

# **PLAN ZAPEWNIENIA CIĄGŁOŚCI DZIAŁANIA**

**w przypadku zakłócenia teleinformatycznego  
środowiska pracy**

Opracował:

Zarząd:



## 1. CEL I ZAKRES

### Cel

Niniejszy plan zapewnienia ciągłości działania (zwany dalej Planem) określa podstawy do skutecznego i sprawnego zarządzania funkcjonowaniem „ELTUR-SERWIS” Sp. z o.o., poprzez zaplanowane działania ukierunkowane na ograniczanie zagrożenia związanego z zakłóceniem teleinformatycznego środowiska pracy w zakresie

1. Infrastruktury technicznej:
  - 1.1. serwerów
  - 1.2. stacji roboczych
2. Oprogramowanie:
  - 2.1. wadliwe działanie
  - 2.2. wirusy:
3. Zasoby ludzkie
  - 3.1. Wysoka absencja pracowników Biura IT
4. Utrata istotnych usługodawców

### Zakres

Plan zawiera regulacje w zakresie działań w przypadku wystąpienia sytuacji krytycznej oraz określa obowiązki, kompetencje i odpowiedzialność podmiotów uczestniczących w procesie Zapewnienia Ciągłości Działania.

## 2. ODPOWIEDZIALNOŚĆ

Przewodniczący Zespołu Kryzysowego w zakresie:

- wdrożenia i przestrzegania prawidłowości stosowania Planu,
- kierowania działaniami w ramach realizacji PCB.

Kierownik Biura IT w zakresie:

- obowiązków jednostki właściwej ds. zapewnienia ciągłości działania.

## 3. DOKUMENTY POWIĄZANE

- Regulamin Korzystania z Zasobów Informatycznych i Telekomunikacyjnych (ICT) w PGE Górnictwo i Energetyka Konwencjonalna Spółka Akcyjna
- Instrukcja Administrowania Zasobami Informatycznymi i Telekomunikacyjnymi (ICT) w PGE Górnictwo i Energetyka Konwencjonalna Spółka Akcyjna
- Regulamin korzystania ze sprzętu i oprogramowania komputerowego w "ELTUR-SERWIS" Sp. z o.o.

## 4. ZAŁĄCZNIKI

- Załącznik nr 1. Schemat podejmowania decyzji w zakresie Planu.
- Załącznik nr 2. Protokół zgłoszenia wystąpienia sytuacji krytycznej.
- Załącznik nr 3. Protokół końcowy dokumentujący podjęte działania w związku z wystąpieniem sytuacji krytycznej.

## 5. SKRÓTY I DEFINICJE

### Skróty użyte na potrzeby niniejszego dokumentu:

**BCP** (ang. Business Continuity Plans) plany kontynuowania działalności Przedsiębiorstwa Usługowo-Produkcyjnego "ELTUR-SERWIS" Spółka z ograniczoną odpowiedzialnością po wystąpieniu awarii

**PZCD** - Plan Zapewnienia Ciągłości Działania dalej zwany Planem

### Definicje pojęć użyte na potrzeby niniejszego dokumentu:

- a. **Aktywa** – wszystkie zasoby, które mają wartość dla Spółki (m.in. zasoby ludzkie, finansowe, informacyjne, organizacyjne, technologiczne i fizyczne oraz wartość marki).
- b. **Aktywa krytyczne** – aktywa mające kluczowe znaczenie dla zapewnienia realizacji zadań statutowych Spółki.

