głównych (krytycznych) i wspierających (pomocniczych) poprzez ograniczenie prawdopodobieństwa wystąpienia incydentów oraz zapewnienie gotowości do sprawnego odzyskiwania zdolności operacyjnej. System Zarządzania Ciągłością Działania stanowi fundament odporności państwa w obszarze właściwości Ministra Aktywów Państwowych.

2. Deklaracja kierownictwa

Kierownictwo Ministerstwa Aktywów Państwowych zapewnia skuteczność Systemu Zarządzania Ciągłością Działania oraz deklaruje wsparcie dla inicjatyw budujących odporność organizacji, w szczególności poprzez:

- 1) zapewnienie zasobów kadrowych, technicznych i finansowych niezbędnych do funkcjonowania oraz ciągłego doskonalenia Systemu Zarządzania Ciągłością Działania;
- 2) sprawowanie nadzoru nad mechanizmami ochrony informacji, aktywów oraz kluczowych procesów Ministerstwa Aktywów Państwowych;
- 3) kształtowanie kultury organizacyjnej zorientowanej na odporność operacyjną i gotowość do reagowania na incydenty;
- 4) wspieranie pracowników w realizacji zadań z zakresu ciągłości działania;
- 5) systematyczne podnoszenie świadomości i kompetencji pracowników w obszarze procedur odtwarzania oraz bezpieczeństwa informacji.

3. Użyte skróty i określenia

- 1) analiza wpływu biznesowego (BIA – ang. Business Impact Analysis) – proces polegający na identyfikacji kluczowych funkcji organizacji oraz ocenie skutków: finansowych, operacyjnych, prawnych, a także wizerunkowych, jakie mogą wystąpić w wyniku ich zakłócenia;
- 2) gotowość operacyjna – zdolność zespołu/ów, systemu/ów lub organizacji do podjęcia działań i wykonywania swoich funkcji zgodnie z założeniami, na wstępnym lub pełnym poziomie;
- 3) kierownictwo – minister, sekretarze stanu, podsekretarze stanu, dyrektor generalny oraz szef Gabinetu Politycznego;
- 4) kierujący komórką organizacyjną – dyrektor departamentu lub biura, a w przypadku nieobecności osoba wyznaczona do jego zastępowania;
- 5) Ministerstwo – Ministerstwo Aktywów Państwowych;
- 6) plany ciągłości działania – udokumentowane procedury określające zasady reagowania i odzyskiwania zdolności operacyjnej w sytuacjach kryzysowych;
- 7) pracownik – osoba zatrudniona w Ministerstwie bez względu na zajmowane stanowisko, wymiar czasu pracy oraz podstawę nawiązania stosunku pracy;
- 8) proces – uporządkowany zbiór działań wzajemnie powiązanych lub oddziałujących, które przekształcają wejścia (dane, zasoby) w określone wyjścia (wyniki, decyzje, usługi);

- 9) proces główny (krytyczny) – proces o najwyższym priorytecie dla funkcjonowania Ministerstwa, którego przerwanie lub nienależyta realizacja uniemożliwiłaby wypełnianie zadań ustawowych i statutowych, generując nieakceptowalne skutki prawne, społeczne, finansowe lub wizerunkowe;
- 10) proces wspierający (pomocniczy) – proces zapewniający zasoby, narzędzia i warunki niezbędne do prawidłowego przebiegu procesów głównych, a w sytuacjach wystąpienia zakłóceń umożliwiając ich sprawne odtworzenie oraz utrzymanie na zdefiniowanym poziomie operacyjnym;
- 11) punkt odtworzenia danych (RPO – ang. Recovery Point Objective) – akceptowalny poziom utraty danych wyrażony w czasie, po przekroczeniu którego realizacja procesu będzie niemożliwa lub poważnie zakłócona;
- 12) scenariusz zdarzeń – opis najbardziej dotkliwych oraz prawdopodobnych zagrożeń, które w momencie wystąpienia mogą doprowadzić do całkowitego przerwania realizacji procesów głównych (krytycznych) i stanowią podstawę do opracowania strategii ciągłości działania;
- 13) SZCD – System Zarządzania Ciągłością Działania;
- 14) testy – zaplanowane działania mające na celu praktyczną weryfikację skuteczności planów ciągłości działania oraz dostępności i sprawności niezbędnych zasobów;
- 15) wymagany czas odtworzenia procesu (RTO – ang. Recovery Time Objective) – maksymalny dopuszczalny czas, w jakim należy wznowić proces przerwany w wyniku zakłócenia działalności, stanowiący kluczowy element planów ciągłości działania, wyznaczający ramy czasowe dla procedur odzyskiwania zasobów oraz infrastruktury;
- 16) Zespół – Zespół zarządzania ciągłością działania w Ministerstwie Aktywów Państwowych z uwzględnieniem Normy ISO 22301.

