

Plan Ciągłości Działania (BCP)

Instytut Rozrodu Zwierząt i Badań Żywności Polskiej Akademii Nauk, ul. Trylińskiego 18, 10-683 Olsztyn, NIP: 739-05-04-515

Data opracowania:

12.12.2024

Wersja dokumentu:

1.0

Osoba odpowiedzialna za dokument:

Jan Maciejski, Informatyk

1. Cel dokumentu

Celem niniejszego dokumentu jest zapewnienie kontynuacji kluczowych procesów działalności Instytutu w przypadku wystąpienia sytuacji kryzysowej, awarii lub innego zakłócenia funkcjonowania, w szczególności awarii technicznych, katastrof naturalnych, ataków cybernetycznych, epidemii itp.

2. Zakres dokumentu

Plan dotyczy wszystkich kluczowych jednostek i procesów Instytutu, w tym:

- badań naukowych,
- działalności dydaktycznej,
- obsługi administracyjnej,
- infrastruktury IT i laboratoriów,
- ochrony danych i informacji.

3. Kluczowe funkcje i zasoby

KLUCZOWE FUNKCJE	KLUCZOWE ZASOBY
Przetwarzanie zamówień I sprzedaż	Zasoby ludzkie – pracownicy o kluczowych kompetencjach, zastępowalność i dostępność personelu
Obsługa klienta	Zasoby technologiczne – systemy informatyczne, serwery, sieci komputerowe, łącza internetowe, kopie zapasowe, systemy odzyskiwania danych
Usługi IT	Zasoby ifizyczne – sprzęt techniczny, maszyn, wyposażenie laboratorium
Zarządzanie finansami	Zasoby informacyjne – dokumentacja techniczna, operacyjna, administracyjna, naukowa
	Dostawcy i Partnerzy – kluczowi dostawcy usług lub materiałów

4. Analiza ryzyk

l.p.	Funkcja krytyczna	Opis funkcji / procesu	Kluczowe zasoby	Czas przywrócenia	Skutki przerwy
1	Prowadzenie badan naukowych	Realizacja projektów badawczych – np. Grantów, zleceń	Laboratoria, aparatura badawcza, oprogramowania, dane, zespół	24 h	Opóźnienie projektów, utrata finansowania, niewywiązywanie się z umów
2	Obsługa grantów i projektów	Nadzór nad budżetami, raportowanie, rozliczenia	Systemy finansowe, dane projektowe, kadra projektowa	24 h	Ryzyko utraty dofinansowania, problemy audytowe

3	System IT i przechowywanie danych	Serwery, bazy danych, repozytoria wyników i dokumentów	Serwerownia, systemy backupowe, dostęp zdalny, administratorzy	8 h	Utrata danych, wstrzymanie pracy zdalnej i badań
6	Obsługa administracyjno-kadrowa	Kadry, płace, umowy o pracę, szkolenia BHP	System kadrowo-płacowy, dane pracowników	8 h	Brak dostępu do dokumentacji kontrolnej lub projektowej

5. Procedury działania w sytuacjach kryzysowych

5.1. Rodzaje sytuacji kryzysowych

- Awaria systemów informatycznych (np. utrata dostępu do serwerów, cyberatak)
- Pożar, powódź, zalanie laboratoriów lub biur
- Przerwa w dostawie mediów (prąd, internet, woda)
- Włamanie, kradzież lub sabotaż
- Poważna awaria sprzętu badawczego
- Zagrożenie epidemiologiczne lub inne zdarzenie zagrażające zdrowiu
- Wypadki z udziałem pracowników lub gości (np. w laboratorium)
- Nagłe odejście lub niedostępność kluczowego personelu

5.2. Ogólna procedura reagowania

1. Zidentyfikowanie incydentu

Osoba, która jako pierwsza zauważy incydent, zgłasza go niezwłocznie do:

- przełożonego,
- osoby odpowiedzialnej za bezpieczeństwo
- działu IT / administracji, w zależności od rodzaju incydentu.

