Numer sprawy: TT/3/2021

Załącznik 1 do Zapytania Ofertowego

OPIS PRZEDMIOTU ZAMÓWIENIA

w postępowaniu o udzielenie zamówienia

w trybie zapytania ofertowego, którego przedmiotem jest:

Wdrożenie aplikacji wspomagającej pracę Trade & Travel Company

realizowanego w ramach projektu pn.

„Dywersyfikacja i automatyzacja usług w Trade & Travel Company"

współfinansowanego w ramach Regionalnego Programu Operacyjnego Województwa Łódzkiego na lata 2014-2020

Łódź, 2 sierpnia 2021 roku

Spis treści

ROZDZIAŁ 1 - PODSTAWOWE INFORMACJE

1.1. PRZEDMIOT ZAMÓWIENIA

1. Przedmiotem zamówienia jest wdrożenie oprogramowania systemu przeznaczonego do wspomagania procesów wewnętrznych oraz usprawnienia obsługi klientów Zamawiającego
2. Zakres zamówienia:
   2.1. wykonanie oprogramowania,
   2.2. instalacja,
   2.3. konfiguracja,
   2.4. migracja danych z obecnie użytkowanego systemu,
   2.5. produkcyjne uruchomienie,
   2.6. asysta w okresie stabilizacji,
   2.7. szkolenia użytkowników,
   2.8. wykonanie i przekazanie dokumentacji powykonawczej,
   2.9. zapewnienie środowiska chmurowego dla działania oprogramowania stanowiącego przedmiot zamówienia

1.2. WYMAGANIA FORMALNE I ORGANIZACYJNE

1. Zamawiający wymaga wnikliwego zapoznania się z treścią OPZ.
2. OPZ stanowi podstawę opracowania oferty Wykonawcy, a po wyborze Wykonawcy, realizacji niniejszego zamówienia. Udzielanie wyjaśnień dotyczących zapisów zawartych w OPZ i ewentualne zmiany w ich treści są możliwe jedynie w toku postępowania ofertowego.
3. Wszelkie wątpliwości i zapytania ze strony Wykonawcy, powstałe w toku realizacji zadania, związane z zakresem, sposobem realizacji a także wystąpieniem sytuacji nieprzewidzianych w obowiązujących przepisach prawnych i w OPZ Wykonawca zobowiązany jest uzgadniać z Zamawiającym.
4. W związku z obowiązkami Zamawiającego związanymi z realizacją projektu współfinansowanego ze środków UE, dotyczącymi działań informacyjnych i promocyjnych, na dokumentach związanych z realizowanym zadaniem, należy umieszczać znaki i oznaczenia zgodne z Podręcznikiem wnioskodawcy i beneficjenta programów polityki spójności. Wzory znaków są dostępne na stronie http://www.rpo.lodzkie.pl.
5. Wykonawca zobowiązany jest do wyznaczenia Project Managera, który będzie upoważniony do kontaktów w sprawie realizacji zamówienia z Zamawiającym.
6. Wykonawca, na każdym etapie realizacji prac, zapewni stały dostęp do wszelkich materiałów i dokumentów, które powstają w trakcie realizacji zamówienia.
7. Wykonawca zobowiązuje się do stosowania zaleceń wydawanych przez Zamawiającego.

1.3. WYMAGANIA PRAWNE

1. Zamawiający wymaga, aby dla oprogramowania stanowiącego przedmiot niniejszego zamówienia, Wykonawca przekazał Zamawiającemu autorskie prawa majątkowe.
2. Wykonawca zapewnia i zobowiązuje się, że korzystanie przez Zamawiającego z dostarczonych produktów nie będzie stanowić naruszenia majątkowych praw autorskich osób trzecich.
3. Wykonawca jest odpowiedzialny za wszelkie wady fizyczne w wykonanych pracach.
4. Wykonawca jest odpowiedzialny za wszelkie wady prawne, w tym również za ewentualne roszczenia osób trzecich wynikające z naruszenia praw własności intelektualnej lub przemysłowej, w tym praw autorskich, patentów, praw ochronnych na znaki towarowe oraz praw z rejestracji na wzory użytkowe i przemysłowe, pozostające w związku z wprowadzeniem ich do obrotu na terytorium Rzeczypospolitej Polskiej.
5. Wykonawca odpowiada za wszelkie naruszenia praw osób trzecich, które mogą wystąpić w związku z wykonywaniem przedmiotu zamówienia.
6. Zamawiający wymaga, aby system informatyczny powstały w wyniku realizacji niniejszego zamówienia funkcjonował zgodnie z obowiązującymi przepisami prawa oraz standardami technicznymi.
7. Wykonawca odpowiada za wszelkie szkody związane z realizacją przedmiotu zamówienia wynikające z przyczyn leżących po stronie Wykonawcy lub podmiotów, którymi przy wykonywaniu zamówienia będzie się posługiwał.

1.4. NEUTRALNOŚĆ TECHNOLOGICZNA

1. W ramach zamówienia przyjmuje się założenie neutralności technologicznej – nie wskazuje się i nie faworyzuje żadnej konkretnej technologii i oprogramowania (za wyjątkiem obowiązujących norm europejskich i krajowych oraz powszechnie stosowanych technologii o charakterze standardów.
2. Zamawiający informuje, że jeżeli w Zapytaniu Ofertowym zostały wskazane typy i symbole produktów oraz nazwy ich producentów to mają one jedynie charakter przykładowy. Zostały określone jedynie w celu sprecyzowania parametrów i wymogów techniczno-użytkowych przedmiotu zamówienia.

1.5. SPOSÓB OBLICZENIA CENY OFERTY

W cenie oferty Wykonawca winien skalkulować wszelkie koszty jakie poniesie w związku z realizacją zamówienia, w tym w szczególności: czasu pracy, wykorzystanych materiałów i urządzeń, ubezpieczenia, dokonania odbiorów, gwarancji, kosztów zapewnienie środowiska chmurowego dla działania oprogramowania stanowiącego przedmiot zamówienia, kosztów przekazania autorskich praw majątkowych oraz koszty wymaganych prawem opłat i podatków, a także wszystkie inne dodatkowe koszty, które powstaną w trakcie realizacji zamówienia.

