Załącznik Nr 6-4 do SWZ

Szczegółowy opis przedmiotu zamówienia

Zadanie nr 4 - Usługi informatyczne w zakresie wdrożenia, konserwacji, serwisu sprzętu informatycznego i oprogramowania oraz szkolenia

Przedmiot zamówienia obejmuje dostawę, instalację, konfigurację i uruchomienie usług Publicznych e-Podatki/e-Odpady i integrację posiadanych systemów dziedzinowych z posiadanym oprogramowaniem elektronicznego Zarządzania Dokumentami i systemem BIP.

Przedmiot zamówienia obejmuje dostarczenie i uruchomienie:

1. Platformy Usług Publicznych e-Podatki/e-Odpady zintegrowanej z Systemem Płatności Elektronicznych,
2. przynajmniej dwóch e-usług wraz z formularzami elektronicznymi,
3. szyny usług integrującej usługi ePUAP, EZD i systemy dziedzinowe, pozwalającą na automatyzację przepływu deklaracji podatkowych z platformy ePUAP do EZD i systemów podatkowych,
4. integracji systemów dziedzinowych umożliwiających obsługę systemów e-usług (podatki, odpady, opłaty lokalne),
5. brokera integracyjnego umożliwiającego używanie profilu zaufanego ePUAP do logowania w module obsługi interesanta,
6. systemu Autoryzacji i Rozliczeń,
7. brokera integracyjnego umożliwiający publikację w Biuletynie Informacji Publicznej rejestrów publicznych z poziomu systemu EZD,
8. Systemu Płatności Elektronicznych. System musi umożliwiać dokonywanie płatności przez Internet w ramach świadczonych e-usług o wysokim poziomie dojrzałości umożliwiających dokonanie opłaty np. za podatki lokalne, wydanie decyzji. W ramach sytemu uruchomiony będzie moduł płatności spełniający wymagania obsługiwanych usług,
9. modernizacji EZD oraz systemu do obsługi strony podmiotowej BIP, oraz ich integracja,
10. Przeprowadzenie szkolenia z obsługi wdrożonych rozwiązań i oprogramowania dziedzinowego.

Ogólne wymagania

1. Łatwość pracy z systemem:

System musi cechować się przyjaznym interfejsem użytkownika wykorzystującym: menu, moduły, listy, formularze, przyciski, referencje (linki), itp.

System musi posiadać interfejs użytkownika w języku polskim. W języku polskim muszą być również wyświetlane wszystkie komunikaty, włącznie z komunikatami o błędach.

Komponenty Systemu użytkowane wewnątrz Jednostki powinny posiadać wbudowany mechanizm zdalnej asysty technicznej pozwalającej na wsparcie użytkowników systemu przez uprawnionych do tego administratorów.

2. **Bezpieczeństwo:**

Wdrożone rozwiązanie powinno docelowo zapewniać możliwość tworzenia kopii zapasowych danych.

Poszczególne komponenty Systemu umieszczone w różnych lokalizacjach powinny komunikować się ze sobą oraz z systemami zewnętrznymi w sposób zapewniający poufność danych. Dopuszcza się jako rozwiązanie wykorzystanie protokołu SSL lub połączenia VPN.

Uwierzytelnianie użytkowników powinno odbywać się za pomocą loginu i hasła (powinna być możliwość ustawiania siły hasła jak i możliwość wymuszania zmiany hasła). Dodatkowo w ramach tych komponentów powinna istnieć możliwość wyświetlenia zdarzeń wykonywanych przez danego użytkownika – rozliczalność i niezaprzeczalność wykonywanych czynności przez danego użytkownika.

System musi posiadać mechanizmy zapewniające autentyczność i integralność danych wewnątrz dostarczonego Systemu oraz ograniczenie dostępu do danych i funkcji Systemu przez nieuprawnionych użytkowników. Modułowość systemu.