- c. **Awaria** – sytuacja krytyczna, która została zidentyfikowana i przewidziano dla niej stosowną procedurę powrotu do stanu działania w warunkach normalnych, zgodnie z Planem Zapewniania Ciągłości Działania.
- d. **Bezpieczeństwo** - zdolność do unikania szkód będących wynikiem ryzyka, niebezpieczeństwa lub zagrożenia.
- e. **Dostępność** - właściwość polegająca na tym, że określone aktywa mogą być dostępne i wykorzystywane na żądanie uprawnionego podmiotu.
- f. **Jednostka organizacyjna PGE S.A. właściwa ds. bezpieczeństwa** – jednostka organizacyjna w PGE S.A., która jest odpowiedzialna za kreowanie standardów sporządzania Planów zapewnienia ciągłości działania w GK PGE.
- g. **Kierownik komórki organizacyjnej** – Pracownik zatrudniony na stanowisku kierowniczym, któremu podporządkowano komórkę organizacyjną rozumianą jako wieloosobowy element struktury organizacyjnej utworzony do wykonywania określonych celów Spółki.
- h. **Plan zapewnienia ciągłości działania** - jest scenariuszem postępowania Spółki w sytuacji, gdy niemożliwe jest wykonywanie przez nią zadań w sposób zazwyczaj przyjęty lub gdy możliwe jest tylko niepełne wykonywanie tych zadań.
- i. **Pracownik** – osoba z którą Pracodawca nawiązał stosunek pracy w rozumieniu art. 22 K.P., nie obejmuje osób wykonujących pracę na innej podstawie niż stosunek pracy.
- j. **Procesy krytyczne** – procesy, których zatrzymanie może spowodować istotne negatywne konsekwencje dla ekonomicznej kondycji Spółki.
- k. **Przełożony** – osoba zajmująca stanowisko, którego miejsce w strukturze organizacyjnej Spółki oraz powiązany z nim zakres obowiązków i wynikająca z niego odpowiedzialność wymaga i umożliwia wydanie poleceń służbowych oraz egzekwowanie ich wykonania od pracowników zatrudnionych w wyznaczonym obszarze struktury organizacyjnej Spółki.
- l. **Ryzyko** - możliwość całkowitego lub częściowego niezrealizowania celu biznesowego stawianego przed Spółką.
- m. **Spółka** - „ELTUR-SERWIS” Sp. z o.o.
- n. **System** – system zapewniania ciągłości działania w przypadku wystąpienia sytuacji krytycznej.
- o. **Sytuacja krytyczna** – zdarzenie uniemożliwiające lub poważnie utrudniające normalne działanie Spółki przez czas określony w Planie.
- p. **Zagrożenie** – potencjalna możliwość wystąpienia sytuacji krytycznej.
- q. **Zespół Awaryjny** – zespół osób powołany w obrębie danej komórki organizacyjnej do realizacji określonych zadań związanych z sytuacjami krytycznymi.
- r. **Zespół Kryzysowy** – zespół osób powoływany do rozwiązywania sytuacji krytycznych.

## 6. REALIZACJA

### 6.1. POSTANOWIENIA OGÓLNE

- 6.1.1 Za koordynowanie przedsięwzięć związanych z zapewnianiem ciągłości działania odpowiada powołany przez Zarząd Spółki Zespół Kryzysowy.
- 6.1.2 Rola poszczególnych podmiotów uczestniczących w procesie Zapewniania Ciągłości Działania ujęte zostały w załączniku nr 1 „Schemat podejmowania decyzji w zakresie Planu PZCD”.
- 6.1.3 W przypadku wystąpienia sytuacji krytycznej, której skutki można usunąć za pomocą istniejących procedur wewnętrznych w czasie do 72 godzin, nie jest uruchamiany Plan.
- 6.1.4 Znajomość i poprawne stosowanie postanowień Planu obowiązuje wszystkich Pracowników Spółki w zakresie przewidzianym w Planie.
- 6.1.5 Za ujęcie w Planie Finansowym Spółki nakładów przewidywanych w odniesieniu do BCP odpowiedzialny jest Przewodniczący Zespołu Kryzysowego.
- 6.1.6 Plan, po jego zatwierdzeniu przez Zarząd Spółki, podlega realizacji na zasadach ogólnych, a jego nieprzestrzeganie może być traktowane jako naruszenie obowiązków pracowniczych.

## 6.2. ZESPÓŁ KRYZYSOWY

6.2.1 W celu koordynacji przedsięwzięć związanych z usuwaniem sytuacji krytycznych, Zarząd Spółki powołuje Zespół Kryzysowy, w składzie: Przewodniczący, Wiceprzewodniczący, Sekretarz, Członkowie.