1.6. SPOSÓB WYKONANIA UMOWY

1. Wykonawca w ramach niniejszego zamówienia, dla oprogramowania stanowiącego przedmiot zamówienia, wykona minimum następujące prace:
   1.1. instalację oprogramowania na zaoferowanym środowisku chmurowym,
   1.2. konfigurację oprogramowania do działania w środowisku Zamawiającego,
   1.3. migrację danych z obecnie użytkowanego systemu,
   1.4. produkcyjne uruchomienie,
   1.5. zapewni minimum miesięczną asystę w okresie stabilizacji działania Oprogramowania przeszkoli maksymalnie 20 użytkowników Zamawiającego:
   1.6. dla oprogramowania stanowiącego przedmiot zamówienia, przez okres trwania gwarancji zadeklarowany w Formularzu Ofertowym, zapewni środowisko chmurowe dla działania oprogramowania;
2. Podczas prac Wykonawca musi zachować następującą kolejność prac:
   2.1. uzgodnić z Zamawiającym na minimum 2 dni przed rozpoczęciem planowanych prac wymagających uczestnictwa pracowników Zamawiającego lub prac powodujących przeszkody lub przerwy w normalnej działalności Zamawiającego;
   2.2. wykonać prace w sposób możliwie najmniej absorbujący pracowników Zamawiającego;
   2.3. wykonać prace w sposób możliwie niepowodujący przerw w normalnej działalności Zamawiającego.
   2.4. dokonać weryfikacji poprawności wykonanych prac,
   2.5. zgłosić Zamawiającemu zakończenie prac.
3. Wykonawca niezwłocznie poinformuje Zamawiającego o incydentach zagrażających bezpieczeństwu danych;
4. Wykonawca zobowiązany jest do przestrzegania obowiązujących przepisów i instrukcji obowiązujących u Zamawiającego.

1.7. ZASADY ODBIORU PRAC

1. Wykonawca zgłosi przedmiot zamówienia do kontroli Zamawiającego.
2. Oprogramowanie przed zgłoszeniem do odbioru musi zostać poddane przez Wykonawcę:
   1.1. Testom wewnętrznym funkcjonalności Oprogramowania
   1.2. testom bezpieczeństwa. Testy bezpieczeństwa muszą być wykonywane w oparciu o standard OWASP.
3. Zgłoszenie do odbioru Oprogramowania może nastąpić po przedstawieniu przez Wykonawcę Zamawiającemu:
   1.3. Raportu z testów wewnętrznych
   1.4. Raportu z testów bezpieczeństwa .
4. Zamawiający w terminie do 7 dni roboczych wykona kontrolą zgłoszonego przedmiotu zamówienia, w zakresie zgodności wykonania przedmiotu prac z OPZ;

5. Odbiór Przedmiotu Umowy zostanie dokonany poprzez przeprowadzenie Testów Akceptacyjnych (TA).
6. TA mają na celu zweryfikowanie w rzeczywistych warunkach pracy osiągnięcie wymaganej umową funkcjonalności.
7. Plan Testów Akceptacyjnych (PTA) przygotuje Wykonawca i przedstawi Zamawiający na minimum 10 dni przed planowaną datą przeprowadzenia TA
8. PTA musi zawierać:
   8.1. Scenariusze testowe dostarczone przez Wykonawcę oraz scenariusze własne Zamawiającego, umożliwiające potwierdzenie osiągnięcia kluczowych funkcjonalności Oprogramowania wynikające z wymogów funkcjonalnych określonych w Załączniku 2 oraz uwzględniać adekwatne wymogi technologiczne i bezpieczeństwa.
   8.2. Harmonogram testów
9. Procedura akceptacji PTA
   9.1. Zamawiający w terminie do 5 dni od dnia otrzymania PTA sprawdzi ich kompletność oraz poprawność merytoryczną, oceni dokument i dokona jego akceptacji lub odrzuci, przekazując jednocześnie Wykonawcy swoje zastrzeżenia,
   9.2. W przypadku, gdy Zamawiający odrzuci PTA, Wykonawca w terminie kolejnych 5 dni od przekazania zastrzeżeń do PTA, dokona zmian w PTA, zgodnie z uwagami Zamawiającego i przekaże kolejną wersję PTA do oceny Zamawiającego.
   9.3. Zamawiający po otrzymaniu kolejnej wersji PTA, w terminie kolejnych 5 dni dokona oceny przekazanej PTA i dokona jej odbioru lub odrzuci, przekazując swoje zastrzeżenia Wykonawcy.
   9.4. Procedura opisana w punktach 9.2 do 9.3 będzie powtarzana aż do przyjęcia PTA.
10. Warunkiem przystąpienia do TA jest zatwierdzony PTA.
11. Procedura TA
    11.1. Zamawiający w terminie do 3 dni od dnia akceptacji PTA wyznaczy termin TA.
    11.2. Zamawiający przy wsparciu Wykonawcy przeprowadzi TA według scenariuszy zawartych w PTA.
    11.3. W przypadku poprawności merytorycznej TA Zamawiający dokona odbioru Przedmiotu Umowy, pod warunkiem spełnienia okoliczności opisanych w punkcie 13;
    11.4. W przypadku, gdy TA nie zakończą się wynikiem pozytywnym, Zamawiający nie dokona odbioru i poinformuje Wykonawcę o swoich zastrzeżeniach w formie pisemnej zawierającej numer testu zakończonego niepowodzeniem, opis sytuacji oraz zrut ekranowy.
    11.5. Wykonawca dokona zmian w Oprogramowaniu i zgłosi Oprogramowanie do kolejnych TA.
    11.6. Zamawiający po otrzymaniu zgłoszenia o gotowości do przeprowadzenia po raz kolejny TA,, przeprowadzi TA i w przypadku pozytywnego wyniku TA, dokona odbioru Przedmiotu Umowy, pod warunkiem spełnienia okoliczności opisanych w punkcie 13
    11.7. W przypadku, gdy TA nie zakończą się wynikiem pozytywnym, Zamawiający nie dokona odbioru i poinformuje Wykonawcę o swoich zastrzeżeniach w formie pisemnej zawierającej numer testu zakończonego niepowodzeniem, opis sytuacji oraz zrzut ekranowy.
    11.8. Procedura opisana w punktach 11.4 do 11.7 będzie powtarzana, aż do zaakceptowania przez Zamawiającego wyników TA.
12. Pomyślne zakończenie TA jest warunkiem koniecznym do uznania umowy za zrealizowaną zgodnie z Umową.
13. Warunkiem koniecznym dla podpisania Protokołu Odbioru Końcowego jest zaakceptowanie przez Zamawiającego dostarczonej przez Wykonawcę Dokumentacji Powykonawczej przedmiotu zamówienia, której forma i zakres zostały szczegółowo opisane w rozdziale 1.8.
14. Potwierdzeniem wykonania Umowy będzie podpisany przez Zamawiającego Protokół Odbioru Końcowego Umowę będzie uważać się za wykonaną w terminie, pod warunkiem, podpisania przez Zamawiającego Protokół Odbioru Końcowego przed terminem określonym w rozdziale IV Zapytania Ofertowego.
15. Zamawiający może odmówić odbioru przedmiotu zamówienia w przypadku, gdy nie został on wykonany w sposób określony w OPZ, niezgodnie z zasadami sztuki i wiedzy zawodowej lub przepisami prawa.