4. Odpowiedzialność i role

Kierownictwo:

- 1) ustanawia i dokonuje cyklicznego przeglądu Polityki, wyznaczając kierunki rozwoju SZCD;
- 2) zapewnia niezbędne zasoby (finansowe, kadrowe, technologiczne) oraz promuje kulturę odporności organizacyjnej;
- 3) odpowiada za komunikowanie znaczenia skutecznego SZCD;
- 4) nadzoruje proces identyfikacji ryzyk strategicznych oraz zatwierdza wyniki analizy wpływu na biznes (BIA), wyznaczając akceptowalne czasy przestoju (RTO/RPO).

Zespół:

- 1) zapewnia spójność i kompletność dokumentacji SZCD;
- 2) koordynuje przeprowadzanie cyklicznych testów (w tym testów komunikacyjnych i technicznych), opracowuje ich harmonogram oraz zbiorcze raporty z wnioskami;
- 3) monitoruje postępy prac w komórkach organizacyjnych, sprawuje bieżący nadzór nad poprawnością procedur i dokonuje okresowych przeglądów SZCD;
- 4) definiuje zakres merytoryczny szkoleń oraz wspiera merytorycznie kierujących komórkami organizacyjnymi w opracowywaniu planów ciągłości.

Kierujący komórkami organizacyjnymi:

- 1) identyfikują i priorytetyzują procesy kluczowe w podległych obszarach oraz wyznaczają osoby do ról krytycznych w SZCD;
- 2) odpowiadają za opracowanie, regularną aktualizację i realność planów ciągłości działania, w tym zapewnienie ich drożności w sytuacjach kryzysowych;
- 3) zapewniają realizację testów procedur komunikacyjnych w swoich obszarach, gwarantując aktualność danych kontaktowych i sprawność kanałów powiadamiania;
- 4) budują świadomość operacyjną podległych pracowników, włączając zagadnienia ciągłości działania do codziennej pracy.

Osoby pełniące role przypisane w SZCD:

- 1) odpowiadają za czynny udział w testach, ćwiczeniach i symulacjach, weryfikując praktyczną użyteczność procedur;
- 2) realizują zadania wynikające z planów operacyjnych, w tym procedury komunikacyjne koordynowane przez Zespół;
- 3) uczestniczą w procesie doskonalenia SZCD poprzez raportowanie luk, ryzyk i propozycji usprawnień po każdym teście lub wystąpieniu incydentu.

Pracownicy:

- 1) utrzymują indywidualną gotowość do działania w warunkach nadzwyczajnych, znając swoje miejsce w strukturze;
- 2) realizują zadania zgodnie z planami ciągłości w ramach posiadanych uprawnień i kompetencji;
- 3) uczestniczą w szkoleniach i testach, dbają o aktualność swoich danych kontaktowych w systemach kadrowych i alarmowych;
- 4) niezwłocznie raportują wszelkie zdarzenia, anomalie lub zagrożenia (w tym próby cyberataków), które mogą wpłynąć na stabilność procesów Ministerstwa.