2. Ocena zagrożenia

Osoby odpowiedzialne dokonują szybkiej analizy:

- Czy sytuacja wymaga ewakuacji?
- Jakie zasoby są zagrożone?
- Jakie działania trzeba podjąć natychmiast?

3. Uruchomienie procedur awaryjnych

W zależności od sytuacji, uruchamia się odpowiednie plany:

- Plan awaryjnego przywrócenia systemów IT
- Ewakuacja pracowników (zgodnie z instrukcją przeciwpożarową)
- Przejście na tryb pracy zdalnej
- Przekierowanie działań do innej jednostki/laboratorium

4. Powiadomienie interesariuszy

Informacje przekazuje się do:

- kadry kierowniczej,
- partnerów projektowych i grantodawców (jeśli dotyczy projektów),
- służb ratunkowych (jeśli potrzebne),
- pracowników (poprzez ustalone kanały: e-mail, SMS, intranet).

5. Dokumentacja i analiza

Po zakończeniu kryzysu:

- Sporządza się raport incydentu,
- Dokonuje się przeglądu skuteczności działań,
- Wdraża się działania korygujące i zapobiegawcze (lessons learned).

5.3. Role i odpowiedzialności

Rola	Zakres odpowiedzialności
Koordinator BCP	Nadzór nad realizacją planu, kontakt z kierownictwem
Dział IT	Przywrócenie systemów, kopii zapasowych
Kierownik administracyjny	Zapewnienie bezpieczeństwa fizycznego i organizacyjnego
Kierownicy projektów	Ocena wpływu na badania i informowanie partnerów
Dział HR	Komunikacja z pracownikami i wsparcie kadrowe

5.4. Lista kontaktowa awaryjna

Zawiera numery telefonów i e-maile do:

- kierownictwa,
- działów odpowiedzialnych (IT, BHP, administracja),
- służb ratunkowych,
- lokalnych dostawców usług (media, IT).

6. Plan komunikacji kryzysowej

6.1. Główna osoba kontaktowa

- **Imię i nazwisko:** *Krzysztof Szerejko*
- **Funkcja:** *Kierownik Działu Inwestycyjno - Gospodarczego*
- **Telefon służbowy:** 693 555 902
- **E-mail:** k.szerejko@pan.olsztyn.pl

6.2. Alternatywna osoba kontaktowa

- **Imię i nazwisko:** Janusz Wróblewski
- **Funkcja:** *Specjalista*
- **Telefon / E-mail:** j.wroblewski@pan.olsztyn.pl; +48 89 500 32 50

6.3. Kanały komunikacji

Do przekazywania informacji kryzysowych używane będą następujące kanały – w zależności od dostępności i pilności:

Kanał	Przeznaczenie	Uwagi
E-mail	Główne komunikaty, raporty, dokumentacja	Do całej kadry lub wybranych grup
SMS	Szybkie powiadomienie wszystkich pracowników	Szczególnie przy awariach lub ewakuacji
Komunikatory (np. Teams, Whatsapp)	Robocze uzgodnienia, komunikacja w zespołach	Wymaga dostępu do sieci lub VPN
Telefon	Krytyczne, bezpośrednie kontakty	Szczególnie do kluczowych osób
Strona WWW / Intranet	Aktualności dla pracowników i interesariuszy	Aktualizacja przez dział PR / IT

6.4. Zasady komunikacji

- Komunikaty muszą być **krótkie, rzeczowe i wiarygodne**.
- Informacje są przekazywane wyłącznie przez osoby wyznaczone.
- Wszystkie wiadomości powinny zawierać:
 - *Opis sytuacji*
 - *Podjęte działania*

- *Zalecenia / działania do wykonania*
- *Kontakt do osoby odpowiedzialnej*

6.5. Grupy odbiorców komunikatów

- **Pracownicy** (naukowi, techniczni, administracyjni)
- **Zarząd instytutu**
- **Partnerzy/ Najemcy oraz goście**
- **Media i opinia publiczna** (przy poważnych zdarzeniach – za pośrednictwem rzecznika)