1.8. DOKUMENTACJA POWYKONAWCZA

2. Dokumentacja Powykonawcza - stanowi zbiór dokumentów określających sposób wykonania przedmiotu zamówienia, prac wdrożeniowych oraz wskazujących sposób eksploatacji i utrzymania pracy Systemu, które muszą spełniać następujące warunki
   2.1. zostały napisane w języku polskim,
   2.2. przygotowane w formie elektronicznej w formacie plików MS Office zgodnie z zasadami profesjonalizmu,
   2.3. zawierać wskazanie wersji systemu, której dotyczą
   2.4. sporządzone w sposób umożliwiający ich sprawdzenie i weryfikację
   2.5. wszystkie rysunki i zrzuty ekranu muszą być wykonane przejrzyście z naniesionymi czytelnie opisami.
3. Dokumentacja Powykonawcza składa się z następujących elementów:
   3.1. Instrukcji obsługi dla użytkowników zawierającej:
      3.1.1. Opis wszystkich funkcji Systemu,
      3.1.2. Instrukcję obsługi Systemu, w tym
         3.1.2.1. Instrukcję wykonywania wszystkich czynności w Systemie
         3.1.2.2. Dostępne dla użytkownika opcje konfiguracyjne wraz z ich znaczeniem dla pracy użytkownika
         3.1.2.3. Opis zależności między poszczególnymi komponentami Systemu
         3.1.2.4. Listę najczęściej pojawiających się problemów wraz z sugerowanym postępowaniem
   3.2. Instrukcji obsługi dla administratora zawierającej:
      3.2.1. Opis zadań administratora
      3.2.2. Szczegółową listę czynności administratora
      3.2.3. Szczegółowe procedury administrowania Systemem, określające sposób wykonywania zadań, w tym konfigurowania pracy Systemu
      3.2.4. Opis architektury logicznej i technicznej Systemu
      3.2.5. Opis parametrów systemowych
   3.3. Instrukcji zarządzania Systemem służącej do przetwarzania danych osobowych, zgodnie z ustawą o ochronie danych osobowych zawierającej:
      3.3.1. Opis zastosowanych metod i środków uwierzytelniania,
      3.3.2. Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników Systemu.
      3.3.3. Sposób odnotowywania informacji o odbiorcach, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia,
   3.4. Dokumentacji technicznej, która powinna zawierać informacje w zakresie:
      3.4.1. Architektury i integracji:
         3.4.1.1. Schemat architektury technicznej (sprzęt), logicznej/integracyjnej systemu, schemat ruchu sieciowego z opisami i wskazanymi portami komunikacji,
         3.4.1.2. Zasady integracji Systemu z innymi systemami zewnętrznymi (interfejsy),
         3.4.1.3. Specyfikacje interfejsów wymiany danych z systemami zewnętrznymi:
            3.4.1.3.1. ogólne zasady funkcjonowania poszczególnych interfejsów- modele danych stosowane w interfejsach,
            3.4.1.3.2. specyfikacja szczegółowa poszczególnych interfejsów (wymagalność pól, typy pól, dopuszczalne zakresy wartości pól, opis znaczenia pól, powiązania z innymi polami, wykorzystanie słowników,
         3.4.1.4. Przykłady użycia wszystkich interfejsów:
            3.4.1.4.1. dla interfejsów plikowych: wzorcowe pliki na każdy przypadek użycia,
            3.4.1.4.2. dla interfejsów on-line'owych (webserwisy, adaptery i mediacje na szynie danych, procedury wbudowane itp.) przykłady wszystkich dopuszczalnych typów wywołań z ich parametrami,
         3.4.1.5. Lista i struktura słowników Systemu.
      3.4.2. Opisu konfiguracji serwerów, na których działa oprogramowanie, w tym:
         3.4.2.1. procesor – ilość corów wirtualnych
         3.4.2.2. RAM – wielkość pamięci RAM
         3.4.2.3. dyski – wielkość wymaganych zasobów dyskowych,

3.4.2.4. jeżeli System wykorzystuje dodatkowe urządzenia, należy podać pełną specyfikację komponentu (typ, numer seryjny) oraz dostarczyć sterowniki dla danego systemu operacyjnego
3.4.2.5. wymagania konfiguracji sieciowej (używane protokoły sieciowe, porty)
3.4.3. Opisu systemu operacyjnego, w tym:
3.4.3.1. wersja systemu operacyjnego,
3.4.3.2. wartości parametrów systemu operacyjnego które należy od wartości standardowej zmienić w związku z wymaganiami prawidłowego działania Systemu (np. ulimit, kernel.shmmni, kernel.sem),
3.4.3.3. lista pakietów oraz wersje niezbędne do prawidłowego działania Systemu,
3.4.4. Opisu baz danych, w tym:
3.4.4.1. wersja bazy danych (łącznie ze wszystkimi wymaganymi poprawkami)
3.4.4.2. lokalizacje plików binarnych systemu bazy danych oraz plików bazy danych (z podziałem na podkatalogi)
3.4.4.3. konfiguracja użytkowników w bazie danych, właściciel schematu Systemu, role, uprawnienia innych użytkowników bazy niezbędnych do pracy Systemu ich role i uprawnienia (Nie dopuszczalne jest nadawania roli Administrator lub DBA jako właściciela schematu Systemu)
3.4.4.4. konfiguracja przestrzeni tabel
3.4.4.5. kodowanie znaków w bazie danych
3.4.4.6. pliki konfiguracyjne bazy danych (kluczowe parametry niezbędne do wydajnego działania)
3.4.5. Serwera aplikacyjnego
3.4.5.1. wersja zainstalowanego oprogramowania aplikacyjnego (łącznie ze wszystkimi poprawkami)
3.4.5.2. opis instalacji
3.4.5.3. procedury aktualizacji
3.4.5.4. lista portów niezbędnych do prawidłowego działania,
3.4.5.5. lokalizacje plików konfiguracyjnych i logów
3.4.5.6. metody uruchamiania i zatrzymywania,
3.4.5.7. metody sprawdzania poprawności działania, monitorowania i weryfikowania poprawności pracy
3.4.5.8. informacje o sposobie uruchamiania się przy starcie systemu operacyjnego, jeżeli tak to dostarczenie odpowiednich skryptów startowych
3.4.5.9. konfiguracja plików systemowych (systemu operacyjnego), które są modyfikowane podczas instalacji
3.4.5.10. opis konfiguracji, parametry puli połączeń, alokacja pamięci itp.
3.4.5.11. procedury uruchamiania/zatrzymywania
3.5. Instrukcja wykonywania kopii zapasowej i archiwalnej, która powinna:
3.5.1. wskazać pliki i aplikacje niezbędne do działania systemu, które powinny podlegać archiwizowaniu,
3.5.2. jeżeli wykonanie kopii bezpieczeństwa wymaga zatrzymania systemu, Wykonawca powinien przedstawić odpowiedni skrypt lub procedurę do zatrzymywania i uruchamiania systemu,
3.5.3. zawierać procedury backupu systemu lub serwera aplikacyjnego jeśli jest dedykowany dla systemu
3.6. Procedury awaryjne zawierające:
3.6.1. procedury awaryjne powinny uwzględniać co najmniej dwa przypadki:
3.6.1.1. uszkodzenie logiczne Systemu (np. błędna edycja plików konfiguracyjnych, błąd przy wgrywaniu poprawek, błąd przy wprowadzaniu zmian konfiguracyjnych)
3.6.1.2. uszkodzenie fizyczne serwera (np. awaria dysków serwera, całej maszyny)
3.6.2. procedury postępowania w przypadku wystąpienia awarii.
3.6.3. procedury powinny mieć charakter scenariusza działań (krok po kroku opisane czynności administracyjne oraz diagnostyczne).

