

PLAN CIĄGŁOŚCI DZIAŁANIA NA WYPADEK DYSFUNKCJI SYSTEMU INFORMATYCZNEGO

BIBLIOTEKA PUBLICZNA W BISZTYNKU

CEL PROCEDURY

§ 1

1. Celem niniejszej Procedury jest zapewnienie systemowego i uporządkowanego podejścia do zarządzania incydentami oraz zakłóceniami w funkcjonowaniu systemów teleinformatycznych, w taki sposób, aby ograniczyć ich negatywny wpływ na realizację działalności statutowej jednostki.

Procedura ma na celu w szczególności minimalizację skutków dysfunkcji systemów informatycznych poprzez zapewnienie ciągłości działania procesów biznesowych, utrzymanie wymaganej dostępności, integralności oraz poufności przetwarzanych informacji, a także skrócenie czasu reakcji na występujące incydenty i ich skuteczne usuwanie.

W ramach realizacji powyższego celu Procedura określa zasady identyfikacji, rejestrowania, klasyfikacji, analizy oraz obsługi incydentów, jak również przypisuje odpowiedzialności w zakresie reagowania na zdarzenia mogące zakłócić prawidłowe funkcjonowanie systemów teleinformatycznych.

Dodatkowo celem Procedury jest ograniczenie ryzyka powtarzalności incydentów poprzez analizę ich przyczyn źródłowych oraz wdrażanie działań korygujących i zapobiegawczych, a także zapewnienie zgodności działań jednostki z obowiązującymi przepisami prawa oraz wewnętrznymi regulacjami w obszarze bezpieczeństwa informacji.

Procedura wspiera również budowanie świadomości pracowników w zakresie cyberbezpieczeństwa oraz zapewnia podstawy do prowadzenia monitoringu, raportowania i doskonalenia systemu zarządzania bezpieczeństwem informacji w jednostce.

PRZEDMIOT

§ 2

1. Przedmiotem niniejszej Procedury jest określenie zasad, trybu oraz odpowiedzialności w zakresie postępowania w przypadku wystąpienia zdarzeń mających rzeczywisty lub potencjalny wpływ na bezpieczeństwo informacji oraz ciągłość działania jednostki.
 - a. Procedura obejmuje w szczególności działania związane z identyfikacją, zgłaszaniem, analizą oraz obsługą incydentów i zakłóceń w funkcjonowaniu systemów teleinformatycznych, a także określa zasady przywracania prawidłowego funkcjonowania procesów biznesowych.
 - b. Postanowienia niniejszej Procedury mają zastosowanie do wszystkich pracowników, współpracowników oraz innych osób mających dostęp do zasobów informacyjnych jednostki, niezależnie od formy zatrudnienia lub współpracy.

ZAKRES STOSOWANIA

§ 3

1. Zakres stosowania niniejszej Procedury obejmuje wszystkie systemy teleinformatyczne, zasoby informacyjne oraz procesy przetwarzania danych wykorzystywane w działalności jednostki.
2. Procedura określa i definiuje działania, jakie należy podjąć w przypadku wystąpienia dysfunkcji systemu informatycznego, incydentu cyberbezpieczeństwa lub innego zdarzenia mogącego wpłynąć na bezpieczeństwo informacji lub ciągłość działania.
3. Zakres Procedury obejmuje w szczególności:
 - a) identyfikację i klasyfikację zdarzeń;
 - b) zasady eskalacji incydentów;
 - c) przypisanie odpowiedzialności za podejmowanie działań;
 - d) sposób reagowania i przywracania ciągłości działania;
 - e) działania korygujące i zapobiegawcze.

ODPOWIEDZIALNOŚĆ I UPRAWNIENIA

§ 4

1. Odpowiedzialność za funkcjonowanie niniejszej Procedury kształtuje się następująco:

- a) za opracowanie, aktualizację oraz utrzymanie niniejszego planu ciągłości działania odpowiada Administrator Danych Osobowych.
- b) za nadzór nad wdrożeniem, stosowaniem oraz doskonaleniem niniejszego planu ciągłości działania odpowiada osoba posiadająca uprawnienia do zarządzania systemem informatycznym.
- c) za podejmowanie decyzji strategicznych w sytuacjach incydentów oraz uruchomienie planu ciągłości działania odpowiada Administrator Danych Osobowych (ADO), działający samodzielnie lub w porozumieniu z IOD i/lub osobą posiadającą uprawnienia do zarządzania systemem informatycznym;
- d) za realizację działań operacyjnych przewidzianych w niniejszym planie odpowiadają osoby wskazane w Procedurze, zgodnie z przypisanymi im rolami i kompetencjami;
- e) wszyscy pracownicy oraz współpracownicy jednostki zobowiązani są do niezwłocznego zgłaszania zdarzeń mogących stanowić incydent cyberbezpieczeństwa oraz do współpracy przy ich obsłudze.