## 6.3. PRZEWODNICZĄCY ZESPOŁU KRYZYSOWEGO

- 6.3.1 Przewodniczący Zespołu Kryzysowego opracowuje Plan i przekazuje go do zatwierdzenia Zarządowi Spółki.
- 6.3.2 Przewodniczący Zespołu Kryzysowego kieruje pracą Zespołu Kryzysowego, wydaje decyzje dotyczące działania Systemu.
- 6.3.3 Przewodniczący Zespołu Kryzysowego ma prawo przekazywania Kierownikom Komórek Organizacyjnych wytycznych dotyczących realizacji zadań niezbędnych dla osiągnięcia celów Systemu w zakresie działania podległych im jednostek.

## 6.4. ZASADY URUCHAMIANIA PLANU

- 6.4.1. Stan normalnej pracy środowiska teleinformatycznego.
- dostępna jest domena ActivDirectory, logowanie do domeny przebiega w sposób prawidłowy
  - wszystkie serwery są sprawne i dostępne
  - dostępna jest sieć internetowa, intranetowa oraz połączenia VPN
  - wszystkie urządzenia aktywne są sprawne
  - dostępne są połączenia telefoniczne i internetowe na zewnątrz realizowane za pośrednictwem telefonów stacjonarnych
  - frekwencja pracowników Biura IT powyżej 70%

Zagrożenia:

brak, praca w Spółce przebiega w warunkach normalnych.

*Działania zapobiegawcze (BCP nie jest uruchamiany)*

- 6.4.2. Wystąpienie zagrożenia infrastruktury technicznej

Zagrożenia:

brak dostępu do systemu Infra-Comfort spowodowany awarią serwera

Działania:

- powiadomienie Biura IT
- podjęcie działań administracyjnych przez pracownika Biura IT zmierzających do przywrócenia dostępu do systemu Infra-Comfort
- w przypadku braku efektów pracownik Biura IT powiadamia kierownika Biura IT i sporządza protokół zgłoszenia wystąpienia sytuacji krytycznej, zgodnie z załącznikiem nr 2 do niniejszego Planu.
- protokół zgłoszenia wystąpienia sytuacji krytycznej, pracownik Biura IT, w sposób skuteczny przekazuje do Przewodniczącego Zespołu Kryzysowego.
- Przewodniczący Zespołu Kryzysowego podejmuje decyzję o uruchomieniu / nie uruchomieniu BCP.

Zagrożenia:

brak dostępu do sieci

Działania:

- powiadomienie Biura IT
- podjęcie działań administracyjnych przez pracownika Biura IT zmierzających do przywrócenia dostępu do sieci
- w przypadku braku efektów pracownik Biura IT powiadamia kierownika Biura IT i

- sporządza protokół zgłoszenia wystąpienia sytuacji krytycznej, zgodnie z załącznikiem nr 2 do niniejszego Planu.
- protokół zgłoszenia wystąpienia sytuacji krytycznej, pracownik Biura IT, w sposób skuteczny przekazuje do Przewodniczącego Zespołu Kryzysowego.
- Przewodniczący Zespołu Kryzysowego podejmuje decyzję o uruchomieniu / nie uruchomieniu BCP.

#### 6.4.3. Wystąpienie zagrożenia oprogramowania

Zagrożenia:

wadliwe działanie oprogramowania

Działania:

- powiadomienie Biura IT
- podjęcie działań administracyjnych przez pracownika Biura IT zmierzających do przywrócenia prawidłowego działania oprogramowania
- w przypadku braku efektów pracownik Biura IT powiadamia kierownika Biura IT i sporządza protokół zgłoszenia wystąpienia sytuacji krytycznej, zgodnie z załącznikiem nr 2 do niniejszego Planu.
- protokół zgłoszenia wystąpienia sytuacji krytycznej, pracownik Biura IT, w sposób skuteczny przekazuje do Przewodniczącego Zespołu Kryzysowego.
- Przewodniczący Zespołu Kryzysowego podejmuje decyzję o uruchomieniu / nie uruchomieniu BCP.