5. Elementy i etapy działań związane z wdrażaniem SZCD

SZCD obejmuje wszystkie komórki organizacyjne Ministerstwa. Proces wdrażania SZCD realizowany jest poprzez następujące działania:

- 1) **określenie kontekstu organizacji** – identyfikacja wewnętrznych i zewnętrznych czynników wpływających na zdolność Ministerstwa do realizacji zadań statutowych;
- 2) **zapewnienie zasobów i kompetencji** – zdefiniowanie ról w strukturze SZCD, przypisanie pracownikom konkretnych uprawnień i odpowiedzialności oraz zapewnienie szkoleń podnoszących świadomość i umiejętności operacyjne;
- 3) **inwentaryzacja i identyfikacja procesów** – inwentaryzacja procesów realizowanych w komórkach organizacyjnych wraz z ich powiązaniem oraz podział na procesy główne (krytyczne) i procesy pomocnicze (wspierające);
- 4) **analiza wpływu biznesowego na ciągłość działania (BIA)** – ocena skutków przerwania procesów w czasie, mająca na celu wytypowanie procesów głównych (krytycznych) oraz wyznaczenie priorytetów odtwarzania oraz parametrów czasowych;
- 5) **analiza ryzyka** – identyfikacja i ocena zagrożeń dla procesów głównych (krytycznych) oraz określenie prawdopodobieństwa wystąpienia zdarzeń naruszających ciągłość działania wraz z ich skutkami;
- 6) **strategia ciągłości działania** – wybór optymalnych wariantów postępowania, które pozwolą na utrzymanie lub odtworzenie procesów głównych (krytycznych) na akceptowalnym poziomie;
- 7) **opracowanie planów i procedur ciągłości działania** – opracowanie szczegółowych procedur określających działania w przypadku wystąpienia zakłócenia;
- 8) **system ostrzegania i komunikacji** – ustanowienie kanałów i procedur przepływu informacji wewnątrz Ministerstwa oraz pomiędzy Ministerstwem i interesariuszami zewnętrznymi w sytuacjach kryzysowych;
- 9) **utrzymanie, doskonalenie i weryfikacja SZCD** – regularne testowanie skuteczności planów, aktualizacja dokumentacji oraz jego przeglądy w celu zapewnienia ciągłej adekwatności do zmieniającego się otoczenia.

5.1. Określenie kontekstu organizacji

Kontekst organizacji stanowi fundament SZCD i obejmuje analizę czynników wewnętrznych oraz zewnętrznych, które mają istotny wpływ na zdolność Ministerstwa do osiągnięcia celów strategicznych oraz niezakłóconej realizacji polityki państwa w obszarze

działów administracji rządowej: aktywa państwowe i łączność, a także w zakresie zamawiania usług na potrzeby własne.

W ramach monitorowania kontekstu uwzględnia się w szczególności:

- 1) **czynniki zewnętrzne** – uwarunkowania pochodzące z otoczenia zewnętrznego, mogące stanowić dla Ministerstwa zagrożenia lub szanse, w tym czynniki np. prawne i polityczne, technologiczne i gospodarcze oraz społeczne;
- 2) **czynniki wewnętrzne** – uwarunkowania związane z samą organizacją Ministerstwa, podlegające jego bezpośredniej kontroli, w tym czynniki np. struktura organizacyjna, zasoby ludzkie i techniczne oraz procesy operacyjne.

Kontekst organizacji podlega regularnemu przeglądowi, dokonywanemu nie rzadziej niż raz w roku przez Zespół. Ma to na celu zapewnienie, że kontekst organizacji pozostaje adekwatny do aktualnej sytuacji operacyjnej oraz zmieniającego się otoczenia, w którym funkcjonuje Ministerstwo.

5.2. Zapewnienie zasobów i kompetencji

Skuteczne funkcjonowanie SZCD wymaga od kierujących komórkami organizacyjnymi wyznaczenia pracowników do ról zdefiniowanych w SZCD, wraz z precyzyjnym określeniem ich uprawnień i zakresów odpowiedzialności. Kierujący posiadają elastyczność w dostosowywaniu struktur zarządzania ciągłością działania do specyfiki realizowanych zadań.

Ministerstwo zapewnia – uwzględniając rekomendacje Zespołu – regularne podnoszenie kompetencji pracowników w celu zwiększenia skuteczności działań w sytuacjach zakłóceń. Programy szkoleniowe obejmują wszystkich zatrudnionych, ze szczególnym uwzględnieniem osób pełniących kluczowe role w planach ciągłości działania.