Uprawnienia osób wskazanych w niniejszym paragrafie obejmują dostęp do niezbędnych zasobów, informacji oraz systemów w zakresie wymaganym do skutecznej realizacji działań związanych z obsługą incydentów i zapewnieniem ciągłości działania.

OPIS POSTĘPOWANIA

§ 5

1. Warunki uruchomienia planu

2. Plan ciągłości działania uruchamiany jest w przypadku wystąpienia zdarzenia powodującego lub mogącego powodować dysfunkcję systemu informatycznego, która ma istotny wpływ na ciągłość działania jednostki, w szczególności w przypadku:

- a) niedostępności kluczowych systemów;
- b) utraty lub uszkodzenia danych;
- c) naruszenia bezpieczeństwa informacji;
- d) zakłócenia realizacji podstawowych procesów biznesowych.

3. Decyzja o uruchomieniu planu

- a) Decyzję o uruchomieniu planu podejmuje Administrator Danych Osobowych (ADO), samodzielnie lub w porozumieniu z Inspektorem Ochrony Danych (IOD) oraz/lub osobą posiadającą uprawnienia do zarządzania systemem informatycznym
- b) W przypadku braku możliwości kontaktu z ADO, decyzję może podjąć osoba posiadająca uprawnienia do zarządzania systemem informatycznym, kierując się oceną wpływu zdarzenia na ciągłość działania oraz bezpieczeństwo informacji.

4. Osoby i zasoby wymagane do realizacji planu

- a) W realizację planu zaangażowane są osoby pełniące kluczowe funkcje w obszarze bezpieczeństwa informacji oraz utrzymania systemów teleinformatycznych, w szczególności ADO, osoba posiadająca uprawnienia do zarządzania systemem informatycznym oraz inne osoby wyznaczone do realizacji określonych zadań.
- b) Do realizacji planu wykorzystuje się dostępne zasoby techniczne i organizacyjne, w tym systemy zapasowe, kopie bezpieczeństwa, alternatywne kanały komunikacji oraz dokumentację operacyjną.
- c) Zakres wykorzystania zasobów oraz przydział zadań powinien być adekwatny do skali i charakteru zdarzenia, z uwzględnieniem konieczności zapewnienia ciągłości działania kluczowych procesów jednostki.

Działania podejmowane w ramach realizacji planu powinny być dokumentowane, a po zakończeniu incydentu należy przeprowadzić analizę jego przebiegu oraz wdrożyć ewentualne działania korygujące i zapobiegawcze.

DZIAŁANIA ZAPEWNIAJĄCE PRZYWRÓCENIE ZDOLNOŚCI REALIZACJI DZIAŁALNOŚCI STATUTOWEJ

§ 6

FUNKCJA / ETAP	OPIS DZIAŁAŃ	WYMAGANE ZASOBY / ODPOWIEDZIALNOŚĆ
WERYFIKACJA ZASADNOŚCI ZGŁOSZENIA	Dokonanie wstępnej analizy zgłoszenia przekazanego przez użytkownika w celu potwierdzenia, czy dotyczy ono zdarzenia związanego z dysfunkcją systemu informatycznego. Weryfikacja obejmuje analizę objawów, zakresu problemu oraz jego potencjalnego wpływu na funkcjonowanie jednostki.	Zapewnienie dostępu do infrastruktury informatycznej na stanowisku użytkownika, z którego pochodzi zgłoszenie. Odpowiedzialny: ADO
IDENTYFIKACJA ŹRÓDŁA AWARII	Ustalenie przyczyny zdarzenia poprzez analizę dostępnych informacji oraz diagnostykę techniczną. W szczególności należy określić, czy awaria wynika z: przerwy w zasilaniu, braku dostępu do sieci Internet, uszkodzenia sprzętu, błędów aplikacji lub systemu operacyjnego.	Zapewnienie dostępu do serwerowni oraz urządzeń objętych awarią. Zapewnienie możliwości kontaktu z personelem technicznym oraz osobami posiadającymi dostęp do pomieszczeń.
OKREŚLENIE SKALI AWARII	Ocena zakresu oddziaływania incydentu na działalność jednostki, w tym ustalenie, czy awaria dotyczy pojedynczego stanowiska, czy całej jednostki. Wynik oceny wpływa na dalsze decyzje operacyjne i priorytety działań.	Zapewnienie kontaktu z kluczowymi pracownikami poszczególnych komórek organizacyjnych. Odpowiedzialny: ADO