1.9. OCHRONA DANYCH OSOBOWYCH

Wykaz aktów prawnych określających uwarunkowania prawne w zakresie ochrony danych osobowych:

1. Ustawie z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2018 r., poz. 1000);
2. Rozporządzenia 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. Urz. UE L 119 z 04.05.2016, str. 1), dalej „RODO".

1.10. WYMAGANIA W ZAKRESIE BEZPIECZEŃSTWA

1. Wymagania podstawowe
   - 1.1. System ma posiadać mechanizmy zapewniające bezpieczeństwo przetwarzanych danych (Funkcje bezpieczeństwa). Funkcja bezpieczeństwa oznacza właściwość jaką mechanizmy bezpieczeństwa zapewniają przetwarzanym danym, tj.:
     - 1.1.1. dostępność danych - właściwość polegająca na tym, że dana osoba może korzystać z danych tylko w zakresie, w jakim jest do tego upoważniona;
     - 1.1.2. integralność danych - właściwość polegająca na tym, że dane nie zostaną zmienione, dodane lub usunięte w nieautoryzowany sposób;
     - 1.1.3. poufność danych - właściwość polegająca na tym, że dane nie zostaną udostępnione lub ujawnione osobom nieupoważnionym;
     - 1.1.4. rozliczalność działań - właściwość polegająca na tym, że określone działania/ operacje dowolnego użytkownika są jednoznacznie przypisane temu użytkownikowi i zarejestrowane w logach Systemu.
   - 1.2. System ma zapewniać ochronę przed atakami w warstwie aplikacji typu SQL injection, XSS, CSRF poprzez zastosowanie np. Content Security Policy, Content-Security-Policy-Report-Only, Cross-Origin Resource Sharing, X-Frame-Options, X-Content-Type-Options, HTTP Strict Transport Security, X-XSS-Protection.
2. Kontrola dostępu
   - 2.1. Dostęp do Systemu powinien być zintegrowany z Active Directory.
   - 2.2. Każdy użytkownik Systemu ma posiadać indywidualne konto dostępu.
   - 2.3. Dostęp do Systemu ma być poprzedzony identyfikacją i uwierzytelnieniem użytkownika (nie ma możliwości obejścia mechanizmów logowania).
   - 2.4. Podczas wprowadzania hasła do Systemu, nie jest ono wyświetlane jawnym tekstem na ekranie.
   - 2.5. Każdy użytkownik ma mieć możliwość dokonania zmiany i wyboru hasła w dowolnym czasie
   - 2.6. System weryfikuje i potwierdza poprawność zmiany hasła przez użytkownika.
   - 2.7. System wymusza zmianę hasła tymczasowego przy pierwszym logowaniu.
   - 2.8. Wprowadzane przez użytkowników hasła nie mogą być są zapisywane i przechowywane po stronie Klienta.
   - 2.9. System musi posiadać możliwość wykorzystania mechanizmu SSO (Single Sign On)
   - 2.10. Po poprawnym zalogowaniu, System musi prezentować datę i czas ostatniego logowania (udane/ nieudane, data i czas).
   - 2.11. Po próbie błędnego logowania, System nie może wyświetlać informacji nt. rzeczywistych przyczyn odrzucenia dostępu, wyświetlając komunikat "Nieprawidłowy identyfikator użytkownika lub hasło".
   - 2.12. System zapewnia poprawną obsługę błędów i nie prezentuje informacji wewnętrznych aplikacji (z plików, baz danych, kodów źródłowych).
3. Uprawnienia dostępu
   - 3.1. mechanizmy kontroli uprawnień oparte na rolach oraz musi umożliwiać określanie ról i uprawnień w dowolny sposób (bez ograniczeń).
   - 3.2. kontrola poziomu dostępu dla każdego użytkownika, zarówno w zakresie dostępu do przetwarzanych danych, jak i korzystania z jego funkcjonalności.
   - 3.3. Mechanizmy uprawnień muszą umożliwiać ograniczenie dostępu wyłącznie do takich danych oraz takiego zakresu funkcji, jaki jest niezbędny użytkownikowi/roli.
   - 3.4. podział użytkowników na grupy, z możliwością przypisania do kilku grup równocześnie.
   - 3.5. zarządzanie użytkownikami oraz grupami uzytkowników w zakresie ustalania uprawnień dostępu.

3.6. funkcjonalność umożliwiającą zablokowanie/ odblokowanie konta dowolnego użytkownika
3.7. Przydzielanie ról i uprawnień, profili administracyjnych musi odbywać się w Systemie.
3.8. tworzenie kont z dowolnymi uprawnieniami administracyjnymi, np. do zmiany uprawnień, konfiguracji parametrów (bez ograniczeń).
3.9. Dla każdej ze zdefiniowanych ról System musi umożliwiać dodanie opisu zawierającego zakres odpowiedzialności i uprawnień.
3.10. Każde uprawnienie w Systemie musi posiadać szczegółowy opis realizowanej funkcji.
3.11. drukowanie raportów, zawierających informacje o wszystkich profilach i uprawnieniach użytkownika lub grupy użytkowników w określonym przedziale czasowym (zawartość do uzgodnienia z bankiem).
3.12. Całe rozwiązanie musi zapewniać odpowiednie zabezpieczenia przed nieautoryzowanym dostępem na poziomie wszystkich komponentów serwera (system operacyjny, baza danych, serwery aplikacyjne, serwery WWW i inne, jeśli zostaną zastosowane).