3. **Integracja:**

- EZD <-> System Podatków i Opłat Lokalnych – zautomatyzowany proces przekazywania decyzji podatkowych, tytułów wykonawczych, upomnień i inicjowania na ich podstawie spraw zgodnych z JRWA,
- EZD <-> System Podatków i Opłat Lokalnych – obsługa korespondencji seryjnej (masowa obsługa decyzji podatkowych, tytułów wykonawczych, upomnień z poziomu kancelarii EZD),
- EZD <-> System Finansowo – Budżetowy – zautomatyzowany proces księgowania na podstawie informacji o doręczeniu decyzji podatkowych generowanych z poziomu kancelarii EZD Urzędu.
- EZD<-> wymiana danych do i z ePUAP.
- EZD<-> Biuletyn Informacji Publicznej (publikacja rejestrów).
- EPUAP - systemy dziedzinowe - możliwość pobierania danych z formularzy elektronicznych poprzez system EZD
- Wdrożone rozwiązanie powinno zostać zintegrowane z platformą ePUAP w tym również w zakresie wykorzystania konta ePUAP do logowania mieszkańców.
- System e-płatności powinien zostać zintegrowany z dostawcą świadczącym usługi płatności elektronicznych.
- System e-płatności w systemie dziennym powinien przekazywać dokładne informacje o osobie dokonującej płatności (imię nazwisko, tytuł płatności).
- System e-płatności powinien mieć możliwość synchronizacji danych z EZD lub systemem dziedzinowym.

4. **Licencjonowanie:**

- Licencje powinny zostać udzielone na czas nieograniczony.
- Licencje powinny zostać udzielone na nieograniczoną liczbę użytkowników.
- Licencje nie powinny wprowadzać ograniczeń, co do ilości wprowadzanych rekordów.
- Licencje na ewentualne systemy operacyjne bądź systemy bazodanowe powinny zostać dostarczone w ilości umożliwiającej prawidłowe działanie Systemu.
- Mając na uwadze nadrzędność celu, jakim jest uruchomienie Platformy Informatycznej Wykonawca zobowiązany jest dostarczyć wszelkie niezbędne oprogramowanie, które będzie konieczne do osiągnięcia zakładanego celu.

5. **Przepisy prawa i Normy:**

- USTAWA z dnia 6 września 2001 r. o dostępie do informacji publicznej (tj. Dz.U.2016.1764)
- ROZPORZĄDZENIE MINISTRA SPRAW WEWNĘTRZNYCH I ADMINISTRACJI z dnia 18 stycznia 2007 r. w sprawie Biuletynu Informacji Publicznej (tj. Dz.U.2007.10.68)
- USTAWA z dnia 29 sierpnia 1997 r. o ochronie danych osobowych Dz.U.2016.922 z póź zm.
- ROZPORZĄDZENIE MINISTRA ADMINISTRACJI I CYFRYZACJI z dnia 11 maja 2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewniania przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji Dz.U.2015.745
- ROZPORZĄDZENIE MINISTRA ADMINISTRACJI I CYFRYZACJI z dnia 11 maja 2015 r. w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbiorów danych Dz.U.2015.719
- ROZPORZĄDZENIE MINISTRA ADMINISTRACJI I CYFRYZACJI z dnia 10 grudnia 2014 r. w sprawie wzorów zgłoszeń powołania i odwołania administratora bezpieczeństwa informacji Dz.U.2014.1934
- ROZPORZĄDZENIE MINISTRA SPRAW WEWNĘTRZNYCH I ADMINISTRACJI z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych Dz.U.2004.100.1024
- ROZPORZĄDZENIE RADY MINISTRÓW z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych Dz.U.2016.1744
- Dobre praktyki dla administracji publicznej zakresie ochrony danych osobowych jak i informatyzacji Oraz wytyczne grupy 29
- Normy: ISO/ICE 27000; ISO/ICE 27001; ISO/ICE 27002; ISO/ICE 27005; ISO/IEC 20000 — zarządzanie usługami IT; ISO/IEC 27017 Kodeks najlepszych praktyk w zakresie zabezpieczeń dla usług w chmurze obliczeniowej; ISO/IEC 27018 Ochrona Danych Osobowych w Chmurze Dbaj o bezpieczeństwo informacji w cyberprzestrzeni; ISO 22301 Zarządzanie Ciągłością Działania; Zarządzanie Ryzykiem ISO 31000; ISO/IEC 19770, Norma PN-ISO/IEC 17799