7. Harmonogram przeglądów i testów BCP

Aby zapewnić skuteczność planu ciągłości działania (BCP) i jego dostosowanie do zmieniających się warunków, konieczne są regularne przeglądy i testy. Harmonogram przeglądów i testów ma na celu:

- Weryfikację aktualności procedur,
- Sprawdzenie reakcji na różne scenariusze kryzysowe,
- Identyfikację obszarów do poprawy.

7.1. Przeglądy BCP

Rodzaj przeglądu	Termin przeglądu	Zakres przeglądu	Odpowiedzialna osoba
Przegląd roczny	Co 12 miesięcy	Weryfikacja kompletności dokumentacji BCP, aktualności procedur, zmian w strukturze organizacyjnej i zasobach	Koordinator BCP
Przegląd po dużych zmianach organizacyjnych	Po każdej dużej zmianie	Dostosowanie planu do nowych realiów (np. zmiany w strukturze, nowi dostawcy, zmiany technologiczne)	Kierownictwo instytutu
Przegląd po każdej sytuacji kryzysowej	Po zakończeniu sytuacji kryzysowej	Ocena skuteczności działań, identyfikacja słabości i usprawnień	Koordinator BCP

7.2. Testy BCP

Rodzaj testu	Termin	Zakres testu	Odpowiedzialna osoba
Test awaryjnego przywracania systemów IT	Co 6 miesięcy	Test odzyskiwania danych z kopii zapasowych, przywracanie systemów IT	Dział IT
Test ewakuacji	Nie rzadziej niż Co 24 miesiące	Przeprowadzenie ćwiczeń ewakuacyjnych (w tym ewakuacja z laboratoriów)	Specjalista ds. BHP i Ppoż., administracja
Test komunikacji kryzysowej	Co 12 miesięcy	Sprawdzenie skuteczności kanałów komunikacji (SMS, e-mail, komunikatory)	Dział Inwestycyjno - Gospodarczy

7.3. Procedura testów BCP

1. Przygotowanie testu

- Określenie celu testu i scenariusza kryzysowego (np. cyberatak, pożar, awaria systemu).
- Wybór uczestników testu (przedstawiciele wszystkich działów).
- Przygotowanie materiałów informacyjnych.

2. Przeprowadzenie testu

- Symulacja zdarzenia kryzysowego.
- Ocena skuteczności podjętych działań w czasie rzeczywistym.
- Dokumentowanie wyników testu i zgłoszonych problemów.

3. Analiza wyników i raport

- Ocena wykonania zadań, identyfikacja słabych punktów w planie.

- Sporządzenie raportu z wnioskami i rekomendacjami.
- Wdrożenie działań naprawczych i aktualizacja planu.

4. Powiadomienie zainteresowanych stron

- Udzielenie informacji o wynikach testu pracownikom instytutu oraz zainteresowanym partnerom.

7.4. Zasady oceny wyników przeglądów i testów

- **Skuteczność** – Jak dobrze przebiegły testy? Czy procedury działały zgodnie z planem?
- **Czas reakcji** – Jak szybko instytut zareagował na kryzysowy scenariusz?
- **Dokumentacja** – Czy wszystkie procedury były odpowiednio udokumentowane i dostępne dla pracowników?
- **Rekomendacje** – Jakie zmiany lub usprawnienia należy wprowadzić, aby plan był skuteczniejszy?

8. Załączniki

- Schemat organizacyjny
- Lista kontaktowa

za M. Maryli

DYREKTOR

Prof. dr hab. Mariusz W. Piskula
czł. koresp. PAN

STRUKTURA ORGANIZACYJNA INSTYTUTU ROZRODU ZWIERZĄT I BADAŃ ŻYWNOSTCI PAN W OLSZTYNIE