4. Zarzadzanie sesją
4.1. System musi automatycznie zamykać sesję zalogowanego użytkownika po określonym czasie nieaktywności (parametr 0-60 minut - konfigurowany przed administratora w Systemie).
4.2. System musi zapewniać odpowiednie walidowanie wszystkich wprowadzanych danych, uniemożliwiając m.in. przechwycenie sesji zalogowanego użytkownika.
4.3. System musi zapewniać odpowiednie atrybuty bezpieczeństwa ciasteczek sesyjnych (cookie), blokując dostęp do nich z poziomu aktywnego kodu po stronie Systemu używanego przez Klienta (end-usera) oraz umożliwiać przesłanie ciasteczka tylko przez połączenie szyfrowane (httpOnly oraz secure).
4.4. System musi być odporny na tzw. kolizję klucza sesyjnego i zapewniać odpowiednią entropię podczas generowania klucza sesyjnego.
4.5. System musi posiadać ochronę przed obejściem mechanizmów zarządzania sesją.

5. Przechowywanie danych - Dane wrażliwe muszą być przechowywane na serwerze w postaci zaszyfrowanej (np. dane uwierzytelniające, kody, numery kart kredytowych, dane autoryzacyjne do bazy danych).

6. Weryfikacja danych oraz walidacja
6.1. Dane wejściowe do Systemu muszą podlegać mechanizmom kontroli i filtracji, które zapewniają wykrywanie następujących błędów:
6.1.1. wartości spoza dopuszczalnego zakresu,
6.1.2. niewłaściwe znaki w polach danych,
6.1.3. brakujące, niepoprawne lub niekompletne dane,
6.1.4. przekraczanie górnych i dolnych ograniczeń wielkości danych,
6.1.5. nieuprawnione lub niespójne dane kontrolne.
6.2. System musi zapewniać odpowiednie filtrowanie wszystkich wprowadzanych danych, uniemożliwiając nieautoryzowane wywołanie poleceń/zapytań i uzyskanie dostępu do danych lub wykonanie nieautoryzowanych działań w Systemie.
6.3. System musi zapewniać odpowiednie walidowanie wszystkich wprowadzanych danych, uniemożliwiając wykonanie skyptu, podmianę zawartości danych w Systemie lub przekierowanie użytkownika na inną stronę.
6.4. Po stronie serwera muszą być weryfikowane uprawnienia użytkownika do wszelkich żądanych danych, w szczególności realizowane kontrole uniemożliwiające manipulowanie referencjami do wewnętrznych obiektów typu plik, katalog, wartość klucza z bazy danych.
6.5. System musi posiadać zaimplementowane właściwe kontrole (mechanizmy walidacyjne) po stronie serwera, zapewniające, że w przypadku przekazania spreparowanego żądania nie będzie możliwości osiągnąć niedozwolonego działania aplikacji (np. uzyskanie nieautoryzowanego dostępu do danych / możliwość nieautoryzowanego wykonania operacji).
6.6. System musi umożliwiać sprawdzanie integralności przetwarzanych w nim danych cyfrowych oraz komponentów Systemu.

7. Transmisja danych
7.1. System musi wykorzystywać aktualne i silne szyfrowanie danych dla ochrony transmisji danych w relacji Klient (end-user) - Serwer (SSL).

7.2. System musi wykorzystywać szyfrowanie danych pomiędzy ich wymianą w obszarze poszczególnych komponentów Systemu (np. serwer Baz danych - Warstwa aplikacyjna) (SSL).

8. Kryptografia

8.1. Zabezpieczenia kryptograficzne dopuszczone do stosowania w Systemie i połączeniach do niego to:

8.1.1. protokół RSA-2048, AES-256,

8.1.2. funkcje skrótu (SHA-2) SHA-512, SHA-256,

8.1.3. protokół TLS 1.2 (także pomiędzy urządzeniem końcowym a serwerami aplikacyjnymi).

8.2. System musi zapewniać ochronę przed atakami słownikowym, tj. podczas tworzenia skrótów haseł dodawany ma być ciąg zaburzający, mający na celu powiększenie rozmiaru danych będących argumentem funkcji skrótu (min. 8 bajtów soli); dla każdego hasła generowana jest nowa sól (sposób dodawania soli do ustalenia z bankiem).

8.3. Każdy serwer świadczący usługi (dotyczy również mechanizmów webservice) musi być zabezpieczony z wykorzystaniem protokołu HTTPS; System dostarcza certyfikaty w standardzie X.509 wydane przez zaufany urząd certyfikacji (np. Unizeto, VeriSign).

9. Dzienniki zdarzeń

9.1. System musi posiadać mechanizmy umożliwiające rozliczalność działań użytkowników (w tym administratorów).

9.2. System musi posiadać mechanizmy audytu zdarzeń wraz z rejestracją daty i czasu operacji, IP, identyfikatora użytkownika oraz opisu zdarzenia w zakresie:

9.2.1. wywołania Klienta i odpowiedzi serwera (relacja Klient - serwer),

9.2.2. udanych i nieudanych prób dostępu do Systemu,

9.2.3. wylogowania użytkownika oraz zerwane ,

9.2.4. wykonanych działań,

9.2.5. zmiany danych, w tym parametrów systemowych, uprawnień dostępu, zablokowania/ odblokowania konta,

9.2.6. błędów i awarii Systemu, ataków na System.

9.3. System musi monitorować wszystkie zmiany obiektów. Historia zmian musi być zapisywana w dzienniku zdarzeń w sposób umożliwiający inspekcję i raportowanie. Informacje o zmianach, które muszą być zapisywane:

9.3.1. kto utworzył dany rekord,

9.3.2. kiedy dany rekord został utworzony (data i godzina),

9.3.3. kto zmodyfikował dany rekord,

9.3.4. kiedy dany rekord został zmodyfikowany (data i godzina).

9.4. System musi umożliwiać synchronizację czasu w domenie AD lub serwerem NTP.

9.5. System musi posiadać możliwość przesyłania dzienników zdarzeń do zewnętrznego serwera syslog.

9.6. System musi umożliwiać przechowywanie dzienników zdarzeń przez okres co najmniej 5 (pięciu) lat.

9.7. System musi posiadać mechanizmy automatycznego czyszczenia archiwalnych dzienników zdarzeń, np. powyżej 2 (dwóch) lat - retencję danych przechowywanych w dziennikach zdarzeń.

9.8. System musi zapewniać integralność dzienników zdarzeń oraz mechanizmy chroniące przed nieuprawnionym usunięciem.

10. Dodatkowe istotne wymagania

10.1. System przed odbiorem musi zostać poddany testom bezpieczeństwa przez Wykonawcę Systemu (komponenty sieciowe, infrastruktura serwerowa [w tym infrastruktura pamięci masowych], warstwę wirtualizacji [jeżeli jest przewidywana], warstwę systemów operacyjnych obsługujących system, warstwę bazodanową, aplikacyjna oraz front-end). Testy bezpieczeństwa Systemu będą wykonywane przez Wykonawcę w oparciu o aktualny standard OWASP.

10.2. Podczas wykonywania testów bezpieczeństwa przez Wykonawcę powinien także zostać wykonany proces utwardzania (hardeningu) rozwiązania.