Zaleca się różnicowanie zakresu szkoleń w zależności od pełnionej roli w strukturze odporności Ministerstwa:

- 1) **szkolenia dla kierownictwa** – ukierunkowane na uświadomienie znaczenia zarządzania ciągłością działania, niezbędność aktywnego zaangażowania w procesy decyzyjne oraz wskazanie zakresu odpowiedzialności za budowanie odporności organizacji;
- 2) **szkolenia specjalistyczne** – przeznaczone dla osób pełniących kluczowe funkcje w strukturze zarządzania ciągłością działania (np. kierujący komórkami organizacyjnymi, koordynatorzy, członkowie Zespołu), koncentrujące się na procedurach operacyjnych i technikach reagowania kryzysowego oraz metodyce BIA i analizie ryzyka;

- 3) **szkolenia ogólne** – skierowane do wszystkich pracowników Ministerstwa, mające na celu budowanie świadomości w zakresie ciągłości działania, znajomości podstawowych procedur bezpieczeństwa oraz zasad komunikacji w sytuacjach awaryjnych.

5.3. Inwentaryzacja i identyfikacja procesów

Identyfikacja procesów polega na systematycznym zidentyfikowaniu i opisanu wszystkich działań realizowanych w Ministerstwie, w celu określenia ich wpływu na odporność operacyjną urzędu.

Procesy realizowane w Ministerstwie podlegają klasyfikacji na:

- 1) **procesy główne (krytyczne)** – kluczowe działania merytoryczne, do realizacji których Ministerstwo zostało powołane na podstawie przepisów prawa; ich zakłócenie bezpośrednio uniemożliwia wypełnianie misji publicznej i zadań ustawowych;
- 2) **procesy wspierające (pomocnicze)** – działania zapewniające niezbędne zasoby kadrowe, technologiczne, logistyczne, finansowe i prawne niezbędne do prawidłowego przebiegu procesów głównych.

Celem utrzymania procesów wspierających jest zapewnienie zdolności Ministerstwa do kontynuowania misji podstawowej w sytuacjach zagrożenia, przy wykorzystaniu zasobów własnych oraz wsparcia podmiotów zewnętrznych, wynikającego z zawartych umów i porozumień.

Za rzetelną identyfikację, opisanie oraz cykliczną aktualizację wykazu procesów w podległych obszarach merytorycznych odpowiadają kierujący komórkami organizacyjnymi. W ramach inwentaryzacji należy każdorazowo określić:

- 1) **właściciela procesu** – osobę odpowiedzialną za nadzór nad przebiegiem i skutecznością danego działania;
- 2) **wzajemne zależności** – wpływ zakłócenia lub zatrzymania jednego procesu na możliwość realizacji pozostałych zadań wewnątrz Ministerstwa;
- 3) **powiązania zewnętrzne** – zależności od usług i danych dostarczanych przez inne organy administracji publicznej oraz dostawców zewnętrznych;
- 4) **wymagane zasoby** – minimalne zestawienie kadrowe, systemów IT, danych oraz infrastruktury niezbędnej do realizacji procesu na poziomie akceptowalnym.

5.4. Analiza wpływu biznesowego na ciągłość działania (BIA)

Analiza wpływu biznesowego (BIA) jest kluczowym elementem SZCD, służącym do identyfikacji procesów głównych (krytycznych) oraz zasobów niezbędnych do ich utrzymania lub niezwłocznego wznowienia w sytuacjach zakłóceń.

Głównym celem analizy BIA jest:

- 1) **szacowanie skutków** – określenie wpływu przerwania procesów (prawnych, operacyjnych, finansowych, wizerunkowych oraz społecznych) w określonych przedziałach czasowych;
- 2) **wyznaczenie parametrów czasowych odtwarzania**, w tym w RTO, RPO;
- 3) **określenie zasobów krytycznych** – wskazanie minimalnej liczby pracowników, systemów IT, infrastruktury oraz kluczowych dostawców niezbędnych do realizacji procesu na poziomie akceptowalnym.

Analiza BIA stanowi podstawę do opracowania strategii ciągłości działania oraz projektowania adekwatnych rozwiązań technicznych i organizacyjnych.

Kierujący komórkami organizacyjnymi przeprowadzają analizę BIA w podległych im obszarach zgodnie z wytycznymi międzynarodowego standardu ISO/TS 22317:2021 oraz wewnętrzną metodyką Ministerstwa. Wyniki analizy podlegają regularnej aktualizacji (nie rzadziej niż raz w roku) oraz każdorazowo w przypadku istotnych zmian w strukturze lub zadaniach Ministerstwa.