- Inne niezbędne przepisy mające wpływ na ochronę informacji i informatyzację administracji publicznej, inwentaryzację sprzętu oprogramowania, ochrona praw autorskich itp.
- Przedmiot zamówienia musi być zgodny z obowiązującymi przepisami prawa w zakresie Portalów informatycznych wykorzystywanych przez jednostki publiczne, w tym między innymi spełniać wymagania następujących aktów prawnych: Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 roku (Dz. U. 1997, Nr 78 poz. 483 z późn. zm.);
- Ustawa z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (Dz. U. 2014, poz. 1182 z późn. zm.);
- ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) Dz.U. L 119 z 4.5.2016
- Przyszłościowo wydane akty wykonawcze wydane do RODO – nowa ustawa o ochronie danych, rozporządzenia itp.
- Ustawa z dnia 4 lutego 1994 roku o prawie autorskim i prawach pokrewnych (Dz. U. 2006, Nr 90, poz. 631 z późn. zm.);
- Ustawa z dnia 14 lipca 1983 roku o narodowym zasobie archiwalnym i archiwach (Dz. U. 2011, Nr 123, poz. 698);
- Ustawa z dnia 17 lutego 2005 roku o informatyzacji działalności podmiotów realizujących działania publiczne (Dz. U. z 2014 r. poz. 1114);
- Rozporządzenie Ministra Nauki i Informatyzacji z dnia 19 października 2005 roku w sprawie testów akceptacyjnych oraz badania oprogramowania interfejsowego i weryfikacji tego badania (Dz. U. 2005, Nr 217, poz. 1836);
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 30 października 2006 roku w sprawie niezbędnych elementów struktury dokumentów elektronicznych (Dz. U. 2006, Nr 206, poz. 1517);
- Rozporządzenie Prezesa Rady Ministrów z dnia 14 września 2011 r. w sprawie sporządzania i doręczania dokumentów elektronicznych oraz udostępniania formularzy, wzorów i kopii dokumentów elektronicznych (Dz. U. z 2015 r. poz. 971).
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i Portale informatyczne służące do przetwarzania danych osobowych (dz. u. z 2004 r. nr 100, poz. 1024)
- Ustawa o ochronie baz danych z 27 lipca 2001 roku (Dz. U. z 2001 roku, Nr 128, poz.1402, z 2004 r. Nr 96, poz. 959, z 2007 r. Nr 99, poz. 662, Nr 176, poz. 1238.);
- Ustawa z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (Dz. U. z 2017 r. poz. 1579 z późn. zm.)
- Inne niezbędne przepisy mające wpływ na ochronę informacji i informatyzację administracji publicznej, inwentaryzację sprzętu oprogramowania, ochrona praw autorskich oraz wszelkie zmiany obecnych przepisów, akty zastępujące itp.

6. **Wymaganie funkcjonalne:**

Modernizacja systemów dziedzinowych:

- Formularze po przesłaniu do EZD powinny w łatwy sposób mieć możliwość ich wydrukowania w czytelnej formie.
- Z systemu e-płatności powinny przychodzić powiadomienia do EZD lub systemu dziedzinowego odnośnie informacji o płatnościach (Imię nazwisko, za co zostało zapłacone, kwota) jeśli płatność będzie dokonywana z systemu e-odpady, e-podatki, powinna być zawarta dodatkowo informacja o koncie i rodzaju podatku, opłaty
- System EZD powinien zostać tak przekonfigurowany, aby ograniczyć odgraniczyć użytkownikom dostęp do dokumentów innych osób lub działów zgodnie ze strukturą. Aby osoby nieuprawnione nie miały wglądu w dokumenty lub sekretarka przy wysyłce dokumentu nie mogła do otwierać i czytać. A także ustawić uprawnienia poszczególnym osobom zgodnie z kompetencjami do poszczególnych działów systemu.
- Aktualizacja Elektronicznego Archiwum i jego konfiguracja z EZD wraz ze szkoleniem dla Archiwistów.
- Integracja systemu EZD z systemem poczty envelo Poczty Polskiej w celu umożliwienia korzystania z opcji e-doręczeń.