Zagrożenia:

Wirusy

Działania:

- powiadomienie Biura IT
- podjęcie działań administracyjnych przez pracownika Biura IT zmierzających do usunięcia wirusów
- w przypadku braku efektów pracownik Biura IT powiadamia kierownika Biura IT i sporządza protokół zgłoszenia wystąpienia sytuacji krytycznej, zgodnie z załącznikiem nr 2 do niniejszego Planu.
- protokół zgłoszenia wystąpienia sytuacji krytycznej, pracownik Biura IT, w sposób skuteczny przekazuje do Przewodniczącego Zespołu Kryzysowego.
- Przewodniczący Zespołu Kryzysowego podejmuje decyzję o uruchomieniu / nie uruchomieniu BCP.

#### 6.4.4. Wystąpienie zagrożenia zasobów ludzkich

Zagrożenia:

Wysoka, ponad 70 % absencja pracowników Biura IT

Działania:

- powiadomienie przełożonego i Przewodniczącego Zespołu Kryzysowego
- Przewodniczący Zespołu Kryzysowego podejmuje decyzję o uruchomieniu / nie uruchomieniu BCP.

#### 6.4.5. Wystąpienie zagrożenia utrata istotnych usługodawców

Zagrożenia:

Brak nadzoru autorskiego

Działania:

- powiadomienie przełożonego i Przewodniczącego Zespołu Kryzysowego
- Przewodniczący Zespołu Kryzysowego podejmuje decyzję o uruchomieniu / nie uruchomieniu BCP.



## **6.5.PLAN KONTYNUOWANIA DZIAŁALNOŚCI PO WYSTĄPIENIU ZAKŁÓCENIA TELEINFORMATYCZNEGO ŚRODOWISKA PRACY (BCP).**

### **6.5.1. Wystąpienie zagrożenia infrastruktury technicznej**

- W przypadku identyfikacji braku dostępu do systemu Infra-Comfort spowodowanego awarią serwera należy wystawić wniosek o zakup usługi w zakresie usunięcia awarii serwera. Dalszą pracę do momentu usunięcia wady należy kontynuować w oparciu o metody tradycyjne. Po usunięciu awarii należy uzupełnić powstałe braki.
- W przypadku identyfikacji braku dostępu do sieci należy powiadomić usługodawcę sprawującego nadzór nad siecią o zaistniałej sytuacji. Dalszą pracę do momentu usunięcia wady należy kontynuować w oparciu o metody tradycyjne. Po usunięciu awarii należy uzupełnić powstałe braki.

### **6.5.2. Wystąpienie zagrożenia oprogramowania**

- W przypadku identyfikacji wadliwego działania oprogramowania należy wystawić wniosek o zakup usługi do odpowiedniego autora oprogramowania. Przewodniczący Zespołu Kryzysowego powołuje Zespół Awaryjny w skład , którego obligatoryjnie wchodzi Kierownik Biura IT, Kierownik Merytorycznie Odpowiedzialny (określony w Zarządzeniu 11/2012 Dyrektora Naczelnego „Eltur-Serwis” Sp z o.o. z dnia 07/08.2012), pracownicy Biura IT oraz inni pracownicy. Dalszą pracę do momentu usunięcia wady należy kontynuować w oparciu o metody tradycyjne. Po usunięciu awarii należy uzupełnić powstałe braki.
- W przypadku stwierdzenia zawirusowania uniemożliwiającego prowadzenie działalności przez „ELTUR-SERWIS” pracownik Biura IT powiadamia usługodawcę sprawującego nadzór nad oprogramowaniem antywirusowym i Przewodniczącego Zespołu Kryzysowego o zaistniałej sytuacji. W przypadkach nadzwyczajnych Przewodniczący Zespołu Kryzysowego powołuje Zespół Awaryjny. Dalszą pracę do momentu usunięcia zawirusowania należy kontynuować w oparciu o metody tradycyjne. Po usunięciu awarii należy uzupełnić powstałe braki.