5.5. Analiza ryzyka

Analiza ryzyka to proces systematycznej identyfikacji źródeł zagrożeń oraz szacowania ich wpływu na procesy główne (krytyczne) i zasoby niezbędne do ich realizacji. Stanowi ona fundament budowania odporności Ministerstwa oraz zdolności do skutecznej reakcji w obszarach:

- 1) ochrony interesów Skarbu Państwa oraz ciągłości realizacji zadań publicznych;
- 2) gwarancji ciągłości i płynności kluczowych procesów Ministerstwa;
- 3) minimalizacji strat związanych z odtworzeniem procesów i zasobów;
- 4) zarządzania wizerunkiem i reputacją Ministerstwa jako instytucji stabilnej;
- 5) zapewnienia zgodności (ang. compliance) – unikania konsekwencji prawnych wynikających z niewykonania obowiązujących przepisów.

Analiza ryzyka wspiera proces decyzyjny poprzez:

- 1) planowanie i wdrożenie środków zapobiegawczych, ograniczających prawdopodobieństwo wystąpienia zagrożenia;
- 2) wyznaczenie poziomu ryzyka dla poszczególnych grup zasobów oraz nadanie im priorytetów w działaniach mitygacyjnych (łagodzących);

- 3) opracowanie scenariuszy zdarzeń, umożliwiających wdrożenie adekwatnych rozwiązań proceduralnych, organizacyjnych i technicznych dostosowanych do skali potencjalnych zagrożeń.

Precyzyjne określenie wpływu poszczególnych zagrożeń na ciągłość procesów głównych (krytycznych), a także zdefiniowanie scenariuszy zdarzeń, umożliwia usystematyzowanie istniejących i wdrożenie nowych rozwiązań proceduralnych, organizacyjnych i technicznych w zakresie ciągłości działania, adekwatnych do skali prawdopodobnych zdarzeń.

5.6. Strategia ciągłości działania

Celem Strategii ciągłości działania jest:

- 1) zdefiniowanie metod zabezpieczenia i odtworzenia procesów głównych (krytycznych) oraz zasobów niezbędnych do ich realizacji (przywrócenie działań priorytetowych w ustalonych ramach czasowych zdefiniowanych w analizie BIA i na uzgodnionym poziomie wydajności operacyjnej);
- 2) wskazanie najskuteczniejszych środków zapobiegawczych (prewencyjnych i mitygujących) mających na celu minimalizację prawdopodobieństwa wystąpienia zakłóceń, skrócenie czasu ich trwania oraz ograniczenie negatywnego wpływu na realizację zadań ustawowych.

Strategia ciągłości działania określa wymagania dotyczące zasobów niezbędnych do realizacji procesów głównych (krytycznych). Rodzaje zasobów powinny uwzględniać, w szczególności:

- 1) zasoby ludzkie – pracownicy posiadający kluczowe kompetencje, systemy zastępstw oraz wsparcie specjalistyczne;
- 2) informacje i dane – dokumentacja papierowa i elektroniczna, bazy danych, archiwa oraz rejestry publiczne;
- 3) infrastruktura fizyczna – budynki, lokalizacje zapasowe, alternatywne miejsca pracy oraz zabezpieczenia techniczne obiektów;
- 4) systemy teleinformatyczne – aplikacje merytoryczne, infrastruktura sieciowa, bezpieczna łączność oraz kopie zapasowe;
- 5) logistyka i łańcuch dostaw – transport, dostawy krytyczne oraz usługi świadczone przez podmioty zewnętrzne;
- 6) zasoby finansowe – zapewnienie płynności finansowej oraz dostępu do środków niezbędnych do finansowania działań ratunkowych i odtworzeniowych;

- 7) wyposażenie rzeczowe – specjalistyczny sprzęt biurowy, materiały eksploatacyjne oraz środki ochrony.

W sytuacji wystąpienia zagrożenia kierujący komórkami organizacyjnymi realizują procesy główne (krytyczne), wykorzystując dostępne zasoby oraz funkcjonujące mechanizmy operacyjne, w tym zarządzenia, procedury i instrukcje stanowiskowe.

