Numer postępowania: MCOO/ZP/R/16/26

Załącznik nr 4 do SWZ

# Opis Przedmiotu Zamówienia

## Elektroniczny Obieg Dokumentów Kadrowo-Płacowych

1. **Zakres przedmiotu zamówienia**

1.1. **Zakres przedmiotu zamówienia obejmuje minimum:**

1.1.1. Udzielenie Zamawiającemu przez Wykonawcę licencji na system elektronicznego obiegu dokumentów w zakresie dokumentów kadrowo-płacowych,

1.1.2. Instalację i konfiguracja systemu elektronicznego obiegu dokumentów w zakresie kadrowo-płacowym.

1.1.3. Integrację systemu elektronicznego obiegu dokumentów w zakresie kadrowo-płacowym z systemem Elektronicznego obiegu dokumentów finansowo-księgowych, którego Zamawiający jest użytkownikiem.

1.1.4. Integrację elektronicznego obiegu dokumentów w zakresie kadrowo-płacowym z narzędziami utrwalana dokumentów na nośniku trwałym w tzw. technologii blockchain, których Zamawiający jest użytkownikiem,

1.1.5. Integrację obiegu dokumentów w zakresie kadrowo- płacowym z narzędziami podpisu elektronicznego opartego na technologii blockchain, którego Zamawiający jest użytkownikiem,

2. **Wymagania dotyczące Systemu**

2.1. **Wymagania obligatoryjne systemu obiegu danych w zakresie kadrowo-płacowym**

2.1.1. Całość rozwiązania jest napisana i pracuje w architekturze zorientowanej na usługi (SOA). Dla wszystkich obszarów funkcjonalnych wydzielona jest warstwa integracyjna odpowiedzialna za integrację z zewnętrznymi źródłami danych oraz udostępniająca im dane z systemu.

2.1.2. Dane systemu elektronicznego obiegu dokumentów w zakresie kadrowo-płacowym są przechowywane w relacyjnych bazach danych na serwerze SQL,

2.1.3. Podpisywanie dokumentów w Elektronicznym Obiegu Dokumentów kadrowo-płacowych musi odbywać się z wykorzystaniem podpisu elektronicznego opartego na technologii blockchain,

2.1.4. Aplikacje są uruchamiane i wdrażane zgodnie z modelem SaaS (Software as a Service),

2.2. **Wymagania fakultatywne systemu:**

2.2.1. System obiegu dokumentów kadrowo-płacowych musi posiadać możliwość podpisywania dokumentów za pomocą elektronicznego podpisu kwalifikowanego Certum Asseco, Szafir lub równoważnego.

2.3. **Cechy systemu**

2.3.1. System musi być skalowalny.

2.3.2. System elektronicznego obiegu dokumentów w zakresie kadrowo-płacowym musi pracować w architekturze trójwarstwowej – warstwa bazy danych, warstwa aplikacji i warstwa prezentacji.

2.3.3. System elektronicznego obiegu dokumentów w zakresie kadrowo-płacowym musi posiadać następujące cechy dostępne bezpośrednio, jako wbudowane właściwości produktu:

2.3.3.1. Interfejs użytkownika:

- Panel pracownika musi być prosty, przejrzysty i intuicyjny.
- Panel pracownika musi zapewnić przejrzystą nawigację pozwalającą przemieszczać się pomiędzy obszarami funkcjonalnymi.

2.3.4. System elektronicznego obiegu dokumentów w zakresie kadrowo-płacowym musi zostać zintegrowany z elektronicznym obiegiem dokumentów faktur i zabezpieczeń środków, którego Zamawiający jest użytkownikiem, w następującym zakresie:

2.3.4.1. Wspólnego logowania do systemu obiegu dokumentów zarówno dla modułu kadrowo-płacowego jak i modułu faktur i zabezpieczeń środków.

2.3.4.2. Słownika użytkowników

2.3.4.3. Słownika jednostek

2.3.4.4. Słownika budżetowych źródeł finansowania (zadania, rozdziały, paragrafy, rodzaje planów)

2.3.4.5. Planów finansowych (modułu do weryfikacji wykonania planów).

2.3.5. Elektroniczny obieg dokumentów kadrowo-płacowych musi zostać zintegrowany z podpisem elektronicznym, przy czym forma wykorzystania podpisu elektronicznego ma być konfigurowalna w konfiguracji systemu. Do wyboru użytkownika systemu ma być forma podpisu, przy czym dostępne mają być minimum dwie formy:

2.3.5.1. Podpis elektroniczny oparty o technologię blockchain (podpis chmurowy).

2.3.5.2. Podpis kwalifikowany Certum Asseco, Szafir lub równoważnego - wymagania fakultatywne.

2.3.6. Obieg dokumentów kadrowo-płacowych musi zostać zintegrowany z narzędziami utrwalana dokumentów na nośniku trwałym w tzw. technologii blockchain, których Zamawiający jest użytkownikiem,

2.3.7. Obieg dokumentów kadrowo-płacowych ma wykorzystywać pocztę elektroniczną do rozsyłania przez system wiadomości i powiadomień do użytkowników w postaci maili.

2.3.8. Obieg dokumentów kadrowo-płacowych musi pozwalać na jednoczesny dostęp do danych wielu użytkownikom oraz zapewniać ochronę tych danych przed utratą spójności lub zniszczeniem.

2.3.9. Komunikacja użytkownika z obiegiem dokumentów musi odbywać się za pomocą połączenia szyfrowanego SSL.

2.3.10. System musi uniemożliwiać wprowadzanie i modyfikację danych w sposób anonimowy.

3. **Wymagania technologiczne**

3.1. Dostarczone oprogramowanie musi uwzględnić środowisko rozwiązań informatycznych Zamawiającego.

3.2. Preferowana technologia systemu: AJAX, Język interpretowany PHP, baza danych MySQL, serwer WWW Apache.

3.3. Systemy mają działać w przeglądarce internetowej, technologia wykonania zapewniać ma minimalną ilość przeładowań strony (preferowana technologia – AJAX).

3.4. Dostarczone w ramach niniejszego zamówienia oprogramowanie musi poprawnie działać z następującymi przeglądarkami WWW w aktualnych wersjach odpowiednich dla poszczególnych systemów operacyjnych (przynajmniej Microsoft Edge, Mozilla Firefox, Google Chrome).

4. **Wymagania dotyczące rozbudowy systemu**

4.1. System musi być skalowalny, przy czym jego skalowanie może odbywać się przez:

4.1.1. dołączenie dodatkowych stanowisk - zwiększanie liczby użytkowników,

4.1.2. rozbudowę warstwy aplikacyjnej (zwiększenie zasobów serwera obsługującego warstwę poprzez rozbudowę pamięci, zwiększenie liczby procesorów oraz zwiększanie liczby maszyn),

4.1.3. rozbudowę warstwy bazodanowej (zwiększenie zasobów serwera obsługującego warstwę poprzez rozbudowę pamięci, zwiększenie liczby procesorów, zwiększenie pojemności pamięci masowych),

5. **Wymagania dotyczące bezpieczeństwa danych**

5.1. Rozwiązanie techniczne zastosowane w ramach systemów musi umożliwiać tworzenie kopii zapasowych (archiwizacja pełną i przyrostową) danych.

5.2. System musi mieć możliwość tworzenia kopii zapasowych wg dowolnego kalendarza, ale nie rzadziej niż raz dziennie. Kopia zapasowa musi mieć możliwość odtworzenia całego systemu po awarii do punktu wykonania ostatniej kopii bezpieczeństwa.

5.3. System musi zapewniać działania zgodnie z zasadami gwarantującymi taką eksploatację systemu, aby zapewniać bezpieczeństwo informacji rozumiane jako poufność, integralność i dostępność.

**Wymagania fakultatywne systemu:**

5.4. Rozwiązanie musi umożliwić zapis wszystkich czynności wykonywanych w systemie przez jego użytkowników, z możliwością jednoznacznego wskazania użytkownika, który wykonał daną czynność (rozliczalność).

6. **Wymagania licencyjne**

6.1. Wykonawca musi dostarczyć licencje na wskazaną przez Zamawiającego liczbę Jednostek.

6.2. Licencje na dostarczana dla jednostki musi pozwalać na dołączanie do systemu nieograniczonej liczby użytkowników w ramach danej licencji dla jednostki.

