**OR-D-III.272.103.2024.MK**

**Zał. nr 2 do SWZ**

**Załącznik nr 1 do Umowy Nr…..**

**OPIS PRZEDMIOTU ZAMÓWIENIA**

Przedmiotem zamówienia jest Refaktoryzacja Systemu składającego się z modułów: do nadzoru nad aparaturą medyczną, do obsługi rejestru zdarzeń niepożądanych, do administrowania nieruchomością. Zamówienie przewiduje możliwość wdrożenia rozwiązania o tych samych funkcjonalnościach wraz konfiguracją i uruchomieniem na środowisku wskazanym przez Zamawiającego, a także świadczenie Serwisu technicznego, wykonywanie zlecanych Modyfikacji oraz prowadzenie instruktaży.

Funkcjonujące Systemy Dziedzinowe stanowią dedykowany system informatyczny zbudowany na platformie Cameleoo w oparciu o bazę danych PostgreSQL (wersja 9.3.5, 64 bit), obiektowy język programowania Groovy i środowisko Java (jre\_7 u\_11). Podczas budowy systemu wykorzystano autorski system wbudowanych automatycznych algorytmów uzupełniania i nadpisywania baz danych oraz jednoczesnego wprowadzania zmian w samych systemach takich jak m.in.: tabele, skrypty, dodatkowe pola, formularze. Realizacja zleconych zadań obsługi systemów dziedzinowych wiąże się z koniecznością znajomości technologii w stopniu pozwalającym na ich wykonanie , w tym migracji danych, a w razie potrzeby zdolności do przedstawienia koncepcji rozwiązań. Rozwiązanie zostało zainstalowane lokalnie u Partnerów.

Przedmiot zamówienia będzie realizowany zgodnie z niniejszym dokumentem oraz Planem realizacji zamówienia przygotowanym przez Wykonawcę i będącym załącznikiem do Oferty. Plan realizacji zamówienia zawiera:

1. zwięzły opis sposobu oraz podejścia do realizacji przedmiotu zamówienia, w tym zastosowane rozwiązania techniczne wykonania refaktoryzacji lub dostarczenia rozwiązania spełniającego wymagania opisu przedmiotu zamówienia,
2. zwięzły opis sposobu organizacji pracy,
3. sposób komunikacji w zespole oraz z Zamawiającym,
4. monitorowanie procesu realizacji zadań, w tym przez Zamawiającego,
5. stosowane narzędzia, w tym rozwiązania informatyczne,
6. wykorzystanie internetowego systemu zgłoszeniowego do wzajemnej komunikacji interesariuszy,
7. opis metodologii pracy,
8. wykorzystywane metodyki zarządzania realizacją przedmiotu zamówienia,
9. planowany proces wytwórczy, współpraca przy opracowywaniu dokumentacji.

Symbole CPV:

72265000-0 Usługi konfiguracji oprogramowania,

72000000-5 Usługi informatyczne: konsultacyjne, opracowywania oprogramowania, internetowe i wsparcia,

72250000-2 Usługi w zakresie konserwacji i wsparcia systemów,

72260000-5 Usługi w zakresie oprogramowania,

72267000-4 Usługi w zakresie konserwacji i napraw oprogramowania,

72227000-2 Usługi doradcze w zakresie integracji oprogramowania;

72310000-1 Usługi przetwarzania danych;

72312100-6 Usługi przygotowywania danych.

Słownik pojęć i skrótów:

Słownik użytych w OPZ pojęć i skrótów został przedstawiony w § 1 Umowy.

Etap I Umowy – Refaktoryzacja Systemu, o której mowa w § 3 pkt 1) Umowy.