5.7. Opracowanie planów i procedur ciągłości działania

Minister, działając poprzez kierujących komórkami organizacyjnymi, dokumentuje i utrzymuje plany oraz procedury ciągłości działania. Zawierają one wytyczne dotyczące wczesnego ostrzegania, komunikacji oraz reagowania na zakłócenia w celu przywrócenia pełnej sprawności operacyjnej urzędu. Celem planów jest zapewnienie realizacji procesów krytycznych na akceptowalnym poziomie minimalnym oraz ich pełne odtworzenie w zdefiniowanym czasie (RTO), przy zachowaniu dopuszczalnego poziomu utraty danych (RPO).

Plan ciągłości działania określa w szczególności:

- 1) procedury reagowania – szczegółowy sposób postępowania w przypadku wystąpienia zakłócenia, w tym: mierzalne kryteria uruchomienia planu, opis czynności, ramy czasowe ich realizacji, zasady koordynacji i komunikacji oraz kryteria zakończenia działań awaryjnych;
- 2) strukturę osobową – wskazanie osób odpowiedzialnych za realizację poszczególnych działań wraz z precyzyjnym przypisaniem im ról i zakresów odpowiedzialności oraz danych kontaktowych;
- 3) zasoby krytyczne – wykaz niezbędnej infrastruktury, systemów IT, danych oraz materiałów technicznych i logistycznych wymaganych i niezbędnych do podtrzymania procesów;
- 4) zależności i wsparcie – identyfikację powiązań międzyprocesowych oraz wskazanie procesów pomocniczych niezbędnych do nieprzerwanego funkcjonowania procesów głównych (krytycznych);
- 5) zasady sprawozdawczości – wymogi i kanały dotyczące raportowania przebiegu działań ratunkowych oraz postępów w procesie odtwarzania;
- 6) procedurę powrotu (dezaktywacji) – zasady bezpiecznego wycofania się z rozwiązań awaryjnych i płynnego przywrócenia standardowego trybu pracy (tzw. powrotu do normalności).

Plany ciągłości działania są aktywowane niezwłocznie po wystąpieniu zdarzeń naruszających stabilność procesów głównych (krytycznych). W sytuacjach niestandardowych,

nieobjętych istniejącymi scenariuszami, dopuszcza się wdrożenie rozwiązań doraźnych w formie awaryjnych planów ciągłości działania. Ich celem jest zapewnienie tymczasowego bezpieczeństwa realizacji kluczowych zadań Ministerstwa do czasu stabilizacji sytuacji lub wdrożenia docelowych mechanizmów odtworzeniowych w momencie wystąpienia zdarzeń naruszających stabilność procesów głównych (krytycznych).

5.8. System ostrzegania i komunikacja

Tworząc SZCD, należy precyzyjnie określić procedury komunikacji wewnętrznej i zewnętrznej.

Procedury komunikacji określają, w szczególności:

- 1) sposoby i narzędzia komunikacji – z podziałem na komunikację wewnętrzną (pracownicy, kierownictwo) oraz zewnętrzną (interesariusze, dostawcy kluczowych usług, organy nadzorcze, media);
- 2) strukturę odpowiedzialności – wskazanie osób uprawnionych do inicjowania procesów komunikacyjnych oraz pełnienia funkcji rzecznika w sytuacjach kryzysowych;
- 3) hierarchię środków komunikacyjnych – wykaz kanałów podstawowych (np. poczta elektroniczna, komunikatory służbowe) oraz awaryjnych (np. systemy powiadamiania masowego, telefony satelitarne, alternatywne serwery łączności);
- 4) zasady przekazywania informacji – określenie zakresu danych podlegających komunikowaniu, sytuacji wymagających reakcji oraz zdefiniowanie grup odbiorców (komu, co i w jaki sposób przekazywać).

Zespół koordynuje przeprowadzanie cyklicznych testów procedur komunikacyjnych, natomiast kierujący komórkami organizacyjnymi zapewniają ich realizację w podległych im obszarach w celu weryfikacji drożności kanałów łączności oraz aktualności danych kontaktowych.