10.3. System mus być poddawany przez dostawcę okresowym testom bezpieczeństwa za pomocą odpowiednich i aktualnych narzędzi (w celu utrzymania wysokiego poziomu bezpieczeństwa świadczonej usługi.

10.4. W zakresie logowania zdarzeń – wszystkie operacje wykonywane w (na) oraz przez System (pełna rozliczalność) muszą być możliwe do przekazania za pomocą protokołu syslog do serwera zdalnego. Dostawca przedstawi specyfikację komunikatów, umożliwiającą prawidłową interpretację parserów.

10.5. Kod Systemu (jeżeli będzie istniała technologiczna możliwość) zostanie wytworzony z zachowaniem dobrych wzorców projektowych, w zakresie pisania kodu (np. SOLID – programowanie obiektowe).

10.6. Do budowy Systemu zostaną użyte tylko komponenty aktualnie wspierane przez zewnętrznych dostawców rozwiązań, w tym społeczności OpenSource (np.: systemy operacyjne do zastosowań serwerowych, serwery aplikacji, bazy danych, frameworki). Komponenty te muszą być aktualnie wspierane przez zewnętrznych dostawców rozwiązań składowych Systemu, przez cały okres eksploatacji Systemu objęty serwisem Wykonawcy. Nie dopuszcza się tym samym produkcyjnej eksploatacji elementów składowych Systemu, zawierających znane podatności, czy błędy w działaniu jej komponentów, które zostały wyeliminowane przez dostawców zewnętrznych (np. społeczności OpenSource).

10.7. System zostanie zaprojektowany w taki sposób, by nie zaistniała techniczna przeszkoda związana z koniecznością podjęcia działań, zmierzających do usunięcia zidentyfikowanych luki bezpieczeństwa (np. musi istnieć możliwość usunięcia luki bezpieczeństwa związanej ze zidentyfikowaną znana podatnością w module serwera aplikacji).

10.8. Usuwanie Luk bezpieczeństwa Systemu będzie realizowane przez Wykonawcę nieodpłatnie. Luki bezpieczeństwa mogą zostać ujawnione w wyniku realizacji testów bezpieczeństwa przez Wykonawcę (np. podczas wewnętrznego procesu Wykonawcę dotyczącego produkcji i testowania oprogramowania), Zamawiającego lub w wyniku przekazania takiej informacji przez osoby trzecie.

10.9. Definicja Luki bezpieczeństwa: Stan Systemu (lub jego komponentu/modułu) obniżający poziom bezpieczeństwa Systemu (mając wpływ na Funkcje bezpieczeństwa) i umożliwiający wykonanie działań nieautoryzowanych; słabość Systemu mająca negatywny wpływ na Funkcję bezpieczeństwa. W szczególności Luką bezpieczeństwa jest stan, który:

10.9.1. może umożliwić w sposób nieautoryzowany dostęp do Systemu,

10.9.2. może umożliwić zdobycie dostępu do danych z naruszeniem określonych ograniczeń dostępu do tych danych,

10.9.3. może umożliwić podszywanie się pod innego użytkownika,

10.9.4. może umożliwić przeprowadzenie ataku, mogącego prowadzić do destabilizacji pracy Systemu lub czasowej lub ciągłej jego niedostępności, a także do trwałego uszkodzenia,