1. Zadanie dotyczące Refaktoryzacji Systemu polega na aktualizacji Systemu, w tym uruchomieniu funkcjonalności Systemu w technologii umożliwiającej obsługę i rozwój produktu, obsługę poprawek i aktualizacji, ograniczenie podatności na złośliwe oprogramowanie.
2. Wersja Zreafaktoryzowana może zostać wykonana poprzez modyfikację funkcjonującego rozwiązania lub poprzez zastosowanie technologii innej, niż aktualna, z zastrzeżeniem, że musi realizować co najmniej funkcjonalności określone w Dokumentacji stanowiącej załączniki nr 11-14 do Umowy.
3. Realizacja zadania nastąpi poprzez zaktualizowanie funkcjonujących systemów dziedzinowych, w tym zmianę wersji języka programowania na powszechnie stosowane języki w ich najnowszej wersji na dzień dostarczenia Wersji Zrefaktoryzowanej lub poprzez wdrożenie rozwiązania równoważnego do obecnie użytkowanych systemów dziedzinowych pod względem funkcjonalności Systemu.
4. Każda wdrażana wersja musi być wykonana w technologii lub języku oraz działać na silnikach i frameworkach podlegających publicznym automatycznym aktualizacjom, zawierającym w szczególności funkcje rozszerzenia oraz poprawki, mające na celu zwiększenie bezpieczeństwa i wydajności tworzenia i obsługi programów, co najmniej przez okres trwania zobowiązań Umowy.
5. Refaktoryzacja musi uwzględniać wymagania dotyczące funkcjonalności jak i bezpieczeństwa danych, w tym uruchomienie środowiska odpornego na podatności, w technologii umożliwiającej wdrożenie poprawek i aktualizacji Systemu oraz powiązanych środowisk.
6. Refaktoryzacja może zostać wykonana poprzez dostarczenie i wdrożenie rozwiązania równoważnego, przez które rozumie się wdrożenie systemu analogicznego do Systemu, o tym samym przeznaczeniu, obsługującego co najmniej te same procesy, posiadającego co najmniej funkcjonalności oraz spełniającego wymagania bezpieczeństwa określone w OPZ i Dokumentacji.
7. Wykonawca nie może w jakikolwiek sposób (systemowo, prawnie, formalnie lub technicznie, w tym poprzez ograniczenia w Systemie) ograniczać Zamawiającemu dostępu do jakichkolwiek mechanizmów bazodanowych i integracyjnych Wersji Zreafaktoryzowanej.
8. Wersja Zrefaktoryzowana nie może mieć ograniczeń użytkowania w zakresie liczby użytkowników, liczby wprowadzonych rekordów, woluminu przechowywanych lub przetwarzanych danych, ograniczenia możliwej do przydzielenia pamięci RAM, zasobów procesora.
9. Realizacja zadania obejmuje instalację i konfigurację Systemu na infrastrukturze wskazanej przez Zamawiającego.
10. System ma umożliwiać obsługę wielu użytkowników, przypisanych do jednostek organizacyjnych poszczególnych Partnerów, na zasadzie unikalnych kont użytkownika wraz z możliwością przypisania użytkownikom ról. Liczba Partnerów dla których nastąpi uruchomienie będzie nie większa niż liczba jednostek wskazanych w Załączniku nr 15 do Umowy, przy czym zakłada się maksymalnie 100 użytkowników korzystających jednocześnie z Systemu.
11. Refaktoryzacja Systemu uwzględnia sporządzenie analizy zaangażowania zasobów niezbędnych do przeprowadzenia instalacji systemu na infrastrukturze wskazanej przez Zamawiającego, wydzielenia odseparowanej przestrzeni dla poszczególnych Partnerów oraz przypisanie zasobów sprzętowych, w tym pamięci i zasobów procesora dla obsługi zadania. System zrefaktoryzowany musi być przystosowany do pracy w modelu wielofirmowym, przede wszystkim poprzez obsługę wielu jednostek jednocześnie oraz możliwość logicznego wydzielenia różnych jednostek, obsługiwanych procesów i przetwarzanych danych w jednym systemie zainstalowanym na jednej platformie w jednym środowisku.
12. W ramach zadania Wykonawca będzie współpracował z administratorem lokalnym Partnera w zakresie obsługi połączenia z infrastrukturą na której postawiono System.
13. Dane umieszczone przez Partnera w Systemie stanowią jego własność podlegającą ochronie, w związku z tym należy ograniczyć możliwość wglądu do przechowywanych informacji wyłącznie do przedstawicieli danego Partnera, zgodnie z nadanymi uprawnieniami dla poszczególnych użytkowników w ramach poszczególnych Partnerów.
14. Architektura systemu powinna pozwalać na automatyczne (harmonogramowane) tworzenie lokalnych kopii bezpieczeństwa danych na infrastrukturze wskazanej przez Partnera oraz możliwość zachowania niezależnej (odrębnej) kopii bezpieczeństwa danych na wskazanej przez Zamawiającego infrastrukturze, obsługiwanych z warstwy aplikacyjnej systemu.
15. Wykonawca skonfiguruje w Systemie politykę haseł zgodnie z wymaganiami Zamawiającego, w zakresie:
16. obowiązku zastosowania różnych i niepowtarzających się w bezpośrednim następstwie znaków, gdzie hasło musi zawierać wielkie i małe litery, cyfry i symbole specjalne i minimalnej oraz ustanowienia minimalnej liczby znaków hasła na 16 znaków,
17. obowiązku okresowej zmiany hasła w określonym przedziale czasu lub po wskazaniu konkretnej daty dla zmiany hasła oraz wymuszenie przejścia procedury zmiany hasła,
18. weryfikacji powtarzalności stosowanych haseł oraz zapisywania starych haseł, aby użytkownicy nie używali w okresie co najmniej 3 m-cy zastosowanych wcześniej haseł,
19. możliwości zmiany hasła przez użytkownika w dowolnym momencie, przy wykorzystaniu rozwiązania potwierdzającego tożsamość użytkownika, tj. wysłanie linka na email użytkownika lub uwierzytelnianie dwuskładnikowe.