5.9. Utrzymanie, doskonalenie i weryfikacja SZCD

Utrzymanie i doskonalenie SZCD jest ciągłym procesem zapewniającym zdolność Ministerstwa do skutecznego reagowania na zakłócenia oraz terminowego wznawiania procesów głównych (krytycznych). Proces ten obejmuje systematyczną identyfikację ryzyk, aktualizację analizy wpływu biznesowego (BIA), opracowywanie i aktualizację planów ciągłości działania oraz szkolenia pracowników. Celem tych działań jest utrzymanie odporności operacyjnej na poziomie akceptowalnym przez Kierownictwo.

Zaleca się systematyczną weryfikację aktualności dokumentacji Ministerstwa, która wpływa na bezpieczeństwo i odporność organizacji. Dokumentacja ta, w szczególności plany awaryjne, instrukcje operacyjne oraz plany ochrony obiektów, musi być spójna z procedurami SZCD. Proces weryfikacji ma na celu potwierdzenie zgodności przyjętych rozwiązań z otoczeniem prawnym oraz zapewnienie pełnej korelacji dokumentacji operacyjnej z planami ciągłości działania.

Cykliczne testowanie rozwiązań zawartych w planach ciągłości działania stanowi podstawowe narzędzie weryfikacji skuteczności SZCD. Testy dostarczają wiarygodnych informacji o stanie gotowości Ministerstwa, pozwalają ocenić adekwatność planów do zmieniających się procesów i otoczenia oraz minimalizują ryzyko wystąpienia strat.

Testy mogą być przeprowadzane w formie ćwiczeń symulacyjnych, testów stolikowych lub testów pełnych i mogą dotyczyć całego systemu lub jego wybranych elementów (np. procedur komunikacyjnych).

Zasady przeprowadzania testów:

- 1) częstotliwość przeprowadzania testów – testy przeprowadza się co najmniej raz w roku kalendarzowym lub niezwłocznie po wprowadzeniu istotnych zmian organizacyjnych lub technologicznych;
- 2) scenariusze – testy realizowane są na podstawie aktualnych scenariuszy, uwzględniających najbardziej dotkliwe i prawdopodobne zagrożenia zidentyfikowane w analizie ryzyka;
- 3) raportowanie – każdy test kończy się sporządzeniem raportu dla kierownictwa, zawierającego ocenę skuteczności działań oraz wykaz stwierdzonych luk i nieprawidłowości;
- 4) działania korygujące – na podstawie raportu formułowane są rekomendacje, które wskazują osoby odpowiedzialne za wdrożenie zmian oraz terminy ich realizacji.

6. Aktualizacja i przegląd SZCD

Aktualizacji SZCD dokonuje się niezwłocznie w przypadku wystąpienia istotnych zmian wpływających na odporność operacyjną Ministerstwa, w szczególności w przypadku:

- 1) zmiany kontekstu organizacji lub struktury organizacyjnej;
- 2) zmiany siedziby lub lokalizacji kluczowych zasobów technicznych;
- 3) modyfikacji systemów teleinformatycznych wspierających procesy główne (krytyczne);
- 4) zmian w strukturze zarządzania lub sposobie realizacji zadań ustawowych;
- 5) identyfikacji luk w wyniku przeprowadzonych testów, ćwiczeń lub realnych incydentów.

Przegląd SZCD służy systematycznej weryfikacji jego spójności, kompletności oraz skuteczności.

W ramach przeglądu ocenie podlegają w szczególności:

- 1) poprawność i aktualność identyfikacji procesów głównych (krytycznych) oraz analizy BIA;
- 2) adekwatność przyjętych scenariuszy zakłóceń oraz ich potencjalnego wpływu na Ministerstwo;
- 3) skuteczność struktur zarządzania oraz podmiotów zaangażowanych w SZCD;
- 4) realność osiągnięcia założonych parametrów ciągłości działania w tym czasów odtworzenia (RTO);
- 5) poziom przygotowania oraz świadomości pracowników w zakresie stosowania procedur awaryjnych;
- 6) stopień wdrożenia rekomendacji z poprzednich przeglądów, audytów oraz wniosków z przeprowadzonych testów.

Przegląd SZCD dokonuje się okresowo, nie rzadziej niż raz w roku kalendarzowym, lub każdorazowo w przypadku wystąpienia istotnych zmian organizacyjnych lub technologicznych.