6.3. Licencja musi pozwalać na użytkowanie systemu przez Zamawiającego i obsługiwane przez niego Jednostki Oświatowe.

6.4. Wykonawca musi zagwarantować Zamawiającemu, że wykonanie przedmiotu zamówienia nie spowoduje naruszenia przez Wykonawcę lub Zamawiającego praw autorskich innych podmiotów, znaków handlowych i towarowych, patentów, know–how oraz innych praw chronionych oraz, że Wykonawca uprawniony jest do udzielenia lub dostarczenia Zamawiającemu licencji na dostarczone w ramach systemu oprogramowanie.

6.5. Wykonawca musi przyjąć na siebie wszelką odpowiedzialność za roszczenia osób trzecich w związku z realizacją umowy, a w szczególności dotyczące naruszenia praw autorskich innych podmiotów, znaków handlowych i towarowych, patentów, know–how oraz innych praw chronionych.

6.6. Zamawiający lub podmiot przez niego wskazany uprawniony jest do wykonywania kopii bezpieczeństwa licencjonowanego oprogramowania objętego przedmiotem zamówienia.

6.7. Udzielona licencja, z zastrzeżeniem spraw inaczej uregulowanych, uprawnia zamawiającego do korzystania z systemu na następujących polach eksploatacji:

6.7.1. sporządzenie kopii zapasowej,

6.7.2. przechowywanie,

6.7.3. ładowanie,

6.7.4. instalacja,

6.7.5. uruchamianie i wyświetlanie.

7. **Wymagania w zakresie administracja i bezpieczeństwo**

7.1. System elektronicznego obiegu dokumentów kadrowo-płacowych musi pozwalać na zmianę parametrów wykonywaną przez administratora systemu bez interwencji Wykonawcy,

7.2. System elektronicznego obiegu dokumentów kadrowo-płacowych musi dawać możliwość zdefiniowania wielopoziomowej struktury organizacyjnej, składającej się co najmniej
z jednostek organizacyjnych i stanowisk w dowolnej liczbie.

7.3. System elektronicznego obiegu dokumentów kadrowo-płacowych musi pozwalać na zdefiniowanie polityki bezpieczeństwa (poziom skomplikowania hasła, okres ważności hasła, powtarzalność hasła),

7.4. System elektronicznego obiegu dokumentów kadrowo-płacowych musi posiadać panel administracyjny dostępny z poziomu strony WWW.

7.5. System elektronicznego obiegu dokumentów kadrowo-płacowych w zakresie administracja i bezpieczeństwo ma posiadać dostęp do następujących funkcjonalności:

7.5.1. uwierzytelnienie,

7.5.2. inicjowanie sesji,

7.5.3. wylogowanie.

7.6. System elektronicznego obiegu dokumentów kadrowo-płacowych musi pozwalać na definiowania słowników systemowych oraz ustawiania poszczególnych wpisów w słownikach, co najmniej na "aktywny", "nieaktywny".

7.7. Dostęp do systemu elektronicznego obiegu dokumentów kadrowo-płacowych odbywa się po zabezpieczonym i szyfrowanym łączu z wykorzystaniem certyfikatu SSL.

8. **Ogólne wymagania funkcjonalne dla obiegu dokumentów kadrowo-płacowych**

8.1. System obiegu dokumentów kadrowo-płacowych musi spełniać następujące wymagania podstawowe.

8.1.1. Zapewnia obsługę dokumentacji kadrowo-płacowej pomiędzy Zamawiającym jako podmiotem obsługującym a Jednostkami Oświatowymi będącymi obsługiwanymi przez Zamawiającego.

8.1.2. Posiada funkcję wprowadzenia obrazu oryginalnego dokumentu w postaci obrazu lub skanu, jako załącznika do formatki obiegu dokumentu. Maksymalna wielkość dodawanego pliku nie może przekraczać 4 MB.

8.1.3. Dostęp do systemu i rejestracja elektronicznych dokumentów w obiegu dokumentów musi odbywać się z wykorzystaniem przeglądarki WWW,

8.1.4. Posiada zestaw raportów dotyczących aktywności obsługi obiegu dokumentów,

8.1.5. Posiada wyszukiwanie dokumentów po wielu kryteriach równocześnie,

8.1.6. Posiada funkcję obsługi statusów dokumentów,

8.1.7. Posiada możliwość podpisywania dokumentów podpisem elektronicznym opartym na technologii blockchain,

8.1.8. Posiada podgląd listy załączników (plików) oraz funkcję pobrania i zapisania załącznika,

8.1.9. Posiada funkcję uniemożliwiającą zmianę dokumentu po określonych stopniach zatwierdzeń.

**Wymagania fakultatywne systemu:**

8.1.10. Możliwość dodawania przez użytkownika informacji opisujących poszczególne dokumenty, przesyłki lub sprawy w postaci notatek lub komentarzy.

8.2. **Modułowość systemu**

8.2.1. System musi posiadać funkcjonalności w postaci odrębnych modułów lub umożliwiać jasną kategoryzację dokumentów na minimum następujące kategorie:

- Dokumenty z Jednostek Obsługiwanych
- Dokumenty dla Jednostek Obsługiwanych
- Listy Płac pracowników Jednostek Obsługiwanych

8.2.2. Dostęp do każdej z nich ustalany ma być za pomocą odpowiednio skonfigurowanych uprawnień użytkownika systemu.

**Workflow**

9. **Wymagania w zakresie workflow**

9.1. System zapewnia edytowalny słownik stanowisk umożliwiający co najmniej wykaz:

- opisujących dokumenty,
- weryfikujących dokumenty,
- zatwierdzających dokumenty,
- możliwość odwzorowania struktury organizacyjnej.

9.2. System posiada mechanizm e-mailowy powiadamiający użytkownika o wystąpieniu zdarzeń w systemie,

9.3. System posiada mechanizm kontroli obejmujący co najmniej:

- statusu dokumentu,
- czas utworzenia dokumentu,
- czas zatwierdzenia dokumentu na poszczególnych etapach workflow,
- czas podpisania dokumentu podpisem elektronicznym,
- numerację dokumentów jednoznacznie wskazującą na miejsce powstawiania dokumentu (unikatowy identyfikator, seria itp.) w elektronicznym obiegu dokumentów zawierającą co najmniej:
    - oznaczenie jednostki tworzącej dokument
    - rok, miesiąc utworzenia dokumentów
    - inny sposób wyraźnie identyfikujący dokument w systemie obiegu dokumentów.

9.4. Uprawnienia do etapów workflow

9.4.1. Dostęp do wybranych etapów workflow odbywać się ma za pomocą definiowania uprawnień użytkownika w panelu administracyjnym systemu.

9.4.2. W konfiguracji systemu będzie możliwość zdefiniowania konieczności wykorzystywania przez użytkowników podpisu elektronicznego opartego na technologii blockchain w celu akceptowania dokumentów na wybranych etapach workflow.

**Moduł List Płac i Dokumentów kadrowo-płacowych**

10. **Wymagania szczegółowe systemu**

10.1. Wymagania w zakresie konfiguracji formularzy kadrowo-płacowych

10.1.1. Formularze kadrowo-płacowe muszą być podzielone na co najmniej trzy typy:

- Listy płac
- Dokumenty kadrowo-płacowe wysyłane z Jednostki Obsługiwanej do Zamawiającego
- Dokumenty kadrowo-płacowe wysyłane od Zamawiającego do Jednostki Obsługiwanej

10.1.2. Wymagania szczegółowe dotyczące pól i funkcjonalności formularza listy płac.

10.1.3. System zapewnia rejestrację dokumentu listy płac w postaci formularza, który musi mieć możliwość rejestracji poszczególnych etapów akceptacji dokumentu i zawierać następujące pola i funkcjonalności:

- numer dokumentu listy płac – automat do nadawania numerów zgodnie z miejscem przeznaczenia dokumentu listy płac oznaczającym Jednostkę Oświatową będącą odbiorcą formularza,
- nazwę jednostki, dla której formatka listy płac jest sporządzana i przekazywana do akceptacji (combobox z danymi słownikowymi z konfiguracji systemu),
- numer listy płac z systemu płacowo-kadrowego,
- datę płatności listy płac z możliwością wykorzystania kalendarza systemowego (polski kalendarz) do wypełnienia danych,
- opis merytoryczny listy płac – pole tekstowe,
- Dodawanie oryginału dokumentu listy płac w postaci załącznika w wersji elektronicznej w formacie pdf, jpg, png, tiff, przy czym załącznik nie może być większy niż 4 MB.
- Podgląd załączonego oryginału dokumentu listy płac z możliwością pobrania i zapisania go na komputerze końcowym użytkownika,
- Akceptacja dokumentu podpisem elektronicznym w technologii blockchain.
- Potwierdzenie akceptacji formatki listy płac przez użytkownika w formacie:
    - Data akceptacji
    - Godzina akceptacji
    - Imię nazwisko użytkownika

    - W przypadku podpisu elektronicznego w technologii blockchain odpowiedni zapis o wykonaniu podpisu z oznaczeniem daty podpisania oraz imienia i nazwiska osoby dokonującej podpisu.
- Utrwalanie dokumentu na nośniku trwałym z wykorzystaniem technologii blockchian, którego to rozwiązania zamawiający jest użytkownikiem.