Hasła użytkowników powinny być przechowywane w Systemie w sposób zaszyfrowany algorytmem ustalonym z Zamawiającym.

1. Połączenie do Systemu powinno być szyfrowane protokołem https oraz certyfikatem SSL. Wykonawca jest zobowiązany do instalacji i aktualizacji niezbędnych certyfikatów w czasie trwania Umowy.
2. System musi umożliwiać przeprowadzenie audytu operacji wykonywanych przez użytkowników.
3. Instalację, konfigurację oraz uruchomienie Systemu w infrastrukturze teleinformatycznej  wskazanej przez Zamawiającego należy zrealizować zgodnie z wytycznymi ustalonymi z Zamawiającym.
4. Wymagane jest wsparcie dla przeglądarek internetowych (Microsoft Edge, Mozilla Firefox, Chrome), Safari w najnowszych stabilnych wersjach oraz dostosowanie do aktualizowanych wersji przeglądarki, co najmniej w okresie świadczenia wsparcia wynikającego z Umowy.
5. System musi dynamicznie przypisywać użytkownikom poziom bezpieczeństwa, bazując na atrybutach przypisanych użytkownikowi w procesie autentykacji.
6. System musi działać restryktywnie udzielając użytkownikom dostępu w zakresie posiadanych uprawnień.
7. Wykonawca przygotuje i wdroży rozwiązanie dotyczące podziału i zasad przyznawania uprawnień dla poszczególnych użytkowników i grup użytkowników.
8. Wykonawca utworzy środowiska deweloperskie, testowe i produkcyjne na wskazanych przez Zamawiającego serwerach wirtualnych zgodnie z przyjętymi założeniami:

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Rodzaj sprzętu/parametru technicznego**  | **Wartość minimalna parametru technicznego** | **Wartość maksymalna parametru technicznego** |
| Infrastruktura na środowisko produkcyjne |
| 1. | Przyznana liczba rdzeni procesora na serwerze wirtualnym | 16 | 64 |
| 2. | Szybkość taktowania procesora fizycznego | 2,0 GHz | 3,2 GHz |
| 3. | Pamięć operacyjna pojemność | 64GB | 128GB |
| 4. | Przestrzeń dyskowa | 10TB | 25TB |
| Infrastruktura na środowisko testowe |
| 1. | Przyznana liczba rdzeni procesora na serwerze wirtualnym | 16 | 32 |
| 2. | Szybkość taktowania procesora fizycznego | 2,0 GHz | 3,2 GHz |
| 3. | Pamięć operacyjna pojemność | 32GB | 128GB |
| 4. | Przestrzeń dyskowa | 1TB | 15TB |
| Infrastruktura na środowisko deweloperskie |
| 1. | Przyznana liczba rdzeni procesora na serwerze wirtualnym | 4 | 32 |
| 2. | Szybkość taktowania procesora fizycznego | 2,0 GHz | 3,2 GHz |
| 3. | Pamięć operacyjna pojemność | 32GB | 64GB |
| 4. | Przestrzeń dyskowa | 1TB | 15TB |