7. **Wymagania wdrożeniowe**

Prace wdrożeniowe

Wykonawca w ramach zamówienia wykona prace niezbędne do poprawnego uruchomienia rozwiązania. Prace wdrożeniowe obejmują pełen zakres prac integracyjnych dla poniższych obszarów z poniżej opisanymi systemami dziedzinowymi:

Obszar integracji (systemy dziedzinowe)

Producent obecnego rozwiązania:

System Finansowo – Budżetowy

Nefeni sp. z o.o.

System Podatków i Opłat Lokalnych

Nefeni sp. z o.o.

System EZD

Nefeni sp. z o.o.

Biuletyn Informacji Publicznej

Nefeni sp. z o.o.

W celu zapewnienia możliwości przeprowadzenia oraz integracji Zamawiający zapewni dostęp do baz danych rozwiązań obecnie wykorzystywanych (dla wymienionych obszarów podlegających i integracji). Zamawiający nie dopuszcza wymiany obecnie wykorzystywanych systemów.

8. Szkolenie i wdrożenie

Wykonawca w ramach zamówienia przeprowadzi prace wdrożeniowe wraz ze szkoleniami użytkowników zgodnie z poniższym podziałem:

- **Modernizacja EZD i integracja z e-usługami**

Wdrożenie modułu archiwum EZD, modernizacja oprogramowania EZD dostosowująca do archiwizacji dokumentów i obsługi integracji z oprogramowaniem dziedzinowym oraz e-usługami.

- **Modernizacja i integracja posiadanych systemów dziedzinowych w ramach platformy e-usług**

Wdrożenie zintegrowanego systemu płatności elektronicznych (e-płatności) model integracyjny umożliwiający używanie profilu zaufanego ePUAP do podpisywania wniosków/formularzy w module obsługi interesanta.

Wdrożenie szyny usług integrującej usługi ePUAP, EZD i systemów dziedzinowych. Wdrożenie platformy e-usług publicznych udostępniającą dane z systemów dziedzinowych.

- **Szkolenie z platformy e-usług publicznych udostępniającą dane z systemów dziedzinowych**

Szkolenia zaawansowane z posiadanych systemów dziedzinowych i EZD.

- **Szkolenia dla urzędników w zakresie cyberbezpieczeństwa – 2 szt.**

W ramach zadania wykonawca przeprowadzi szkolenia w zakresie cyberbezpieczeństwa dla pracowników Urzędu Miasta i Gminy w Kłodawie.

Szkolenia będą zrealizowane jako szkolenia zamknięte, przeprowadzone w języku polskim, realizowane stacjonarnie w miejscu wyznaczony przez zamawiającego na terenie miejscowości Kłodawa; tym samym zamawiający zapewni salę wyposażoną w sprzęt nagłaśniający, projektor oraz laptop w której przeprowadzone zostaną szkolenia.

Szkolenia powinny odbywać się w 2 grupach nie większych niż 20 osób i trwać nie dłużej niż 7 godzin lekcyjnych (45 minut). Liczba osób do przeszkolenia 40.

Przykładowy zakres merytoryczny szkolenia.