10.1.4. Wymagania szczegółowe dotyczące pól i funkcjonalności formularza załącznika wysyłanego z Jednostki Obsługiwanej do Zamawiającego.

10.1.5. System zapewnia rejestrację dokumentu załącznika wysyłanego z Jednostki Obsługiwanej do Zamawiającego w postaci formularza, który musi mieć możliwość rejestracji poszczególnych etapów akceptacji dokumentu i zawierać następujące pola i funkcjonalności:

- numer załącznika kadrowo-płacowego – automat do nadawania numerów zgodnie z miejscem przeznaczenia dokumentu załącznika wysyłanego z Jednostki Obsługiwanej do Zamawiającego oznaczającym Jednostkę Oświatową będącą nadawcą formularza,
- opis merytoryczny załącznika wysyłanego z Jednostki Obsługiwanej do Zamawiającego – pole tekstowe,
- Dodawanie oryginału dokumentu załącznika wysyłanego z Jednostki Obsługiwanej do Zamawiającego w postaci załącznika w wersji elektronicznej w formacie pdf, jpg, png, tiff, przy czym załącznik nie może być większy niż 4 MB.
- Podgląd załączonego oryginału dokumentu załącznika wysyłanego z Jednostki Obsługiwanej do Zamawiającego z możliwością pobrania i zapisania go na komputerze końcowym użytkownika,
- Akceptacja dokumentu.
- Potwierdzenie akceptacji formatki listy płac przez użytkownika w formacie:
    - Data akceptacji
    - Godzina akceptacji
    - Imię nazwisko użytkownika
- Utrwalanie dokumentu na nośniku trwałym z wykorzystaniem technologii blockchian, którego to rozwiązania zamawiający jest użytkownikiem.

10.1.6. Wymagania szczegółowe dotyczące pól i funkcjonalności formularza załącznika kadrowo-płacowego wysyłanego od Zamawiającego do Jednostki Obsługiwanej.

10.1.7. System zapewnia rejestrację dokumentu załącznika kadrowo-płacowego wysyłanego od Zamawiającego do Jednostki Obsługiwanej w postaci formularza,

który musi mieć możliwość rejestracji poszczególnych etapów akceptacji dokumentu i zawierać następujące pola i funkcjonalności:

- numer załącznika kadrowo-płacowego – automat do nadawania numerów zgodnie z miejscem przeznaczenia dokumentu załącznika kadrowo-płacowego wysyłanego od Zamawiającego do Jednostki Obsługiwanej oznaczającym Jednostkę Oświatową będącą odbiorcą formularza,
- Nazwę jednostki obsługiwanej (combobox z danymi słownikowymi z konfiguracji systemu),
- opis merytoryczny załącznika kadrowo-płacowego wysyłanego od Zamawiającego do Jednostki Obsługiwanej – pole tekstowe,
- Dodawanie oryginału dokumentu załącznika kadrowo-płacowego wysyłanego od Zamawiającego do Jednostki Obsługiwanej w postaci załącznika w wersji elektronicznej w formacie pdf, jpg, png, tiff, przy czym załącznik nie może być większy niż 4 MB.
- Podgląd załączonego oryginału dokumentu załącznika kadrowo-płacowego wysyłanego od Zamawiającego do Jednostki Obsługiwanej z możliwością pobrania i zapisania go na komputerze końcowym użytkownika,
- Akceptacja dokumentu.
- Potwierdzenie akceptacji formatki listy płac przez użytkownika w formacie:
    - Data akceptacji
    - Godzina akceptacji
    - Imię nazwisko użytkownika
- Utrwalanie dokumentu na nośniku trwałym z wykorzystaniem technologii blockchian, którego to rozwiązania Zamawiający jest użytkownikiem.

**Wymaganie fakultatywne systemu:**

10.1.8. Mechanizm konfigurowania dodatkowych pól w formie atrybutów do formatki listy płac, załącznika wysyłanego z Jednostki Oświatowej do Zamawiającego, załącznika od Zamawiającego do Jednostki Oświatowej, przy czym atrybuty muszą mieć minimalnie następujące funkcjonalności i rodzaje:

- Funkcjonalności
    - Możliwość konfigurowania wyświetlania atrybutu w odpowiednim kroku procedury akceptacji dokumentu,

- Możliwość konfigurowania obowiązku wypełnienia atrybutu w celu zatwierdzenia dokumentu na wskazanym kroku procedury akceptacji dokumentu,

- Możliwość konfigurowania rodzaju pola, które pełnić będzie rolę atrybuty, przy czym pole to musi obejmować minimalnie następujące rodzaje:
    - Selectbox,
    - Selectbox z możliwością pobrania danych do pola z pomocą kwerendy SQL,
    - Pole tekstowe,
    - Pole numeryczne,
    - Pole daty (z funkcją wykorzystania kalendarza do wyboru daty),
    - Pole etykiety grupy,

10.1.9. Opisanie dokumentu listy płac pod kątem źródeł finansowania, które muszą być przedstawione w formie tabeli i muszą zawierać co najmniej:

- Dane szczegółowe dotyczące źródeł finansowania dokumentu zakupu, które muszą być przedstawione w formie tabeli i muszą zawierać co najmniej:
    - Rodzaj Planu finansowego (combobox z danymi słownikowymi z konfiguracji systemu),
    - Rejestr planu finansowego (combobox z danymi słownikowymi z konfiguracji systemu),
    - Numer i nazwa rozdziału combobox z danymi słownikowymi z konfiguracji systemu),
    - Numer i nazwę paragrafu combobox z danymi słownikowymi z konfiguracji systemu),
    - Symbol i nazwę zadania combobox z danymi słownikowymi z konfiguracji systemu),
    - Stawkę podatku VAT combobox z danymi słownikowymi z konfiguracji systemu),
    - Kwotę listy płac,

10.1.10. Pola pozwalające na określenia kategorii załączników wysyłanych z Jednostki Oświatowej do Zamawiającego, jak i załącznika od Zamawiającego do Jednostki Oświatowej, przy czym konfiguracja musi pozwalać na minimum następujące funkcjonalności:

- Określenie kategorii dokumentu, combobox z danymi słownikowymi z konfiguracji systemu, przy czym minimalne kategorie dokumentów to:

- Umowa o pracę,
- Zajęcie komornicze,
- Zaświadczenie o dochodach,
- Lista płac pracowników oświatowych,
- Lista płac pracowników administracyjnych,

10.1.11. Możliwość dodawania przez użytkownika informacji opisujących poszczególne dokumenty w postaci notatek lub komentarzy.

10.1.12. Możliwość dodawania przez użytkownika załączników do komentarzy w postaci dokumentu w wersji elektronicznej w formacie pdf, jpg, png, tiff, które stanowić będą załącznik do komentarza, przy czym załącznik nie może być większy niż 2 MB.

10.1.13. Możliwość drukowania dokumentu listy płac w postaci umożliwiającej wykorzystanie wydruku, jako elementy potwierdzającego podpisanie dokumentu podpisem elektronicznym, przy czy wydruk musi posiadać minimum następujące pola:

- Zatwierdzenie przez Dyrektora Zamawiającego.
- Zatwierdzenie przez Dyrektora Jednostki obsługiwanej przez Zamawiającego
- Zatwierdzenie przez Głównego Księgowego Zamawiającego
- Potwierdzenie, (Zatwierdzenie) sprawdzenie pod względem formalno-rachunkowym (kierownik działu wynagrodzeń Zamawiającego)
- Potwierdzenie środków w planie finansowym przez pracownika Zamawiającego
- Potwierdzenie pod względem merytorycznym przez Dyrektora Jednostki lub upoważnionego pracownika,
- Sporządzający, pracownik Zamawiającego

**Schemat akceptacji formatek kadrowo płacowych**

10.1.14. System ma pozwalać na import raportów list płac z Zintegrowanego Systemu Zarządzania Oświatą, którego Zamawiający jest użytkownikiem, z wykorzystaniem pliku xls,
w oparciu o następujące elementy i funkcjonalności:

- podział na rodzaj budżetu, paragrafy, rozdziały i pozycje,
- numer dokumentu listy płac,

- rodzaj listy,
- miesiąc i rok,
- odpowiednią klasyfikację budżetową.