1. Wykonawca zobowiązany jest do przeprowadzania wszelkich zmian w Systemie w sposób, który nie spowoduje zakłóceń w funkcjonowaniu integracji Systemów Dziedzinowych z Systemem Business Intelligence posiadanym przez Zamawiającego.
2. Funkcjonalności Systemu, w tym jego Modyfikacje muszą być zgodne z zakresem integracji z Systemem Business Intelligence, który jest zasilany danymi funkcjonujących Systemów Dziedzinowych, w tym umożliwiać eksport danych do innych systemów.
3. W przypadku wystąpienia problemów z integracją z Systemem Business Intelligence, Wykonawca zobowiązany jest do niezwłocznego podjęcia działań naprawczych w celu przywrócenia pełnej funkcjonalności integracji, bez dodatkowych kosztów dla Zamawiającego.
4. Wykonawca zapewni wsparcie w zakresie analizy i rozwiązywania problemów z integracją z Systemem Business Intelligence, które mogą wynikać z wdrażanych zmian.
5. Wykonawca zobowiązany jest do bezwzględnego przestrzegania wszelkich obowiązujących u Zamawiającego i przekazanych do Wykonawcy zasad i procedur bezpieczeństwa, w szczególności udzielać odpowiedzi i wyjaśnień w przypadku przeprowadzania kontroli bezpieczeństwa.
6. Wykonawca jest zobowiązany do dostarczenia wersji instalacyjnej Systemu oraz paczki instalacyjnej zawierającej gotowy obraz maszyny wirtualnej z zainstalowanym Systemem oraz wykonać konfigurację Systemu. Konfiguracja Systemu ma odbywać się poprzez wczytanie pliku konfiguracyjnego jak również manualnie poprzez panel administracyjny.

Etap II Umowy. Świadczenie usług serwisu technicznego, o których mowa w § 3 pkt 2), pkt 4) Umowy