OCENA MOŻLIWOŚCI KONTYNUACJI DZIAŁANIA W DOTYCHCZASOWEJ LOKALIZACJI	Weryfikacja, czy usługi mogą zostać przywrócone w aktualnej lokalizacji, czy też konieczne jest uruchomienie ich w środowisku alternatywnym. Analiza uwzględnia dostępność infrastruktury, zasilania oraz bezpieczeństwo środowiska pracy.	Zapewnienie infrastruktury sieciowej oraz dostępu do zasilania. Możliwość wykorzystania lokalizacji zapasowej. Odpowiedzialny: ADO lub osoba posiadająca uprawnienia do zarządzania systemem informatycznym
ZAPEWNIENIE ZASOBÓW TECHNICZNYCH (NAPRAWA / ZAKUP)	Podjęcie działań mających na celu usunięcie awarii poprzez naprawę lub wymianę uszkodzonych elementów infrastruktury. W przypadku braku możliwości zakupu – wdrożenie rozwiązań alternatywnych (np. migracja usług na inne środowisko).	Zapewnienie środków finansowych oraz dostępu do dostawców sprzętu i usług. Odpowiedzialny: ADO
WERYFIKACJA MOŻLIWOŚCI MIGRACJI USŁUG	Ocena możliwości uruchomienia systemu na alternatywnym serwerze lub środowisku technicznym, z uwzględnieniem kompatybilności oraz dostępnych zasobów.	Dostęp do infrastruktury serwerowej oraz dokumentacji systemowej. Odpowiedzialny: ADO
PRZYGOTOWANIE ŚRODOWISKA ZASTĘPCZEGO	Konfiguracja serwera zastępczego (np. stacji roboczej typu desktop) w sposób umożliwiający uruchomienie podstawowych usług. Po konfiguracji należy przeprowadzić testy poprawności działania.	Zapewnienie sprzętu spełniającego minimalne wymagania techniczne. Dostęp do oprogramowania i konfiguracji systemowej. Odpowiedzialny: ADO
PODJĘCIE DECYZJI O ODTWORZENIU SYSTEMU	Ustalenie terminu oraz trybu odtworzenia systemu lub aplikacji, z uwzględnieniem wpływu na działalność jednostki.	Zapewnienie kontaktu z kadrą kierowniczą oraz dostęp do informacji o priorytetach. Odpowiedzialny: ADO
ODTWORZENIE FUNKCJONOWANIA SYSTEMU / APLIKACJI	Przywrócenie działania systemu poprzez usunięcie przyczyny awarii lub odtworzenie środowiska z kopii zapasowych. Proces powinien uwzględniać integralność i aktualność danych.	Dostęp do aktualnych kopii zapasowych, aplikacji oraz baz danych. Odpowiedzialny: osoba posiadająca uprawnienia do zarządzania systemem informatycznym

WERYFIKACJA POPRAWNOŚCI DZIAŁANIA	Przeprowadzenie testów funkcjonalnych i technicznych potwierdzających prawidłowe działanie systemu po jego uruchomieniu lub migracji.	Dostęp do środowiska testowego oraz użytkowników weryfikujących działanie systemu. Odpowiedzialny: osoba posiadającą uprawnienia do zarządzania systemem informatycznym
PRZYWRÓCENIE USŁUGI I KOMUNIKACJA	Uruchomienie usług w środowisku produkcyjnym oraz poinformowanie właściwych interesariuszy o przywróceniu działania systemu.	Zapewnienie aktualnej listy kontaktowej do pracowników. Odpowiedzialny: ADO

TESTOWANIE PLANU

§ 8

LP.	OPIS TESTU	TERMIN REALIZACJI	OCZEKIWANY WYNIK	OSOBA ODPOWIEDZIALNA
1)	Przeprowadzenie testu polegającego na symulacji awarii serwera obsługującego wybraną aplikację, skutkującej całkowitym brakiem możliwości świadczenia usług przez system. Test realizowany jest na podstawie wcześniej opracowanego i zatwierdzonego scenariusza, zawartego w protokole testowym, obejmującego wszystkie etapy postępowania zgodnie z procedurą ciągłości działania.	1 dzień roboczy, zgodnie z harmonogramem testów lub planem ciągłości działania	Skuteczne przywrócenie działania usługi w założonym czasie, w szczególności poprzez uruchomienie aplikacji na środowisku alternatywnym (np. serwerze zastępczym) oraz zapewnienie dostępności dla użytkowników końcowych. Dodatkowo potwierdzenie integralności danych oraz poprawności działania systemu po odtworzeniu.	osoba posiadająca uprawnienia do zarządzania systemem informatycznym

SZKOLENIE DLA UCZESTNIKÓW PLANU

§ 9

1. Uczestnicy planu ciągłości działania są każdorazowo zapoznawani z jego aktualną treścią przed przystąpieniem do przeprowadzenia testów, w zakresie niezbędnym do prawidłowej realizacji przypisanych im zadań.

Zapoznanie to obejmuje w szczególności omówienie scenariusza testowego, ról i odpowiedzialności poszczególnych uczestników, zasad komunikacji oraz oczekiwanych rezultatów testu. Proces ten powinien być udokumentowany (np. w formie listy obecności lub potwierdzenia zapoznania się), w celu zapewnienia rozliczalności oraz możliwości wykazania spełnienia wymagań w trakcie audytu.

AKTUALIZACJA PLANU

§ 10

1. Plan aktualizowany jest każdorazowo w przypadku zmian kadrowych oraz w przypadku niepowodzenia w jego testowaniu.

(data i podpis beneficjenta jednostki)