### **6.5.3. Wystąpienie zagrożenia zasobów ludzkich**

- W przypadku stwierdzenia wysokiej absencji w Biurze IT należy powiadomić Przewodniczącego Zespołu Kryzysowego o zaistniałej sytuacji. Przewodniczący Zespołu Kryzysowego podejmuje decyzję o czasowym skierowaniu do pracy w Biurze IT pracowników, z innych komórek organizacyjnych, posiadających wiedzę informatyczną

### **6.5.4. Wystąpienie zagrożenia utrata istotnych usługodawców**

- W przypadku stwierdzenia utraty istotnego usługodawcy należy powiadomić Przewodniczącego Zespołu Kryzysowego o zaistniałej sytuacji. Przewodniczący Zespołu Kryzysowego podejmuje decyzję o wszczęciu postępowania mającego na celu pozyskanie nowego usługodawcy.

6.5.5. Po ustaniu zagrożenia, należy sporządzić Protokół końcowy dokumentujący podjęte działania w związku z wystąpieniem sytuacji krytycznej, zgodnie z załącznikiem nr 3 do niniejszego Planu.

## **6.6.RAPORTOWANIE.**

6.6.1. Przewodniczący Zespołu Kryzysowego sporządza każdorazowo po zaistnieniu zdarzenia mającego wpływ na ciągłość działania Spółki, szczegółową informację zawierającą opis, skutki, podjęte działania i przekazuje ją do jednostki organizacyjnej PGE S.A. właściwej ds.

bezpieczeństwa w wiadomości e-mail niezwłocznie, lecz nie później niż w dniu następnym po zaistnieniu zdarzenia.

6.6.2. Powyższa informacja przekazywana jest do wiadomości Zarządowi Spółki.

## **6.7. UTRZYMANIE, AKTUALIZACJA, TESTOWANIE PLANU.**

6.7.1. Każdy Pracownik ma prawo składać wnioski do Przewodniczącego Zespołu Kryzysowego, drogą służbową, o zmiany w Planie.

6.7.2. Przewodniczący Zespołu Kryzysowego ma obowiązek sprawdzić oraz zaakceptować zaktualizowany Plan.

6.7.3. Kierownik Biura IT ma obowiązek minimum 1 raz w roku zainicjować testowanie Planu. Testowanie Planu powinno się odbyć przed wystąpieniem teleinformatycznego zakłócenia środowiska pracy. W ramach testowania powinno wykonać się wszystkie wymagane Planem czynności.

## **6.8. Działania prewencyjne wymagane w celu utrzymania aktywa w wymaganej sprawności**

6.8.1. Wystąpienie zagrożenia infrastruktury technicznej

W celu minimalizacji ryzyka zagrożenia infrastruktury technicznej należy wyposażyć serwer w zasilacz awaryjny UPS czasowo podtrzymujący zasilanie.

6.8.2. Wystąpienie zagrożenia oprogramowania

W celu minimalizacji ryzyka zagrożenia oprogramowania należy:

- okresowo przeprowadzać skanowanie antywirusowe zasobów na komputerach;
- okresowo przeprowadzać audyt oprogramowania i zasobów przechowywanych na komputerach pod kątem legalności oprogramowania oraz zasobów nie związanych z wykonywanymi obowiązkami służbowymi;
- wykonywać kopię bezpieczeństwa z systemu InFra-Comfort w cyklach 24 godzinnych.

6.8.3. Wystąpienie zagrożenia zasobów ludzkich

W celu minimalizacji ryzyka zagrożenia zasobów ludzkich należy przeszkolić pracowników z innych komórek organizacyjnych.

6.8.4. Wystąpienie zagrożenia utrata istotnych usługodawców

W celu minimalizacji ryzyka zagrożenia utraty istotnych usługodawców należy podpisać stosowne umowy.