1. Realizacja usługi serwisu technicznego Systemu obejmuje:
2. utrzymanie funkcjonalności i wydajności produkcyjnej;
3. usuwanie awarii i usterek;
4. wdrożenie poprawek wynikających z realizacji pkt 1 i 4 - 7 dla utrzymania funkcjonalności i sprawności Systemu;
5. zapewnienie bezpieczeństwa danych;
6. obsługę zadań nadzoru nad Systemem, w tym analizy zachowań i monitoring Systemu pod względem podatności na awarie, diagnozowanie podatności oraz realizowanie działań naprawczych;
7. prowadzenie diagnostyki Systemu;
8. realizację zadań związanych z utrzymaniem Systemu w zgodności z obowiązującymi przepisami prawa;
9. wsparcie Zamawiającego i Partnerów w przygotowaniu i wykonaniu migracji danych;
10. instalację lub deinstalację Systemu na wskazanych przez Zamawiającego środowiskach lokalnych;
11. Realizacja zadań związanych z usługą wsparcia w ramach serwisu technicznego obejmuje:
12. konsultacje telefoniczne w Godzinach Roboczych (usługa infolinii), mających na celu rozwiązywanie problemów z eksploatacją lub działaniem Systemu;
13. konsultacje drogą elektroniczną, w szczególności poprzez ISZ, mające na celu rozwiązywanie problemów związanych z eksploatacją lub działaniem Systemu;
14. obsługę zadań wsparcia Zamawiającego i Partnerów w zakresie przygotowania i migracji danych oraz instalacji Systemu u wskazanych przez Zamawiającego Partnerów;
15. obsługę zgłoszeń awarii Zamawiającego i Partnerów w terminach wskazanych w Umowie;
16. realizację wsparcia Zamawiającego i Partnerów wskazanych w Załączniku nr 15 do Umowy;
17. opracowywanie i aktualizację Dokumentacji i przekazywanie jej Zamawiającemu oraz zamieszczanie zaktualizowanej Dokumentacji w repozytorium dokumentacji w ISZ.
18. Procedura zgłaszania nieprawidłowości w działaniu systemów informatycznych - stanowiąca załącznik nr 2 do OPZ, przedstawia informację w zakresie wymaganej obsługi zgłoszeń w ramach systemu ISZ,
19. Informacje dotyczące komunikacji z zespołem wsparcia użytkownika Systemów Dziedzinowych, w tym adres dostępu do platformy ISZ, adres email i numeru telefonu do kontaktu, wskazane przez Wykonawcę w dokumencie Procedura zgłaszania nieprawidłowości w działaniu systemów informatycznych - stanowiącym załącznik nr 2 do OPZ, są wiążące a w przypadku wystąpienia zmiany, podlegają niezwłocznej aktualizacji przez Wykonawcę i udostępnieniu do Zamawiającego i Partnerów,
20. Obsługa zgłoszeń będzie odbywała się w ISZ udostępnionym przez Wykonawcę dla Partnerów oraz Zamawiającego, po wystąpieniu przez Partnera lub Zamawiającego o nadanie dostępu do platformy zgłoszeniowej ISZ.
21. W przypadku niedostępności ISZ, przez czas jego niedostępności, obsługa zgłoszeń będzie następowała poprzez dedykowany adres email obsługiwany przez Wykonawcę przed rozpoczęciem świadczenia Serwisu technicznego według ;
22. Po ustąpieniu okoliczności związanych z niedostępnością Systemu Zgłoszeniowego, Wykonawca zobowiązany jest do uzupełnienia zgłoszeń w ISZ.
23. W trakcie wykonywania Umowy Strony będą każdorazowo powoływały się na numer nadany w zgłoszeniu lub sygnatury nadanej przy zgłoszeniach email.
24. Usługa konsultacji telefonicznych realizowana będzie pod numerem telefonu wskazanym przez Wykonawcę w formie pisemnej. Wykonawca jest zobowiązany do przekazania informacji o numerze telefonu do obsługi konsultacji telefonicznych przed rozpoczęciem świadczenia usług Serwisu technicznego oraz jego bieżącej aktualizacji. Brak wskazania numeru telefonu do obsługi konsultacji oraz zgłoszeń użytkowników jest równoznaczny z brakiem świadczenia usług serwisowych.
25. Usługa usuwania Awarii i Usterek zgłoszonych przez Zamawiającego podczas eksploatowania Systemu polegać będzie na wykonywaniu napraw i świadczona będzie na warunkach określonych w treści Umowy.
26. Wszelkie dostarczone zmiany Systemu, w szczególności wykonane w ramach serwisu technicznego lub Modyfikacji, muszą zawierać ich opis wyrażony w języku polskim, wraz z wykazem zmian w funkcjonalnościach oprogramowania w porównaniu z wersją poprzednią oraz zaktualizowaną Dokumentację.
27. Wykonana zmiana w Systemie, w szczególności wykonane w ramach serwisu technicznego lub Modyfikacji, po jej zaimplementowaniu w Systemie stanie się ich częścią oraz zostanie objęta warunkami licencyjnymi określonymi w Umowie dla Systemu, a także zostanie objęta usługami serwisu technicznego.
28. W przypadku wystąpienia i zgłoszenia przez Zamawiającego:
	1. Awarii krytycznej - Wykonawca usunie Awarię krytyczną w terminie 36 godzin od momentu zgłoszenia, a w przypadku braku możliwości usunięcia Awarii krytycznej w terminie, Wykonawca zaproponuje Obejście;
	2. Awarii niekrytycznej - Wykonawca usunie Awarię niekrytyczną w terminie 4 Dni Roboczych licząc od dnia następnego po dniu zgłoszenia, a w przypadku niemożności usunięcia Awarii niekrytycznej w takim terminie, Wykonawca zaproponuje Obejście;