- Wprowadzenie do ustawy o krajowym systemie cyberbezpieczeństwa,
- Cyberzagrożenia i cyberprzestępczość,
- Krajowy System Cyberbezpieczeństwa.
- Obowiązki operatorów usług kluczowych,
- Obowiązki dostawców usług cyfrowych,
- Obowiązki podmiotów publicznych,
- Organy właściwe do spraw cyberbezpieczeństwa.
- Najnowsze zagrożenia w sieci i zagrożenie informacji - ile nas to może kosztować?
- Odpowiedzialność za naruszenie zasad bezpieczeństwa informacji.
- Podejrzane urządzenia elektroniczne
- Przykłady zagrożeń laptopy, pendrive, smartfony
- Jak się przed tym chronić?
- Phishing i ransomware co to jest? Jak rozpoznawać zagrożenia.

- Case study ofiar cyberprzestępców - przykłady organizacji, które zostały zaatakowane w sieci w tym również w naszym rejonie.
- Najczęściej wykrywane podatności zagrożeniem dla ochrony informacji.
- Socjotechnika a Bezpieczeństwo.
- Bezpieczna praca z informacją papierową i elektroniczną.
- Zasady korzystania z poczty e-mail oraz zagrożenia z tego płynące.
- Bezpieczeństwo w Internecie, strony www, przeglądarki.
- Bezpieczeństwo urządzeń mobilnych.
- Praca zdalna. Czym jest vpn? Jak bezpiecznie pracować zdalnie na sprzęcie własnym lub służbowym.
- Podsumowanie najważniejszych zasad Cyberbezpieczeństwa.

- Wykonawca gwarantuje, że osoba prowadząca szkolenia posiada odpowiednie predyspozycje do prowadzenia szkoleń oraz wyczerpującą wiedzę, co najmniej na poziomie wymaganym do realizacji szkoleń;

- Wykonawca jest zobowiązany przeprowadzić szkolenie w oparciu o zaakceptowane przez Zamawiającego materiały dydaktyczne.

- Wykonawca prześle do akceptacji zamawiającemu materiały dydaktyczne najpóźniej na 7 dni przed szkoleniem.

- Wykonawca zobowiązany jest w porozumieniu z Zamawiającym ustalić dokładną datę przeprowadzenia szkoleń, zgodnie z opublikowanym harmonogramem jako załącznik do ogłoszenia o zamówieniu.

- Wykonawca zapewni materiały dydaktyczne dla każdego uczestnika szkolenia, oraz poświadczy uczestnictwo w szkoleniu certyfikatem lub innym dokumentem świadczącym o odbyciu szkolenia.

◦ **Przeprowadzenie wewnętrznego audytu z zakresu dostosowania do wymagań ustawy o krajowym systemie cyberbezpieczeństwa.**

Podstawą do przeprowadzenia wewnętrznego audytu są wyniki diagnozy, „Złącznik nr 8 - Formularz informacji związanych z przeprowadzeniem diagnozy cyberbezpieczeństwa” w projekcie Cyfrowa Gmina.

- Zakres zdania:

- Przegląd dokumentacji (zarządzeń, dokumentów wewnętrznych, procedur) związanych z przetwarzaniem danych osobowych w systemach informatycznych urzędu.
- Przegląd i aktualizacja dokumentacji SZBI.
- Opracowanie strategii i polityki ciągłości działania.
- Opracowanie dokumentacji procesu zarządzania podatnościami i zagrożeniami.
- Stworzenie procedur zarządzania incydentami zgodnie z Art. 22 UoKSC
- Rekomendacje i zalecenia dotyczące innych wykrytych nieprawidłowości.
- Raport pokontrolny.

- Wykonawca gwarantuje, że osoby skierowane do przeprowadzenia zadania posiadają odpowiednie predyspozycje oraz wyczerpującą wiedzę.

- Zamawiający wymaga aby osoba przeprowadzająca audyt posiadała uprawnienia wykazane w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu

w rozumieniu art. 15 ustawy z dnia 5 lipca 2018 r. o Krajowym systemie cyberbezpieczeństwa.

9. Wymagana dokumentacja

Wykonawca zobowiązany jest do dostarczania Dokumentacji i ich aktualizacji w trakcie trwania Umowy.

Wymagania ogólne

Dokumentacja musi być sporządzona w języku polskim, chyba że dotyczy kodów źródłowych, fragmentów kodu SQL.