## Schemat podejmowania decyzji w zakresie PZCD

	Zespoły Awaryjne	PGE Systemy S.A.	Jednostka właściwa ds. zapewnienia ciągłości działania	Zespół Kryzysowy	Jednostka właściwa ds. ryzyka
Organizacja przedsięwzięcia i nadzór nad jego realizacją			R		
Określenie wymagań procesów w zakresie aktywów	R		I		
Identyfikacja zagrożeń	I			R	
Wykonanie analizy ryzyka	I			A	R
Zatwierdzenie rezultatów analizy ryzyka				R	
Ustalenie koncepcji działania w sytuacjach krytycznych wynikających ze zidentyfikowanych zagrożeń				R	
Koordinacja planowania Zapewniania Ciągłości Działania				R	
Ustalenie technicznych rozwiązań dotyczących odtwarzania systemów wspierających działalność		R			
Planowanie przeprowadzania testów scenariuszy awaryjnych	I	R		A	
Prowadzenie szkoleń i treningów z zakresu PZCD postępowania w sytuacjach krytycznych	R			A	
Aktualizacja PZCD	R	I		A	
Zatwierdzenie PZCD				R	

### Legenda

R – responsibility – odpowiedzialność  
A – acceptance – akceptacja  
C – communication- komunikacja  
I – information – informacja



**Protokół zgłoszenia wystąpienia sytuacji krytycznej Nr .....**

**Do Przewodniczącego Zespołu Kryzysowego**

Miejsce wystąpienia sytuacji krytycznej (lokalizacja): .....		Termin wystąpienia sytuacji krytycznej: .....
Osoba zgłaszająca wystąpienie sytuacji krytycznej:  ..... <i>imię i nazwisko, stanowisko</i>	Kierownik komórki organizacyjnej w Spółce  ..... <i>imię i nazwisko, stanowisko</i>	
Określenie sposobu stwierdzenia wystąpienia sytuacji krytycznej: ..... .....		
Wstępne określenie przyczyn wystąpienia sytuacji krytycznej: ..... .....		
Określenie przewidywanych skutków sytuacji krytycznej: ..... .....		
Spis proponowanych czynności istotnych z uwagi na proces usuwania sytuacji krytycznej: ..... .....		
Wstępne wnioski dotyczące zapobiegania takim sytuacjom krytycznym w przyszłości: ..... .....		
Przewidywany termin przywrócenia stanu sprzed wystąpienia sytuacji krytycznej:		.....
Data i podpis osoby zgłaszającej sytuację krytyczną	Data i podpis kierownika komórki organizacyjnej Spółki	Data i podpis Przewodniczącego Zespołu Kryzysowego



**Protokół końcowy dokumentujący podjęte działania w związku z wystąpieniem sytuacji krytycznej Nr .....**  
**Do Przewodniczącego Zespołu Kryzysowego**

Miejsce wystąpienia sytuacji krytycznej (lokalizacja):  .....		Termin wystąpienia sytuacji krytycznej:  .....	
Osoba zgłaszająca wystąpienie sytuacji krytycznej:  ..... <i>imię i nazwisko, stanowisko</i>		Kierownik komórki organizacyjnej w Spółce  ..... <i>imię i nazwisko, stanowisko</i>	
Określenie sposobu stwierdzenia wystąpienia sytuacji krytycznej:  ..... ..... .....			
Określenie stwierdzonych przyczyn wystąpienia sytuacji krytycznej:  ..... .....			
Określenie stwierdzonych skutków sytuacji krytycznej:  ..... .....			
Spis wykonanych czynności z uwagi na proces usuwania sytuacji krytycznej:  ..... ..... .....			
Końcowe wnioski dotyczące zapobiegania takim sytuacjom krytycznym w przyszłości:  ..... ..... .....			
Czy wymagana jest korekta Planu Zapewnienia Ciągłości Działania?		TAK	NIE
Faktyczny termin przywrócenia stanu sprzed wystąpienia sytuacji krytycznej:		.....	
Data i podpis osoby zgłaszającej sytuację krytyczną	Data i podpis kierownika komórki organizacyjnej w Spółce	Data i podpis Przewodniczącego Zespołu Kryzysowego	