10.9.5. może umożliwić nieuprawnione gromadzenie informacji,

10.9.6. może umożliwić ukrywanie wykonanych czynności,

ROZDZIAŁ 2 –SZCZEGÓŁOWY ZAKRES PRAC

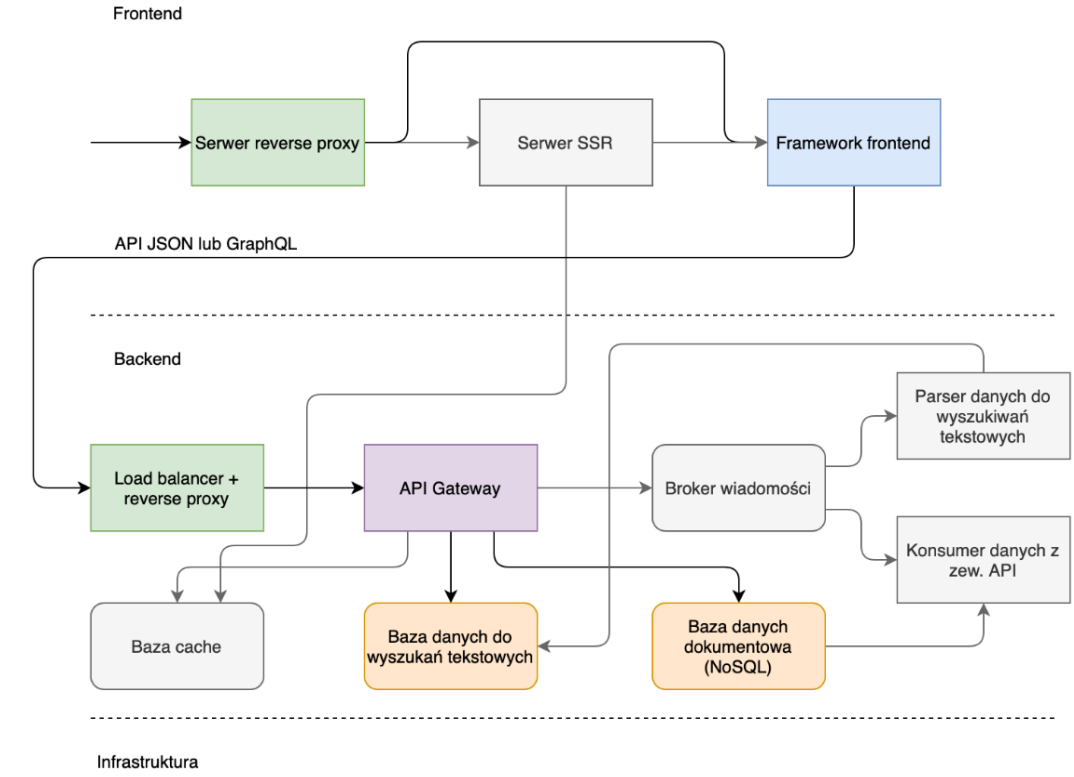
2.1. Wymagania Ogólne

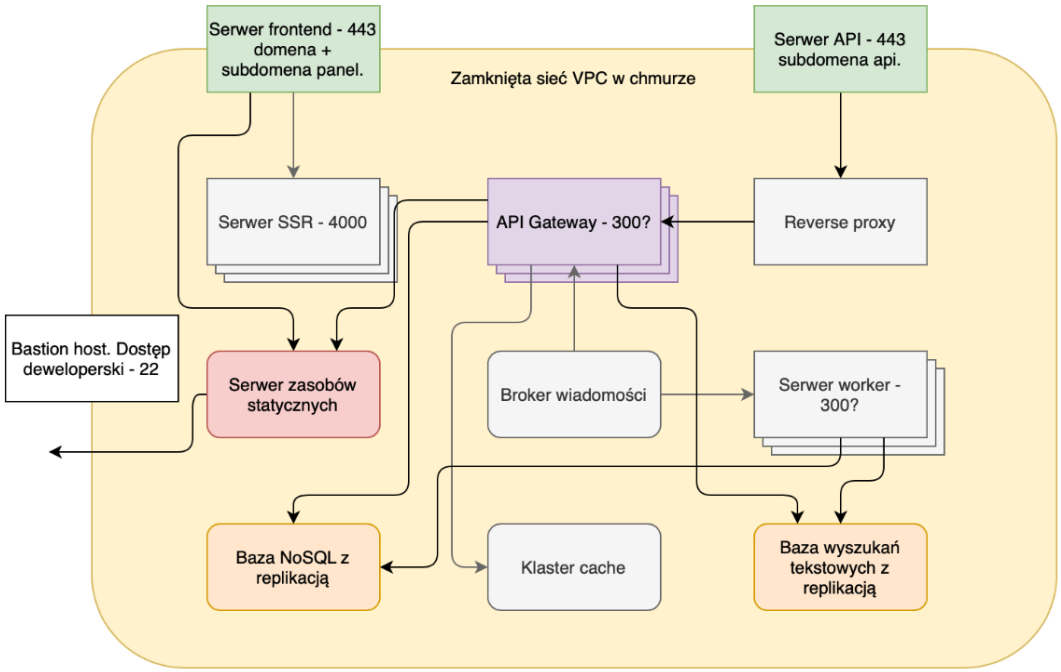
1. Przedmiotem zamówienia jest zaprojektowanie platformy rezerwacyjnej typu all-in-one przeznaczonej do wspomagania działania firmy Zamawiającego oraz usprawnienia obsługi klientów.
2. Zaprojektowany przez Wykonawcę system musi posiadać łatwy, intuicyjny i przyjazny w obsłudze system organizacji imprez turystycznych.
3. System musi zapewniać:
   3.1. szeroki i natychmiastowy dostęp zarówno do rezerwacji ofert krajowych, jak i zagranicznych,
   3.2. ułatwiać porównanie ofert i pozwalać na wybór najlepszej opcji.
   3.3. integrację ofert współpracujących z Zamawiającym dostawców usług i konsolidatorów w celu przygotowania kompleksowej oferty,
   3.4. umożliwiać bezpośrednią rezerwację i zakup imprezy turystycznej.
4. System musi umożliwiać klientowi stworzenie samodzielnej oferty zawierającej:
   4.1. hotele,
   4.2. loty,
   4.3. transfery,
   4.4. wynajem samochodów
   4.5. atrakcje turystyczne
   4.6. rejsy,
   4.7. ubezpieczenia ,
   4.8. pielgrzymki,
   4.9. wycieczki,
   4.10. wycieczki objazdowe
   4.11. kolonie, obozy młodzieżowe
   4.12. parkingi
   4.13. autokary
   4.14. city break
   4.15. pakiety spa
   4.16. pakiety lecznicze/sanatoria
5. System musi umożliwiać:
   5.1. łatwe porównanie wielu ofert w jednym miejscu
   5.2. wybranie najlepszej z punktu widzenia klienta opcji w najlepszej cenie.
   5.3. Łatwe filtrowanie i sortowanie ofert wg wybranych kryteriów
6. Standaryzacja procesu wyszukiwania musi umożliwiać:
   6.1. szybki wybór właściwej oferty,
   6.2. przyśpieszać proces rezerwacji,
   6.3. umożliwiać dostęp do historii rezerwacji,
   6.4. łatwego tworzenia raportów.
7. System musi być zaprojektowany w oparciu o nowoczesne i zaawansowane technologie internetowe, umożliwiające użytkownikom dostęp do systemu w trybie 24/7.
8. System musi być tak zaprojektowany, by być udostępniany:
   8.1. pracownikom Zamawiającego,
   8.2. współpracującym agentom,
   8.3. stałym klientom
   8.4. pracownikom obsługiwanych firm
   8.5. nowym klientom.
9. Za pomocą systemu musi być możliwość samodzielnego wyszukiwania i rezerwowania podróży przez klienta
10. System musi odznaczać się intuicyjnością obsługi.
11. Wymagane jest by praca z systemem była intuicyjna i nie wymagała szkolenia użytkowników.
12. System musi przechowywać ustawienia profili stałych klientów:
13. System musi umożliwiać:

13.1. dostęp do historycznych rezerwacji,
13.2. tworzenia prostych raportów,
13.3. przyspieszać proces rezerwacji w oparciu o dane historyczne.
14. Klient musi mieć możliwość samodzielnego:
14.1. przeglądu historii swoich rezerwacji
14.2. przeglądu ofert,
14.3. ,utworzenia własnej rezerwacji,
14.4.
14.5. dokonania płatności za imprezę,
14.6. dobrania dodatkowych usług jak:
14.6.1. ubezpieczenie,
14.6.2. wizowanie,
14.6.3. dodatkowe atrakcje
15. System musi umożliwiać pracownikom Zamawiającego obsługę finansową sprzedawanych usług, w tym:
15.1. Umów zawieranych z klientami
15.2. Voucherów grupowych i indywidualnych
15.3. Umów ubezpieczeniowych
15.4. Dokumentów sprzedaży, w tym:
15.4.1. Faktur VAT,
15.4.2. Faktur korekt,
15.4.3. Faktur VAT marża,
15.4.4. Korekt faktur VAT marża,
15.4.5. Paragonów,
15.4.6. Paragonów korekt
15.4.7. Not
15.4.8. Not korekt
15.5. Dokumentów kasowych, w tym:
15.5.1. KP,
15.5.2. KW,
15.5.3. Raportów kasowych;
15.6. Wzorce dokumentów Zamawiający dostarczy Wykonawcy na etapie realizacji zamówienia.
15.7. System musi mieć możliwość eksportu danych finansowych do zewnętrznego systemu F/K
15.8. System musi mieć możliwość rozksięgowania operacji w systemie na podstawie zaimportowanego pliku tekstowego, bazującego na standardzie komunikatu SWIFT MT940

2.2. Wymagania architektoniczne

1. Oprogramowanie powinno być zbudowane w architekturze otwartej jako wielowarstwowa aplikacja webowa.
2. Oprogramowanie powinno być zbudowane w architekturze spełniającej następujące wymagania:





Legenda:

- *Zielony - serwery otwarte na świat - dostęp dla użytkowników*
- *Żółty - Chmura / sieć wewnętrzna.*
- *Pomarańcz - bazy danych.*
- *Szary - opcjonalne, może zmienić na odpowiednie technologie?*
- *Fiolet - serwer(y) backendowe.*
- *Niebieski - serwer(y) frontendowe.*
- *Czerwony - serwer plików statycznych.*

3. Architektura rozwiązania powinna być oparta o:
   3.1. rozwiązanie chmurowe (np.: MS Azure, AWS, Google Cloud Platform)
   3.2. rozwiązanie pozwalające na tworzenie sieci wewnętrznych VPC,
   3.3. automatyczny load balancing,
   3.4. uruchamianie maszyn wirtualnych na bazie podanych obrazów,
   3.5. wszystkie serwery wewnętrzne dostępne jedynie wewnątrz sieci.
   3.6. wszystkie bazy zabezpieczone dodatkowo wymaganą autoryzacją.
   3.7. wyjście z VPC przez serwery API oraz frontend poprzez HTTPS,
   3.8. dostęp do bastionu deweloperskiego przez SSH
   3.9. dodatkowy serwis pozwalający na udostępnianie statycznych zasobów
   3.10. rozwiązania zapewniające maksymalnie efektywne pozycjonowanie strony.
4. Wymagania wobec obszaru Backend:
   4.1. API obsługujące frontend oraz parsujące dane z zewnętrznych serwisów.
   4.2. baza danych z wykorzystaniem replikacji.
   4.3. baza danych do wyszukań tekstowych,
   4.4. Parsowanie danych z serwisów zewnętrznych
   4.5. Serwer cache
   4.6. Broker wiadomości.
   4.7. Mechanizm szyfrowania danych
   4.8. Logowanie Single Sign On
5. Wymagania wobec obszaru Frontend:
   5.1. strona główna oraz panele: klienta, agenta i administratora oparte o framework z wykorzystaniem biblioteki do zarządzania stanem.
   5.2. Server side renderingu (SSR) w celu poprawienia wydajności i SEO.
   5.3. Komunikacja z API za pomocą REST JSON lub GraphQL
6. Uprawnienia
   6.1. W aplikacji powinien być zaimplementowany mechanizm zarządzania uprawnieniami oparty na rolach użytkowników.
   6.2. W modelu tym, każdy użytkownik powinien mieć możliwość przypisania wielu ról. Role te mogą w dowolny sposób grupować uprawnienia.
   6.3. Uprawnienia powinny dotyczyć poszczególnych funkcji aplikacji: np. wyświetlanie określonej informacji, edytowanie określonych danych, generowania raportu.
7. Wymagania wobec zastosowanego oprogramowania:
   7.1. Do utworzenia aplikacji muszą być użyte wersje komponentów, które posiadają aktualne wsparcie.
   7.2. Zastosowane rozwiązanie powinno mieć możliwie najniższe koszty utrzymania oraz uwzględniać możliwość zastosowania komponentów typu open source,
   7.3. Komunikacja stacji roboczej z systemem powinna być realizowana wyłącznie z wykorzystaniem https.
   7.4. System musi umożliwiać prace z ostatnimi wersjami najbardziej popularnych na rynku przeglądarek, minimum: Chrom, Edge, Firefox, Opera
8. Integracje
   8.1. Oprogramowanie musi posiadać interfejs wymiany danych w trybie on-line z następującymi kontrahentami:
      8.1.1. hotele i transfery - https://www.hotelbeds.com/home
      8.1.2. hotele:
         8.1.2.1. https://www.hotelston.com
         8.1.2.2. https://www.miki.co.uk
         8.1.2.3. https://www.americantours.com
      8.1.3. przeloty – https://www.epower.amadeus.com
   8.2. Oprogramowanie musi posiadać interfejs zapewniający eksport przygotowanej oferty do systemu Dyn@mite firmy Merlinx https://www.merlinx.pl/

9. Dynamiczne pakietowanie ofert:
   9.1. Oprogramowanie musi posiadać funkcjonalność kalkulowania ofert turystycznych, złożonych z co najmniej kilku usług, w czasie rzeczywistym, tworzonych dynamicznie przy użyciu dostępu do bazy danych podmiotów agregujących oferty, w zakresie:
      9.1.1. hotele i transfery - https://www.hotelbeds.com/home
      9.1.2. hotele:
         9.1.2.1. baza własnych kontrahentów
         9.1.2.2. https://www.hotelston.com
         9.1.2.3. https://www.miki.co.uk
         9.1.2.4. https://www.americantours.com
      9.1.3. przeloty – https://www.epower.amadeus.com
   9.2. Oprogramowanie musi posiadać funkcjonalność dynamicznego łączenie usług turystycznych określonych w punkcie 8.1 i prezentowanie ich w formie gotowych pakietów turystycznych.

2.3. Szczegółowy sposób wykonania umowy

1. Wykonawca dla oprogramowania stanowiącego przedmiot zamówienia, przez okres trwania gwarancji zadeklarowany w Formularzu Ofertowym, zapewni:
   1.1. środowisko chmurowe dla działania oprogramowania;
   1.2. prawidłowe działanie środowiska chmurowego oraz prawidłowe działanie uruchomionego na nim oprogramowania;
   1.3. administrowanie oprogramowaniem
   1.4. bezpieczny dostęp do serwerów, na których zlokalizowane jest Oprogramowanie, chroniony za pomocą systemu zapór ogniowych (firewall);
   1.5. komunikację z Oprogramowaniem za pomocą bezpiecznych szyfrowanych połączeń;
   1.6. bieżącą aktualizację wykorzystanego oprogramowania narzędziowego;
   1.7. bieżącą aktualizację oprogramowania, o ile to będzie konieczne;
   1.8. bezpieczne przechowywanie danych wprowadzonych przez Zamawiającego do oprogramowania, w tym danych osobowych, w zakresie w jakim zostaną umieszczone przez Zamawiającego;
   1.9. wykonywanie minimum raz dziennie aktualnej kopi danych, przechowywanej przez co najmniej przez 90 dni od daty wykonania;
   1.10. zabezpieczy dane Zamawiającego, przechowując je w minimum jednej kopii, zlokalizowanej w środowisku chmurowym oraz udostępni kanał backupu danych na urządzenie wskazane przez Zamawiającego;
2. Wykonawca niezwłocznie poinformuje Zamawiającego o incydentach zagrażających bezpieczeństwu danych;
3. Wykonawca przeszkoli użytkowników Zamawiającego:
   3.1. w liczbie maksymalnie 20 osób,
   3.2. w liczbie minimum 4 godzin lekcyjnych na każdego pracownika
   3.3. w grupach i terminie ustalonym z Zamawiającym,
   3.4. w siedzibie i na sprzęcie Zamawiającego

2.4. Wymagania funkcjonalne

Szczegółowe wymagania funkcjonalne opisane są w Załączniku 1.1 do Zapytania ofertowego.