Załącznik nr 10
do Umowy DZ.271….2023

Wymagania dotyczące zakresu i procedury przeprowadzenia audytu w siedzibie Wykonawcy

A. Wymagania dotyczące procedury przeprowadzenia audytu

1. Audyt może być przeprowadzony przez pracowników LP lub przez firmę audytorską.
2. Audyt może dotyczyć realizacji całości lub części prac określonych w Umowie.
3. Audyt może być przeprowadzony po uprzednim pisemnym ustaleniu:
   1) Terminu realizacji audytu, z co najmniej 14 dniowym wyprzedzeniem
   2) Poinformowaniu o miejscu, czasie i zakresie audytu
4. Audyt może być przeprowadzony wyłącznie w dni robocze w godzinach pracy.
5. W trakcie realizacji audytu Wykonawca zobowiązuje się do pełnej współpracy z Audytorem, a w szczególności do:
   1) Ujawniania na jego wniosek wszystkich informacji związanych z realizacją Umowy.
   2) Dostępu do dokumentów i pomieszczeń bezpośrednio związanych z wykonywaniem przedmiotu umowy.
6. Audyt nie obejmuje dokumentów faktur lub innych dokumentów zw. z kosztami świadczenia przedmiotu umowy.

B. Wymagania dotyczące zakresu przeprowadzenia audytu

1. Audyt obejmuje udostępnienie dokumentów i pomieszczeń bezpośrednio związanych z wykonywaniem przedmiotu umowy.
2. Audyt obejmuje:
   1) Przegląd realizacji zaleceń dotyczących infrastruktury teleinformatycznej (zgodnie z zakresem wymienionym w pkt. C),
   2) Przegląd realizacji procesów zapewniających ciągłość działania środowiska Systemu (zgodnie z zakresem wymienionym w pkt. D).

C. Zalecenia dotyczące infrastruktury teleinformatycznej

1. Udostępnienie zasobów infrastruktury teleinformatycznej celem uzyskania poprawnej, nieprzerwanej pracy Systemu.
2. Zagwarantowanie zdolności Systemu do zwiększenia jego wydajności w przypadku zwiększenia obciążenia Systemu przez użytkowników.
3. Zastosowanie następujących systemów zwiększających bezpieczeństwo portali: firewall, antywirus i IDS/IPS.
4. Zapewnienie:
   1) Wykonanie kopii zapasowych środowiska (serwerów / maszyn wirtualnych) i baz danych,
   2) Testowanie ich użyteczności w procesie odtwarzania.
   3) Odtwarzanie środowiska w przypadku wystąpienia awarii.
5. Sporządzanie dokumentacji dotyczącej wszelkich czynności administratorskich.
6. Stosowanie zabezpieczeń, co najmniej na poziomie określonym w załączniku A do normy ISO/IEC 27001/27002.
7. Przygotowanie i udostępnienie do przeglądu procedur eksploatacyjnych wraz ze szczegółowymi instrukcjami dla działań związanych z Usługą Utrzymania, takich jak:
   1) procedury instalacji, uruchamiania, aktualizacji i zatrzymania serwerów i usług,
   2) procedury tworzenia i odtwarzania kopii zapasowych, a także likwidacji nośników danych,
   3) konserwacji sprzętu i oprogramowania,

4) obsługi błędów.

8. Opracowanie procedury zapewnienia ciągłości działania środowiska e-drewno.
9. Zastosowanie redundantnych zasobów infrastruktury środowiska wspomagających operacyjną ciągłość działania:
   1) dublowanie sprzętu,
   2) zwielokrotnienie linii komunikacyjnych,
   3) zwielokrotnienie punktów dostępu do sieci publicznych,
   4) separacja fizyczna, energetyczna i logiczna głównych elementów infrastruktury,
   5) dyżury specjalistów, monitoring 24h/dobę,
   6) wirtualizacja systemów krytycznych.
10. Zastosowanie redundantnych zasobów infrastruktury Data Center zapewniających operacyjną ciągłość działania:
    1) Systemy klimatyzacji precyzyjnej
       Posiadanie nadmiarowych systemów klimatyzatorów w pomieszczeniach Data Center w celu zabezpieczenia w przypadku awarii jednego z urządzeń lub na wspomaganie w przypadku niedotrzymywania parametrów środowiska przy pracy pojedynczego klimatyzatora.
    2) Zasilanie
       Zapewnienie redundantnego zasilania wszystkich szaf IT wspomaganych dodatkowo przez nadmiarowy system UPSów oraz agregatów prądotwórczych.
    3) Ochrona przeciwpożarowa
       Przebadanie pod kątem szczelności wszystkich pomieszczeń.
       Wykorzystanie systemu wczesnego wykrywania pożarów wraz ze stałym układem gaśniczym.
       Podłączenie wszystkich urządzeń ppoż pod centralę alarmową.
    4) Łączność IT
       Zapewnienie redundantnych sieci opartych o różnych dostawców.
       Zapewnienie redundantnych łączy prowadzonych zwielokrotnionymi torami światłowodowymi lub radioliniami.
       Zapewnienie redundantnych routerów znajdujących się w różnych budynkach wyposażonych w odrębne systemy zasilania awaryjnego.
    5) Fizyczny dostęp do urządzeń
       Zapewnienie kontrolowanego dostępu do budynku Data Center w trybie rejestrowanym przez pracowników ochrony pracujących w trybie (24/7/365).
    6) Monitorowanie środowiska
       Monitorowanie środowiska e-drewno zgodnie z zasadami i wytycznymi w umowie.
11. Przekazanie oświadczenia o posiadaniu aktualnych umów na serwis urządzeń wykorzystywanych podczas świadczenia usługi.