Dokumentacja musi być dostarczona w formie papierowej lub elektronicznej (.pdf, .doc) na nośniku elektronicznym, w postaci umożliwiającej uzyskanie jej wydruku przy pomocy powszechnie używanych narzędzi.

Dokumentacja musi gwarantować kompletność dokumentu rozumianą jako pełne, bez wyraźnych i ewidentnych braków, przedstawienie omawianego problemu obejmujące całość z danego rozpatrywanego zakresu zagadnienia.

Zawartość Dokumentacji musi być zgodna z wytworzonym Rozwiązaniem.

Dokumentacja użytkownika „Rozwiązania”

Wykonawca dostarczy Dokumentację użytkownika oraz opis Ścieżek Postępowania.

Dokumentacja użytkownika musi zawierać opis pełnej funkcjonalności Rozwiązania w sposób przejrzysty umożliwiający samodzielne użytkowanie Rozwiązania.

Wykonawca jest zobowiązany dostarczyć w ramach zamówienia Dokumentację powykonawczą Rozwiązania.

Dokumentacja powykonawcza musi być sporządzona w języku polskim, chyba że dotyczy oprogramowania narzędziowego obcego pochodzenia (Produktu), wykorzystywanego w Rozwiązaniu, dla którego nie ma dokumentacji w języku polskim, w takim przypadku Dokumentacja może zostać przekazana w języku angielskim.

10. Gwarancja

Wykonawca zobowiązuje się do dostarczania wolnych od wad kolejnych wersji Systemu.

Wykonawca zapewni wystarczającą ilość konsultantów do zapewnienia ciągłości usługi gwarancji.

Wykonawca udzieli Zamawiającemu gwarancji na przedmiot zamówienia zapewniając jednocześnie odpowiedni serwis.

W ramach gwarancji Wykonawca zobowiązany jest do nieodpłatnej:

- usuwania Usterki, Wady, Błędu lub Awarii z przyczyn zawinionych przez Wykonawcę będących konsekwencją wystąpienia: błędu w Systemie, błędu lub wady fizycznej pakietu aktualizacyjnego lub instalacyjnego, błędu w dokumentacji administratora lub w dokumentacji użytkownika, błędu w wykonaniu usług przez Wykonawcę;
- usuwania Błędu, Awarii, Wady związanych z realizacją usługi wdrożenia Systemu;
- usuwania Błędów lub Awarii spowodowanych aktualizacjami Systemu.

- Wykonawca musi informować Zamawiającego o dostępnych aktualizacjach i poprawkach Systemów
- Zgłaszający, w przypadku wystąpienia błędu, awarii, usterki przesyła do Wykonawcy przy pomocy środków komunikacji formularz zgłoszenia wystąpienia błędu/awarii.
- Wykonawca zapewnia dostosowanie do obowiązujących przepisów nie później niż w dniu ich wejścia w życie.

11. Asysta techniczna

Zamawiający wymaga, aby Wykonawca świadczył asystę techniczną.

Wykonawca zobowiązuję się do świadczenia konsultacji dla Administratorów w zakresie niezbędnych zmian w konfiguracji systemu.

Wykonawca zapewni usługę wsparcia użytkowników udostępniając:

Usługę typu helpdesk, udostępnioną pod adresem e-mail, numerem telefonu i numerem faksu,

portal typu helpdesk – dostępny on-line w trybie 356/7/24, gdzie będą publikowane statusy zgłoszeń,

Przez niniejszy portal będą mogły być dokonywane zgłoszenia Usterek/Awarii/Wad.

Wsparcie użytkowników obejmuje świadczenie usługi wsparcia technicznego, merytorycznego oraz konsultacji w celu utrzymania poprawnej pracy systemu zgodnego z wymaganiami zamówienia. W ramach usługi Wykonawca zobowiązany jest do udzielania odpowiedzi na pytania Użytkowników i Administratorów związane z bieżącą eksploatacją Systemu.