10.1.15. Import będzie odbywać się z wykorzystaniem pliku xls, który będzie wynikiem eksportu danych z Zintegrowanego Systemu Zarządzania Oświatą.

10.1.16. Do zaimportowania dokumentu dostępny będzie przycisk, hiperłącze lub inny element nawigacyjny (odsyłacz) pozwalający na pobranie pliku ze wskazanej przez użytkownika lokalizacji.

10.1.17. Akceptacja formularzy kadrowo-płacowych musi odbywać się według następujących etapów schematu:

10.1.17.1. Dla list płac:

- Sporządzenie listy płac – wprowadzenie do systemu obiegu dokumentów (pracownik Zamawiającego). W tym etapie wymagane są minimum następujące informacje:
  - nazwę jednostki, dla której formatka listy płac jest sporządzana i przekazywana do akceptacji,
  - numer listy płac z systemu płacowo-kadrowego,
  - datę płatności listy płac,
  - opis merytoryczny listy płac,
  - oryginał dokumentu listy płac w postaci załącznika w wersji elektronicznej,
  - Podgląd załączonego oryginału dokumentu kosztowego z możliwością pobrania
    i zapisania go na komputerze końcowym użytkownika,
  - Opisanie dokumentu listy płac pod kątem źródeł finansowania, które muszą być przedstawione w formie tabeli (o ile Wykonawca spełniać będzie funkcjonalność dodatkową)
  - Potwierdzenie akceptacji formatki listy płac przez użytkownika w formacie:
    - Data akceptacji
    - Godzina akceptacji
    - Imię nazwisko użytkownika
- sprawdził pod względem merytorycznym (pracownik/dyrektor Jednostki obsługiwanej przez Zamawiającego). W tym etapie wymagane są minimum następujące informacje:

- Akceptacja dokumentu podpisem elektronicznym w technologii blockchain
- Potwierdzenie akceptacji formatki listy płac przez użytkownika w formacie:
    - Data akceptacji
    - Godzina akceptacji
    - Imię nazwisko użytkownika
- W przypadku podpisu blockchain, odpowiedni zapis o wykonaniu podpisu z oznaczeniem daty podpisania oraz imienia i nazwiska osoby dokonującej podpisu.
- Utrwalanie dokumentu na nośniku trwałym z wykorzystaniem technologii blockchian, którego to rozwiązania zamawiający jest użytkownikiem.

- sprawdził pod względem zabezpieczenia planu (pracownik księgowości Zamawiającego). W tym etapie wymagane są minimum następujące informacje:
- Akceptacja dokumentu podpisem elektronicznym w technologii blockchain.
- Potwierdzenie akceptacji formatki listy płac przez użytkownika w formacie:
    - Data akceptacji
    - Godzina akceptacji
    - Imię nazwisko użytkownika

- W przypadku podpisu blockchain, odpowiedni zapis o wykonaniu podpisu z oznaczeniem daty podpisania oraz imienia i nazwiska osoby dokonującej podpisu.
- Utrwalanie dokumentu na nośniku trwałym z wykorzystaniem technologii blockchian, którego to rozwiązania zamawiający jest użytkownikiem.

- sprawdził pod względem formalno-rachunkowym (kierownik działu wynagrodzeń Zamawiającego). W tym etapie wymagane są minimum następujące informacje:
- Akceptacja dokumentu podpisem elektronicznym w technologii blockchain.
- Potwierdzenie akceptacji formatki listy płac przez użytkownika w formacie:
    - Data akceptacji
    - Godzina akceptacji
    - Imię nazwisko użytkownika

- W przypadku podpisu elektronicznego blockchain, odpowiedni zapis o wykonaniu podpisu z oznaczeniem daty podpisania oraz imienia i nazwiska osoby dokonującej podpisu.
- Utrwalanie dokumentu na nośniku trwałym z wykorzystaniem technologii blockchian, którego to rozwiązania zamawiający jest użytkownikiem.
    - Zatwierdzenie przez Głównego Księgowego Zamawiającego. W tym etapie wymagane są minimum następujące informacje:
    - Akceptacja dokumentu kwalifikowalnym podpisem elektronicznym,
    - Potwierdzenie akceptacji formatki listy płac przez użytkownika w formacie:
        - Data akceptacji
        - Godzina akceptacji
        - Imię nazwisko użytkownika
- W przypadku kwalifikowanego podpisu elektronicznego odpowiedni zapis o wykonaniu podpisu z oznaczeniem daty podpisania oraz imienia i nazwiska osoby dokonującej podpisu.
- Utrwalanie dokumentu na nośniku trwałym z wykorzystaniem technologii blockchian, którego to rozwiązania zamawiający jest użytkownikiem.
    - zatwierdzenie przez dyrektora Jednostki obsługiwanej przez Zamawiającego. W tym etapie wymagane są minimum następujące informacje:
    - Akceptacja dokumentu kwalifikowalnym podpisem elektronicznym.
    - Potwierdzenie akceptacji formatki listy płac przez użytkownika w formacie:
        - Data akceptacji
        - Godzina akceptacji
        - Imię nazwisko użytkownika
- W przypadku podpisu kwalifikowalnym podpisem elektronicznym odpowiedni zapis o wykonaniu podpisu z oznaczeniem daty podpisania oraz imienia i nazwiska osoby dokonującej podpisu.
- Utrwalanie dokumentu na nośniku trwałym z wykorzystaniem technologii blockchian, którego to rozwiązania zamawiający jest użytkownikiem.
    - Zatwierdzenie przez Dyrektora Zamawiającego. W tym etapie wymagane są minimum następujące informacje:
    - Akceptacja dokumentu kwalifikowanym podpisem elektronicznym.

- Potwierdzenie akceptacji formatki listy płac przez użytkownika w formacie:
    - Data akceptacji
    - Godzina akceptacji
    - Imię nazwisko użytkownika

- W przypadku podpisu kwalifikowalnym podpisem elektronicznym odpowiedni zapis o wykonaniu podpisu z oznaczeniem daty podpisania oraz imienia i nazwiska osoby dokonującej podpisu.
- Utrwalanie dokumentu na nośniku trwałym z wykorzystaniem technologii blockchian, którego to rozwiązania zamawiający jest użytkownikiem.

10.1.17.2. Dla załącznika wysyłanego z Jednostki Obsługiwanej do Zamawiającego:

- Sporządzenie dokumentu przez pracownika Jednostki obsługiwanej. W tym etapie wymagane są minimum następujące informacje:

- opis merytoryczny załącznika wysyłanego z Jednostki Obsługiwanej do Zamawiającego,
- oryginał dokumentu załącznika wysyłanego z Jednostki Obsługiwanej do Zamawiającego w postaci załącznika w wersji elektronicznej,
- Podgląd załączonego oryginału dokumentu kosztowego z możliwością pobrania i zapisania go na komputerze końcowym użytkownika,
- Określenia kategorii wysyłanych załączników,
- Potwierdzenie akceptacji formatki listy płac przez użytkownika w formacie:
    - Data akceptacji
    - Godzina akceptacji
    - Imię nazwisko użytkownika

- Zatwierdzenie dokumentu przez pracownika Zamawiającego (potwierdzenie przyjęcia do realizacji). W tym etapie wymagane są minimum następujące informacje:
    - Potwierdzenie akceptacji załącznika przez użytkownika w formacie:
        - Data akceptacji
        - Godzina akceptacji
        - Imię nazwisko użytkownika

10.1.17.3. Dla załącznika kadrowo-płacowego wysyłanego od Zamawiającego do Jednostki Obsługiwanej:

- Sporządzenie dokumentu przez pracownika Zamawiającego. W tym etapie wymagane są minimum następujące informacje:

- Nazwa jednostki będącej adresatem formularza załącznika kadrowo-płacowego wysyłanego od Zamawiającego do Jednostki Obsługiwanej,
- opis merytoryczny załącznika kadrowo-płacowego wysyłanego od Zamawiającego do Jednostki Obsługiwanej,
- oryginał dokumentu załącznika kadrowo-płacowego wysyłanego od Zamawiającego do Jednostki Obsługiwanej w postaci załącznika w wersji elektronicznej,
- Podgląd załączonego oryginału dokumentu kosztowego z możliwością pobrania i zapisania go na komputerze końcowym użytkownika,
- Określenia kategorii wysyłanych załączników,
    - Potwierdzenie akceptacji formatki listy płac przez użytkownika w formacie:
        - Data akceptacji
        - Godzina akceptacji
        - Imię nazwisko użytkownika

    - Zatwierdzenie dokumentu przez pracownika jednostki obsługiwanej (potwierdzenie przyjęcia do realizacji). W tym etapie wymagane są minimum następujące informacje:
    - Potwierdzenie akceptacji załącznika przez użytkownika w formacie:
        - Data akceptacji
        - Godzina akceptacji
        - Imię nazwisko użytkownika

**Wymaganie fakultatywne systemu:**

- Mechanizm grupowego akceptowania formatek listy płac z wykorzystaniem kwalifikowanego podpisu elektronicznego na następujących etapach akceptacji listy płac:
    - Zatwierdzenie przez Głównego Księgowego Zamawiającego
    - Zatwierdzenie przez dyrektora Jednostki obsługiwanej przez Zamawiającego
    - Zatwierdzenie przez Dyrektora Zamawiającego

- Mechanizm akceptacji grupowej ma być przygotowany w postaci grupy dokumentów wybieranych z listy dokumentów do akceptacji w procesie workflow.
- Mechanizm grupowej akceptacji dokumentów ma pozwalać na jednoczesne zaakceptowanie wielu dokumentów w obiegu dokumentów z równoczesnym podpisaniem go z wykorzystaniem kwalifikowanego podpisu elektronicznego.

**Integracja z blockchain**

11. Integracja systemu elektronicznego obiegu dokumentów z narzędziami utrwalania dokumentów na nośniku trwałym w tzw. technologii blockchain.

11.1. Integracja pomiędzy systemem elektronicznego obiegu dokumentów a narzędziem utrwalania dokumentów na nośniku trwałym w tzw. technologii blockchain (dalej BlockChain) ma odbyć się z wykorzystaniem interfejsu RESTApi.

11.2. Zakres wdrożenia obejmuje Integrację w zakresie synchronizacji dokumentów pomiędzy BlockChain a systemem obiegu dokumentów w zakresie kadrowo - płacowym

11.3. Integracja musi obejmować:

11.3.1. Stworzenie mechanizmów współpracujących z BlockChain.

11.3.2. Realizację podpisu elektronicznego opartego o technologię blockchain

11.4. Cechy systemu elektronicznego obiegu dokumentów kadrowo-płacowych po integracji:

11.4.1. System po integracji będzie musiał posiadać następujące cechy w interfejsie produktu dostępne bezpośrednio, jako wbudowane właściwości produktu:

11.4.1.1. Przycisk, hiperłącze lub inny element nawigacyjny (odsyłacz) pozwalający na bezpośrednie utrwalenie formatki dokumentu listy płac oraz dokumentów kadrowo-płacowych (załączników od i do jednostki obsługiwanej) w sieci BlockChain.

11.4.1.2. Informację o utrwaleniu dokumentu na sieci BlockChain prezentującą co najmniej następujące dane:

- Numer Klucza sha lub skrót hash dokumentu, który jest identyfikatorem formatki
  w sieci BlockChain
- Datę, godzinę, minutę utrwalenia dokumentu w sieci

**Wymaganie fakultatywne systemu:**

11.4.1.3. Przycisk, hiperłącze lub inny element nawigacyjny (odsyłacz) pozwalający na weryfikację integralności dokumentu oraz jego autentyczność, przy czym efektem weryfikacji musi być informacja zawierająca co najmniej następujące informacje:

- Datę utrwalenia
- Godzinę, minutę oraz sekundę, w której dokument został utrwalony
- Informację o ewentualnym naruszeniu integralności dokumentu, jeśli jego treść została zmanipulowana po utrwaleniu.

11.4.1.4. Utrwalanie formatki dokumentu listy płac oraz dokumentów kadrowo-płacowych (załączników od i do jednostki obsługiwanej) w sieci BlockChain może odbywać się w sposób automatyczny w momencie akceptacji dokumentu i wykonania podpisu elektronicznego w technologii blockchain.

11.5. Zintegrowane komponenty muszą komunikować się z serwerami Zamawiającego
w sposób zapewniający poufność danych. Rozwiązanie musi mieć możliwość pracy
z wykorzystaniem protokołu SSL, w szczególności wymaganie dotyczy pracy użytkowników
z sieci zewnętrznej.

11.6. System musi uniemożliwiać wprowadzanie i modyfikację danych w sposób anonimowy.

11.7. Przeprowadzona integracja musi być skalowalna, przy czym jej skalowanie może odbywać się przez dołączenie dodatkowych formatek, które wymagać mogą utrwalenia formatki dokumentu kadrowego lub płacowego w sieci BlockChain,

**11.8. Wymagania szczegółowe w zakresie szkoleń użytkowników z działania systemu obiegu dokumentów kadrowo-płacowych**

11.8.1. Zmawiający wymagał przeprowadzenia szkoleń w zakresie sposobu korzystania z funkcjonalności systemu obiegu dokumentów kadrowo-płacowych po wykonaniu konfiguracji, wdrożenia i integracji.

11.8.2. Szkolenia mają zostać podzielone na 3 kategorie:

11.8.2.1. Szkolenia dla pracowników działu kadrowo-płacowego

11.8.2.2. Szkolenia dla pracowników obsługiwanych jednostek

11.8.2.3. Szkolenia dla administratorów systemu.

11.8.3. Forma, miejsca i terminy szkoleń będą uzgodnienie z  Zamawiającym.

11.8.4. Na zakończeniu szkoleń Wykonawca będzie musiał przekazać Zamawiającemu dokumentacje w postaci:

11.8.4.1. Instrukcja Użytkownika,

11.8.4.2. Instrukcja Administratora.

**Wymagania techniczne systemu**

1. System musi rejestrować czynności związane z poszczególnym dokumentem (np. dekretacji) w postaci historii, przypisując jednoznacznie odpowiedzialność za każdą czynność i dając możliwość szybkiego odczytania tych informacji.
2. System musi zapewniać wysoki stopień bezpieczeństwa i poufności dla zgromadzonych dokumentów oraz danych
3. Administrator powinien mieć możliwość konfiguracji jednostek obsługiwanych (nadanie nazw jednostek, adresu itp.) oraz prawo nadawania uprawnień dla jednostek obsługiwanych.
4. Administrator powinien mieć możliwość konfiguracji uprawnień dostępu do jednostek dla zamawiającego
5. Musi istnieć mechanizm zapewniający bezpieczeństwo danych oraz mechanizmy autoryzacji przez logowanie do aplikacji (z wykorzystaniem uwierzytelniania dwuskładnikowego za pomocą hasła + jednorazowy token wysyłany na email, oraz w opcji jednorazowy token wysyłany na telefon)
6. Dostęp do poszczególnych modułów musi być możliwy przez wyposażenie w funkcje zarządzania rolami użytkowników (przydzielania lub odbieranie uprawnień do poszczególnych modułów i funkcji, a także aktywowanie lub blokowanie kont użytkowników przez Administratora).
7. System powinien dawać możliwość wymuszania zmiany hasła, aby użytkownicy musieli zmieniać hasło w określonym odstępie czasu. System musi też umożliwiać skonfigurowanie wymuszania stosowania tzw. twardego hasła, np. wymuszając stosowanie wielkich i małych liter, cyfr itp. System musi tez umożliwiać definiowanie minimalną długość hasła dla użytkowników systemów
8. System powinien dawać możliwość automatycznej blokady konta po ustalonym przez zamawiającego czasie od ostatniego momentu logowania (np. po 6 miesiącach od momentu ostatniego logowania )
9. System powinien dawać możliwość ustawienia automatycznej blokady konta po wpisaniu nieprawidłowych poświadczeń tzw. Blokada typu miękkiego np. po 5 próbach zalogowania na czas min. 10 minut,