D. Procedura zapewnienia ciągłości działania środowiska e-drewno

1. Procedury zapewnienia ciągłości działania związane z przeciwdziałaniem przerwom w działalności biznesowej oraz ochroną krytycznych procesów biznesowych firmy Wykonawcy (obszary: infrastruktury informatycznej i telekomunikacyjnej, usług Data Center i monitorowania).
   1) Strategia przetrwania obejmująca działania związane z przeciwdziałaniem przerwom w działalności biznesowej oraz ochroną krytycznych procesów biznesowych spowodowanych:
      - destrukcją fizycznego środowiska pracy

- destrukcją funkcjonalnego środowiska pracy
- destrukcją technicznego środowiska pracy
- destrukcją informatycznego środowiska pracy w tym:
  - infrastruktury teleinformatycznej
  - oprogramowania
  - danych
  - obsługi
  - zminimalizowania potencjalnych strat wynikających z przerwania krytycznych procesów,
  - utrzymania działalności organizacji na minimalnym akceptowalnym poziomie,
  - bezpieczne wstrzymanie do odwołania procesów biznesowych uznanych za niekluczowe.

  Procedura powinna opisywać:
  - zasoby ludzkie niezbędne do realizacji procesów kluczowych w sytuacji kryzysowej,
  - lokalizację zapasową, w której będą wykonywane procesy kluczowe na minimalnym akceptowalnym poziomie (tzw. zapasowe miejsce pracy),
  - systemy teleinformatyczne i stacje robocze niezbędne do realizacji procesów kluczowych na minimalnym akceptowalnym poziomie,
  - infrastrukturę biurową niezbędną do realizacji procesów kluczowych na minimalnym akceptowalnym poziomie,
  - dane i informacje niezbędne do realizacji procesów kluczowych na minimalnym akceptowalnym poziomie,
  - usługi podmiotów zewnętrznych związane z realizacją procesów kluczowych.

2) Przeciwdziałanie przerwom w działalności biznesowej oraz ochrona krytycznych procesów biznesowych realizowanych przez infrastrukturę informatyczną i telekomunikacyjną.

   Procedura powinna opisywać:
   - identyfikację zagrożeń i sposobu ich ograniczania,
   - warunki uruchomienia procedur awaryjnych,
   - szczegółowy zakres obowiązków związany w wykonaniem każdego elementu planu,
   - wpływ, jaki przerwy w działaniu mogą wywrzeć na działalność biznesową firmy,
   - wytyczne dotyczące regularnego testowania i aktualizowania przyjętych planów,

   Procedura dotyczy następujących zasobów:
   - przełączniki sieciowe,
   - koncentratory, rutery,
   - konwertery światłowodowe,
   - urządzenia firewall,
   - okablowanie strukturalne
   - urządzenia i oprogramowanie dla obsługi telefonii IP (CallManager itp.)
   - farmy maszyn wirtualnych (VMware, Hyper-V itp.)
   - macierze dyskowe
3) Przeciwdziałanie przerwom w świadczeniu usług Data Center.

Procedura powinna opisywać:

- identyfikację zagrożeń i sposobu ich ograniczania,
- warunki uruchomienia procedury,
- szczegółowy zakres obowiązków związanych w wykonaniem każdego elementu planu,
- wpływ, jaki przerwy w działaniu mogą wywrzeć na działalność biznesową firmy,
- wytyczne dotyczące regularnych przeglądów i aktualizowania przyjętych planów.

Procedura powinna obejmować monitorowanie, testowanie i obsługę awarii:

- systemów klimatyzacji,
- systemów zasilania,
- ochrony przeciwpożarowej,
- łączności IT,
- zarządzania kontrolą dostępu,
- sprzętowa awarią serwerów.

4) Przeciwdziałanie przerwom w realizowaniu usługi monitorowania.
Procedura powinna opisywać:

- identyfikację zagrożeń i sposobu ich ograniczania,
- warunki uruchomienia procedury,
- szczegółowy zakres obowiązków związany w wykonaniem każdego elementu planu,
- wpływ, jaki przerwy w działaniu mogą wywrzeć na działalność biznesową firmy,
- wytyczne dotyczące regularnego testowania i aktualizowania przyjętych planów.

2. Procedura zapewnienia ciągłości działania środowiska dedykowane dla systemu e-drewno (oprogramowanie systemowe i bazodanowe).
    1) Procedura wykonania kopii zapasowych baz danych (backup) obejmująca:
        a) Wykonanie kopii zapasowych baz danych,
        b) Testowanie użyteczności ww. baz danych w procesie odtwarzania,
        c) Odtwarzanie środowiska w przypadku wystąpienia awarii z wykorzystanie ww. kopii bazy danych,
    2) Procedura wykonania kopii środowiska (serwerów / maszyn wirtualnych) obejmująca:
        a) Wykonanie kopii środowiska;
        b) Testowanie użyteczności ww. kopii środowiska i kopii baz danych w procesie odtwarzania. Testowanie przełączenia na zreplikowane środowisko e-drewno;
        c) Odtwarzanie środowiska w przypadku wystąpienia awarii z wykorzystaniem kopii środowiska i kopii baz danych.
3. Procedury zapewnienia ciągłości działania środowiska e-drewno powinny dokumentować informacje obejmujące:
    1) Osoby odpowiedzialne za realizację procedur zapewnienia ciągłości działania,
    2) Identyfikację zagrożeń i szacowanie ryzyka,
    3) Osoby o znaczeniu krytycznym dla ciągłości działań IT, zasady dyżurów oraz zastępstw osób wewnątrz organizacji i z firm zewnętrznych,

4) Przeszkolenie personelu w zakresie uzgodnionych awaryjnych procedur,
5) Kierunki techniczne zapewniające ciągłość działania,
6) Testowanie i aktualizację procedur.