10. System powinien dawać możliwość ustawienia automatycznej blokady konta po wpisaniu nieprawidłowych poświadczeń  tzw. Blokada typu twardego np. po 2 pełnych próbach zalogowania typu miękkiego tj 10 próbach logowania.
11. System powinien  stosować bezpieczny algorytm haszujący do przechowywania haseł
12. System powinien korzystać ze słownika haseł opublikowanych przez CERT POLSKA będącą wynikiem analizy danych upublicznionych w wyciekach. Ma służyć przy wdrożeniu polityki haseł zgodnej z zaleceniami oraz uniemożliwiać stosowanie haseł które zostały opublikowanej na tej liście. (https://cert.pl/uploads/2022/01/hasla/resources/wordlist_pl.zip)
13. Aplikacja musi być dostępna przez przeglądarkę www oraz być dostępna wyłącznie przez szyfrowane połączenie. Aplikacja musi mieć możliwość definiowania zgodnie z Polityką bezpieczeństwa zamawiającego - czasu wygaszania sesji dostępu do aplikacji po określnym czasie nieaktywności.
14. Interfejs aplikacji biznesowych powinien być w języku polskim.
15. System powinien mieć możliwość wdrożenia n/w zasad dla systemu uwierzytelniającego użytkownika:
    - POWINIEN stosować bezpieczny algorytm hashujący do przechowywania haseł
    - NIE POWINIEN pozwalać na ustawienie hasła znajdującego się na liście słabych/często używanych haseł
    - NIE POWINIEN pozwalać na ustawienie hasła zawierającego przewidywalne człony (np. nazwa firmy, usługi)
    - POWINIEN ustalać minimalną długość hasła
    - POWINIEN pozwalać na ustawienie hasła o długości co najmniej do 64 znaków
16. Zarządzanie uprawnieniami powinno umożliwiać również ograniczenie uprawnień do danej jednostki obsługiwanej. Przykładowo użytkownik obsługujący rolą Dyrektor jednostki obsługiwanej  powinien mieć uprawnienia jedynie do swojej jednostki, którą obsługuje.
17. Administrator powinien mieć możliwość włączenia i wyłączenia powiadomień e-mailowych dotyczące wykonywanych operacji dla różnych modułów  dla zamawiającego.
18. Wymagania dot. Kopii bezpieczeństwa

1) System powinien być zabezpieczony tworzeniem kopii bezpieczeństwa danych zgromadzonych w aplikacji.
2) System musi posiadać mechanizmy zabezpieczające dane przed skutkami awarii serwera (systematyczny automatyczny backup danych).
3) Backup musi być wykonywany tak, aby zapewnić parametry:
    a) RTO (czas niezbędny do odtworzenia danych): 4 godziny
    b) RPO (termin wykonania ostatniej kopii): 24 godziny
        a) Okres przechowywanie kopii zapasowych: min 7 dni

19. W ramach interfejsu Użytkownik musi posiadać możliwość korzystania ze wszystkich funkcjonalności systemu, które są dla niego udostępnione zgodnie z przypisanymi mu uprawnieniami.

20. Wdrożenie systemu obejmie:

1. Instruktaże oraz asystę stanowiskową dla administratora systemu polegająca na:
    a. przeprowadzeniu instruktażu obsługi systemu bądź jego części wspomagającego obsługę obszarów działalności zamawiającego dla wskazanych przez zamawiającego pracowników;
    b. przeprowadzeniu instruktażu w zakresie zarządzania użytkownikami i uprawnieniami dla osób pełniących obowiązki administratorów systemu wskazanych przez zamawiającego.

2. Zapewnienie opieki powdrożeniowej systemu w okresie realizacji projektu polegającej na:
    a. świadczeniu pomocy technicznej,
    b. świadczeniu usług utrzymania i konserwacji dla dostarczonego systemu
    c. świadczeniu telefonicznie usług doradztwa i opieki w zakresie eksploatacji systemu.
    d. podejmowaniu czynności związanych z diagnozowaniem problemów oraz usuwaniem przyczyn nieprawidłowego funkcjonowania dostarczonego rozwiązania.

3. Po wdrożeniu Wykonawca przekaże Zamawiającemu wszelkie niezbędne dokumenty w celu umożliwienia mu korzystania z wdrożonego oprogramowania. Dokumenty jakie powinny zostać przekazane to:
    a. dostarczenie wszelkich niezbędnych materiałów uzupełniających do dokumentacji powykonawczej, które są konieczne do właściwej eksploatacji systemu.
    b. instrukcje użytkownika i administratora wdrożonego systemu informatycznego.

**Wymagania w zakresie uruchomienia, konfiguracji i utrzymaniu infrastruktury teleinformatycznej w modelu chmury obliczeniowej na potrzeby aplikacji Zamawiającego (Hosting).**

1. Wykonawca musi dostarczyć usługę uruchomienia, konfiguracji i utrzymania infrastruktury teleinformatycznej w modelu chmury obliczeniowej.
2. Wykonawca musi dostarczyć rozwiązanie w modelu usługowym na infrastrukturze teleinformatycznej Wykonawcy zlokalizowanej w ośrodku przetwarzania danych spełniającym wymogi określone w OPZ.
3. Wykonawca musi:
    a) skonfigurować i utrzymywać instancje serwerowe gotowe do instalacji aplikacji;
    b) zainstalować, utrzymywać i aktualizować na instancjach serwerowych systemy operacyjne (wraz z zapewnieniem niezbędnej ilości licencji);
    c) skonfigurować i utrzymywać połączenia sieciowe pomiędzy poszczególnymi instancjami serwerowymi;
    d) skonfigurować i udostępnić łącza do sieci Internet, zgodnie z określonymi w OPZ minimalnymi parametrami pozwalającymi w sposób niezakłócony realizować usługi ze wszystkich instancji serwerowych zlokalizowanych w środowisku teleinformatycznym dostarczonym przez Wykonawcę;
    e) skonfigurować i utrzymywać ochronę na styku z Internetem w warstwie sieciowej i aplikacyjnej;
    f) skonfigurować i utrzymywać niezależne łącze sieciowe do kluczowych elementów infrastrukturalnych Zamawiającego;
    g) skonfigurować i utrzymywać na każdej instancji serwerowej, na której będzie to wskazane, oprogramowanie antywirusowe, aktualizowane na bieżąco, zarządzane z jednej konsoli administracyjnej, zabezpieczającej przed wirusami, robakami, malwarem, ransomwarem, rootkitami i innymi zagrożeniami należącymi do kategorii zagrożeń wirusowych systemów informatycznych;
    h) zapewnić niezbędne licencje i oprogramowanie związane z realizacją zamówienia;

i) skonfigurować i udostępnić system zbierania i przechowania logów zdarzeń z urządzeń sieciowych w celu stałego monitorowania wydajności rozwiązania.

4. Zamawiający oczekuje udostępnienia w ramach środowiska chmurowego IaaS puli zasobów wirtualnych wraz z niezbędnym do prawidłowego działania oprogramowaniem systemowym i narzędziowym o parametrach nie gorszych niż określone poniżej i pozwalających wykreować dowolną ilość maszyn wirtualnych w ramach przydzielonej puli zasobów:

    a) architektura: x86-64 ;

    b) pamięć podstawowa: 16 GB ;

    c) procesory: 4 vCPU ;

    d) skalowalność: możliwość zwiększenia ilości pamięci operacyjnej i ilości procesorów o min. 50% ;

    e) interfejsy sieciowe: min. 2 x 10 Gbit/s ;

    f) moduł zarządzania środowiskiem wirtualnym: wymagany ;

    g) system operacyjny: Windows Standard 2019 z możliwością podniesienia do najnowszej wersji lub równoważny dla każe maszyny wirtualnej ;

    h) przestrzeń dyskowa 1 TB o wydajności nie mniejszej niż 200000 IOPS ;

    i) adres IP: 1 x IPv4 odseparowane sieci : 4 szt. ;

    j) łącze do sieci Internet: 200 Mbps łącze symetryczne bez limitów transferu wraz z ochroną przed atakami DDoS ;

    k) backup całego środowiska wykonywany raz na dobę.

5. **Wymagania dla ośrodka przetwarzania danych**

6. Wymagania dla ośrodka przetwarzania danych w ramach którego oferowana będzie usługa i Wykonawca będzie przetwarzał dokumenty Zamawiającego**.**

6.1Wymagania obligatoryjne - Ośrodek:

| OBIEKT I LOKALIZACJA | | |
|---|---|---|
| L.p. | Parametry lub kryterium | Wyeliminowanie zagrożenia |
| 1 | Centrum przetwarzania danych zlokalizowane na terenie UE lub Lichtensteinu , Islandii, Norwegii. Wszystkie dane Zamawiającego będą gromadzone i przetwarzane na | Przeciwdziałanie zagrożeniom związanym z przesyłaniem danych poza terytorium UE. Brak spełnienie wymagań RODO / GDPR. |

| | | |
|---|---|---|
| | terenie UE lub Lichtensteinu, Islandii, Norwegii. | |
| 2 | Ogrodzony teren centrum przetwarzania danych. | Brak podstawowej kontroli fizycznego dostępu do infrastruktury ośrodka. |
| 3 | Teren usytuowany poza strefami zalewowymi oraz strefami, na których może nastąpić podtopienie lub zalanie. | Zagrożenie nieprzerwanej pracy urządzeń serwerowych oraz innych urządzeń architektury ośrodka (elementy zasilania, agregaty) w wyniku działań działania sił natury. |
| 4 | Teren powinien być położony co najmniej 5 metrów powyżej poziomu wody stuletniej. | Zagrożenie długotrwałego zalania ośrodka. Wysoka intensywność oddziaływania sytuacji krytycznych. |
| 5 | Minimum 1 km od składowisk lub fabryk produkujących materiały toksyczne, radioaktywne, wybuchowe, żrące, również od stacji paliw lub składowisk paliw płynnych oraz baz wojskowych. | Zagrożenie powstania sytuacji zagrażających zdrowiu lub życiu osób fizycznie obsługujących urządzenia, długotrwałego skażenia terenu lub długotrwałych działań służb zapobiegających zdarzeniom krytycznym (np. odcięcie terenu przez straż pożarną, wojsko). |
| 6 | Minimum 1 km od miejsc narażonych na wandalizm lub zamieszki (stadiony i obiekty sportowe, centra handlowe, miejsca organizacji imprez masowych na minimum 10 tys. osób). | Zagrożenie długotrwałego zablokowania dróg dojazdowych do ośrodka, ryzyko niekontrolowanego zachowania tłumów, ryzyko zamieszek, zniszczeń. |
| 7 | Brak ciągów wodnych, kanalizacyjnych lub innych z substancjami płynnymi, położonych nad pomieszczeniami z serwerami. | Zagrożenie, przecieków, zalania urządzeń lub nagłych zmian warunków środowiskowych pracy urządzeń (wzrost wilgotności). |
| 8 | Minimum 15 m oddalenia urządzeń komputerowych udostępnionych Zamawiającemu od źródeł pól zakłócających (transformatory SN i WN). | Zagrożenie uszkodzenia urządzeń i danych w wyniku niekorzystnego oddziaływania pół zakłócających pracę urządzeń elektrycznych i magnetycznych. |

| | | |
|---|---|---|
| 9 | Wysokość technologiczna wewnątrz pomieszczenia serwerowni z serwerami: min 3,5 m - wysokość mierzona od podłogi technicznej do sufitu. | Zagrożenie zachowania odpowiedniej cyrkulacji powietrza, zachowania stref gorącej i zimnej, zmian parametrów środowiskowych. |
| 10 | Wysokość technologiczna podłogi technicznej w pomieszczeniu serwerowni min 1,0 m. | Zagrożenie dla zachowania cyrkulacji powietrza w wyniku zablokowania przez instalacje podpodłogowe, brak miejsca dla instalacji podpodłogowych. |
| 11 | Odseparowane pomieszczenie na przechowywanie nośników magnetycznych wyposażone w sejf. Sejf powinien posiadać atesty odporności ogniowej S120DIS zgodnie z EN 1047-1 oraz I klasę odporności włamaniowej zgodnie z EN 1143-1. | Przeciwdziałanie zagrożeniu fizycznego uszkodzenia, zniszczenia lub utraty nośników magnetycznych. |
| 12 | Spełnienie wymagania obowiązujących przepisów oraz europejskich i polskich norm w zakresie :budownictwa, energetyki oraz instalacji elektrycznych, BHP, ochrony przeciwpożarowej. | Przeciwdziałanie zagrożeniom budowlanym, pożarowym lub zagrożeniu życia i zdrowia ludzi w wyniku niezastosowania przepisów BHP, stosowania odrębnych od powszechnie stosowanych oznaczeń, błędów instalacji energetycznej. |
| WĘZŁY TELEKOMUNIKACYJNE | | |
| 1 | Podłączenie w pełni niezależnymi drogami światłowodowymi do co najmniej dwóch różnych operatorów telekomunikacyjnych o zasięgu krajowym. | Zagrożenie awarii lub innej przyczyny zaprzestania świadczenia usług transmisji danych przez operatora. |
| 2 | Dojścia połączeń do ośrodka wykonane dwoma niezależnymi trasami kablowymi. | Zagrożenie utraty ciągłości komunikacji danych z ośrodkiem. |

| | | |
|---|---|---|
| 3 | Węzeł dostępowy do sieci Internet dopięty do minimum 2 różnych operatorów z zaimplementowanym protokołem BGP. | Zapewnienie niezawodności i jakości transmisji danych w ramach sieci Internet. Przeciwdziałanie zagrożeniu utraty komunikacji z siecią Internet. |
| 4 | Węzeł dostępowy do sieci Internet ze zdublowanymi urządzeniami o gwarancji dostępności rocznej usługi 99,95% | Zagrożenie utraty ciągłości komunikacji sprzętu z siecią Internet. |
| 5 | Węzeł telekomunikacyjny wyposażony w redundantny system firewall. | Zagrożenie utraty zabezpieczenia systemów informatycznych w wyniku uszkodzenia zapory ogniowej. |
| 6 | Węzeł telekomunikacyjny wyposażony w redundantny system detekcji i prewencji włamań z sieci. | Zagrożenie bezpieczeństwa danych w wyniku ataku informatycznego na systemy. |
| ZASILANIE | | |
| 1 | Dostępność roczna systemu zasilania 99,95% | Zagrożenie ciągłości pracy urządzeń i dostępności urządzeń. |
| 2 | Minimum dwie niezależne linie zasilania dostępne dla sprzętu IT. | Zagrożenie zachowania ciągłości zasilania w wyniku uszkodzenia linii zasilającej lub długotrwałego przywracania ciągłości zasilania. |
| 3 | System zasilania awaryjnego UPS osobno na każdą linię zasilającą . | Zagrożenie dla zachowania nieprzerwanego zasilania urządzeń lub skrócenia pracy urządzeń na zasilaniu awaryjnym poniżej czasu bezpiecznego. |
| 4 | Redundantny system agregatów prądotwórczych. | Zagrożenie braku zachowania zasilania. |
| 5 | System zasilaczy awaryjnych UPS winien podtrzymać zasilanie urządzeń komputerowych przeznaczonych dla Zamawiającego przez przynajmniej 15 minut od zaniku napięcia i nie krócej niż do czasu uruchomienia się | Zagrożenie ciągłości pracy urządzeń w wyniku niedostosowania czasu pracy na zasilaniu awaryjnym do czasu reakcji na awarię zasilania i uruchomienia agregatów. Zagrożenie dla utraty lub uszkodzenia danych w wyniku niedostosowania czasu pracy urządzeń do czasu bezpiecznego zamknięcia wykonywanych na urządzeniach procesów. |

| | | |
|---|---|---|
| | agregatu i jego synchronizacji z siecią energetyczną. | |
| 6 | Agregat prądotwórczy ma posiadać zapas paliwa pozwalający na autonomiczną pracę bez konieczności uzupełniania zbiorników przez co najmniej 8 godzin. Agregat musi umożliwiać uzupełnienie paliwa w trakcie jego pracy. | Zagrożenie powstania przerw w zasilaniu wynikających z zatrzymania pracy agregatów. |
| BEZPIECZEŃSTWO | | |
| 1 | Wyposażenie w system telewizji przemysłowej CCTV, okres archiwizacji min. 21 dni, system kontroli dostępu (SKD). | Zagrożenie braku kontroli i monitorowania fizycznego dostępu do urządzeń. Zagrożenie braku materiałów dowodowych w przypadku naruszenia fizycznego bezpieczeństwa urządzeń. |
| 2 | Wyposażenie w system sygnalizacji włamania i napadu, System wykrywania wody i zalania. | Zagrożenie braku kontroli i reakcji na naruszenie bezpieczeństwa fizycznego lub zalanie obiektu. |
| 3 | Ochrona przez zewnętrzną licencjonowaną firmę. | Element zabezpieczenia bezpieczeństwa fizycznego ośrodka i zmniejszenia czasu interwencji wyspecjalizowanych służb w sytuacji kryzysowej. |
| 4 | System CCTV zapewnia ciągły 365/7/24 dozór obszarów i rejestrację zdarzeń z zachowaniem następujących parametrów funkcjonalnych: monitorowane wszystkie wejścia do obiektu – kamery wewnętrzne, monitorowane wszystkie pomieszczenia technologiczne. | Element zapewnienia wczesnego wykrywania i ostrzegania przed zagrożeniem naruszenia bezpieczeństwa fizycznego obiektu oraz zabezpieczenia materiału dowodowego na wypadek zaistnienia naruszenia, w tym identyfikacji osób. |
| 5 | System SKD dzieli centrum przetwarzania danych wraz z terenem przynależnym na minimum IV strefy dostępu z zastrzeżeniem, że teren | Przeciwdziałanie zagrożeniu nieuprawnionego dostępu do urządzeń lub w pobliże urządzeń. Element wymuszający weryfikację kontroli poziomów uprawnień osób poruszających się po ośrodku. |

| | | |
|---|---|---|
| | bezpośrednio przyległy do obiektu stanowi strefę I. | |
| 7 | Dostęp do strefy I (teren obiektu) uwarunkowany identyfikacją na podstawie dokumentu tożsamości (dla osób) lub rozpoznaniem numeru rejestracyjnego (dla samochodów). | Przeciwdziałanie zagrożeniu nieuprawnionego dostępu do urządzeń lub w pobliże urządzeń. |
| 8 | Dostęp do strefy II (część biurowa obiektu) uwarunkowany identyfikacją na podstawie dokumentu tożsamości ze zdjęciem. | Przeciwdziałanie zagrożeniu nieuprawnionego dostępu do urządzeń lub w pobliże urządzeń. |
| 9 | Dostęp do strefy III (strefa technologiczna) możliwy wyłącznie przy użyciu unikalnej i osobistej karty identyfikacyjnej współpracującej z SKD. | Przeciwdziałanie zagrożeniu nieuprawnionego dostępu do urządzeń lub w pobliże urządzeń. |
| 10 | Dostęp do strefy IV (pomieszczenia ze sprzętem komputerowym Zamawiającego) możliwy wyłącznie przy użyciu łącznie 2 elementów identyfikacji SKD - osobistej karty identyfikacyjnej i hasła (kodu) lub elementu biometrycznego. | Przeciwdziałanie zagrożeniu nieuprawnionego dostępu do urządzeń lub w pobliże urządzeń. |
| 11 | System gaszenia powinien być bezpieczny dla ludzi i sprzętu komputerowego. | Zagrożenie powstania uszczerbku na zdrowiu lub życiu osób w wyniku funkcjonowania systemu gaszenia. |
| 12 | Ściany, stropy części technologicznej o odporności ogniowej minimum 60 minut. Wszystkie drzwi prowadzące do pomieszczeń | Zapewnienie oporności ogniowej do czasu reakcji służb ratowniczych w celu ograniczenia skutków wystąpienia pożaru. Przeciwdziałanie zagrożenia rozprzestrzeniania się pożaru. |

| | | |
|---|---|---|
| | technologicznych o odporności ogniowej 60 minutowej. | |
| MONITOROWANIE | | |
| | System przyjmowania zgłoszeń dotyczących awarii działający w trybie 365/24/7. | Eliminacja zagrożenia braku działań reakcji na zdarzenia krytyczne przypadające poza godzinami pracy biurowej. |
| | Stałe i całodobowe (24/7/365) monitorowanie poprawności pracy infrastruktury ośrodka i urządzeń komputerowych udostępnianej Zamawiającemu. Pomiary mają dotyczyć minimum: wykresy przebiegów temperatury, wykres przebiegu wilgotności. | Zagrożenie braku kontroli parametrów pracy ośrodka oraz długich reakcji niekorzystne zmiany warunków pracy urządzeń. |

7. Wymagania obligatoryjne. Bezpieczeństwo sprzętu informatycznego:

| | Zakres |
|---|---|
| 1 | Izolacja sprzętu krytycznego |
| 2 | Ochrona przed uszkodzeniem |
| 3 | Rejestr wejść i wyjść do obszaru, w którym umieszczony jest sprzęt przeznaczony do obsługi Zamawiającego |
| 4 | Ochrona przed dostępem dla osób nieupoważnionych |

8. Wymagania obligatoryjne. Naprawa i konserwacja sprzętu:

| | Zakres |
|---|---|
| 1 | Ośrodek musi posiadać i stosować procedury kontroli, przeglądu, konserwacji i naprawy sprzętu. |
| 2 | Obsługa i naprawy muszą być dokonywane przez personel posiadający kwalifikacje zgodnie z zaleceniami producenta sprzętu i wewnętrznymi procedurami Ośrodka. |
| 3 | Należy usuwać nośniki danych przed przekazaniem sprzętu do naprawy. |

| | |
|---|---|
| 4 | Ochrona przed dostępem dla osób nieupoważnionych. |
| 5 | Należy stosować bezpieczne zbywanie lub przekazywanie sprzętu do ponownego użycia, w tym skuteczne usuwanie danych z nośników (wraz z systemami operacyjnymi i danymi licencyjnymi). |
| 6 | Należy chronić Zamawiającego przed instalacją złośliwego oprogramowania. |
| 7 | Należy prowadzić rejestr incydentów, awarii i usterek. |
| 8 | Ośrodek musi posiadać i stosować procedury kontroli, przeglądu, konserwacji i naprawy sprzętu. |

9. **Dostępność usług – wymagania SLA i czas reakcji**

10. Wszystkie usługi dostarczane przez usługodawcę będą utrzymywane i dostępne w trybie 24/7/365.

11. SLA dla świadczonej usługi musi wynosić minimum 99% w skali roku. Zapewnienie dostępności usług obejmuje:

    a) Warunki środowiskowe zapewniające prawidłowe funkcjonowanie urządzeń teleinformatycznych, w tym chłodzenie i wilgotność komory serwerowej

    b) Łącze energetyczne dostępne na jednym z dwóch torów zasilania

    c) Łącze internetowe

    d) Połączenie sieci LAN w ramach infrastruktury w celu umożliwienia pracy urządzeń

    e) Zasobów serwerowych określonych w pkt. 12.4

    f) Serwisów Java oraz Lamp

    a. Usługodawca zapewnia monitoring pasywny przechowywanych danych oraz Infrastruktury.

    b. Wykonawca zobowiązuje się informować Klienta z 7 dniowym wyprzedzeniem o potrzebie dokonania serwisu infrastruktury, na której przechowywane są dane, lub całości Infrastruktury. Informacja zostanie wysłana na piśmie z żądaniem zwrotnego potwierdzenia.

    c. Okno serwisowe będzie domyślnie realizowane w każdy pierwszy weekend miesiąca (z piątku na sobotę) w godzinach 0:00 do 6.00.

    d. W przypadku awarii Infrastruktury powodującej brak możliwości lub utrudnienia realizacji Usług lub Przechowywania, Wykonawca przystąpi do usuwania awarii w terminie 8 godzin od zgłoszenia i usunie awarię w terminie

nie dłuższym niż dalsze 24 godziny lub następnego dnia roboczego, gdy termin końcowy usunięcia awarii wypadnie w dzień wolny od pracy.

e. Przyjmowanie zgłoszeń serwisowych musi być realizowane w trybie 24/7/365
w systemie online Wykonawcy, który umożliwia podgląd wszystkich zgłoszeń, czas ich realizacji oraz bieżący status. Dostęp do systemu odbywa się za pomocą indywidualnego konta użytkownika utworzonego dla Zamawiającego.

f. Czas reakcji na zgłoszenie musi wynosić do 1h od przyjęcia zgłoszenia.

g. Czas realizacji zgłoszenia musi wynosić do 4 h od przyjęcia zgłoszenia realizowane w dzień roboczy - dzień, który nie jest dniem ustawowo wolnym od pracy (od poniedziałku do piątku z wyłączeniem sobót, niedziel i określonych ustawą świąt) w godzinach od 7.00 do 17.00.

**Wymagania techniczne Blockchain**

1. Maszyna wirtualna

Ilość: 1

Minimalne wymagania: RAM 16GB, HDD – minimum 100 GB, Procesor – 4 rdzenie

2. System operacyjny 64 bity

Ubuntu 12.04 lub nowszy LTS, Debian 7 lub nowszy LTS

3. Uprawnienia

Dostęp po SSH, Prawa root'a. Otwarte porty http/https (80,443), SSH (22 domyślny), 8570, 8571, 8333