	3. Usterek - Wykonawca usunie Usterkę w terminie 4 Dni Roboczych licząc od dnia następnego po dniu zgłoszenia, a w przypadku niemożności usunięcia Usterki w takim terminie, Wykonawca zaproponuje Obejście;
	4. W przypadku zaproponowania Obejścia termin na usunięcie Awarii /Usterki, określony powyżej zostaje wydłużony odpowiednio do 5 Dni Roboczych w przypadku Awarii krytycznej, do 7 Dni Roboczych w przypadku Awarii niekrytycznej i Usterki.
29. Zgłoszenia problemów i pytań w ramach konsultacji świadczonych drogą elektroniczną przyjmowane będą przez całą dobę z zastrzeżeniem, że zgłoszenia przesłane do Wykonawcy po godzinie 16:00 danego Dnia Roboczego będą traktowane jako zgłoszenia doręczone następnego Dnia Roboczego, a zgłoszenia doręczone Wykonawcy w innym dniu, niż Dni Robocze, traktowane będą jako doręczone w Dniu Roboczym przypadającym bezpośrednio po dniach wolnych (tj. innych niż Dni Robocze).
30. W przypadku zgłoszenia Awarii/Usterki, gdzie zgłoszenie zawiera niepełne lub niewystarczające informacje do jej zdiagnozowania lub usunięcia, Wykonawca wystąpi o uzupełnienie lub skorygowanie informacji podanych w zgłoszeniu. Czas na usunięcie Awarii/Usterki zostanie wówczas zawieszony i nie biegnie dalej aż do chwili udzielenia informacji umożliwiających diagnozę lub usunięcie zgłoszenia danej Awarii/Usterki. Strony dołażą starań, aby treść zgłoszeń zawierała uszczegółowione informację, umożliwi sprawne diagnozowanie zgłaszanych zagadnień.
31. Poprawność realizacji Zgłoszenia będzie potwierdzana poprzez zamknięcie zgłoszenia w ISZ przez Zamawiającego lub Partnera, do którego dane zgłoszenie jest przypisane.
32. W sytuacji gdy dany Zamawiający lub Partner zgłaszający Awarię/Usterkę w Systemie nie potwierdzi poprawności wykonania Usunięcia Awarii lub Usterki przez Wykonawcę w terminie 10 Dni Roboczych tj. nie dokona zamknięcia zgłoszenia, wówczas zgłoszenie zostanie automatycznie uznane jako wykonane poprawnie i zamknięte przez Zamawiającego lub Wykonawcę, z zastrzeżeniem, że Zamawiający lub Partner ma prawo do ponownego zgłoszenia takiego samego błędu.
33. Zamawiający przez okres obowiązywania Umowy udostępni Wykonawcy bezpieczne połączenie do obsługi Systemu, na potrzeby obsługi Awarii/Usterki oraz weryfikacji zgłoszeń dokonywanych przez Zamawiającego lub innych niezbędnych czynności.
34. Uznaje się, że Awaria/Usterka została usunięta w terminie, jeżeli do końca dnia, w którym upływa termin na jej usunięcie w infrastrukturze Zamawiającego lub w innej uzgodnionej lokalizacji wskazanej przez Zamawiającego zostało zaimplementowane rozwiązanie zgłaszanego problemu.
35. Wykonawca jest zobowiązany poinformować Zamawiającego, a w razie instalacji na jego infrastrukturze także Partnera Zamawiającego, zgłaszającego Awarię/Usterkę za pośrednictwem ISZ lub mailowo o planowanych działaniach najpóźniej jeden dzień przed ich realizacją. Przedmiotowe odnosi się również do zapewnienia tymczasowego sposobu postępowania, tzw. Obejścia.
36. Zamawiający zobowiązuje się do współpracy i współdziałania z Wykonawcą w zakresie niezbędnym dla prawidłowego wykonania Umowy.
37. Wykonawca, jako profesjonalny podmiot świadczący tego typu usługi zapewnia, że czynności wykonywane przez jego personel wykonywane będą z należytą starannością zapewniającą bezpieczeństwo danych, odtwarzalność Systemu w przypadku Awarii lub popełnienia błędu serwisowego.
38. Wykonawca zobowiązany będzie do usunięcia wszystkich Awarii/Usterek oraz obsługi wszelkich zgłoszeń Zamawiającego oraz Partnerów w okresie obowiązywania Umowy.
39. Wykonawca zobowiązany jest do monitorowania dostępności Systemu. Poszczególne moduły Systemu pozostają dostępne dla użytkowników na poziomie 97 % w ciągu 12 miesięcy. Maksymalny czas niedostępności Systemu badany jest w okresie referencyjnym kolejnych 6 miesięcy dla którego wartość maksymalna wynosi 1,5%.
40. Świadczenie usługi Serwis technicznego obejmuje wsparcie Systemu zainstalowanego na infrastrukturze wskazanej przez Zamawiającego

Modyfikacje, o których mowa w § 3 pkt 3) i pkt 4) Umowy

Modyfikacje Systemu, a także zlecenia Instruktaży z zakresu funkcjonalności Systemu będą następowały na wniosek Zamawiającego na podstawie odrębnych Zleceń zgodnie z poniższymi wymaganiami:

1. Wykonawca będzie wykonywał usługi Modyfikacji w ramach puli Roboczogodzin określonych w Umowie, przy czym Zamawiający zobowiązany jest zlecić wykonanie prac, o wartości minimalnie 100 Roboczogodzin.
2. Wykonawca wykona usługę Modyfikacji w ramach wynagrodzenia brutto, ustalonego w ramach wyceny zlecenia.
3. Wykonawca zobowiązuje się do wykonywania obowiązków Modyfikacji w sposób zapobiegający utracie danych Zamawiającego.
4. W przypadku, gdy wykonanie czynności z tytułu Modyfikacji wiąże się z ryzykiem utraty danych, Wykonawca zobowiązany jest poinformować o tym Zamawiającego i Partnera przed przystąpieniem do ich wykonywania oraz umożliwić wykonanie kopii zapasowych tych danych.
5. W przypadku niewywiązywania się Wykonawcy z zobowiązań z tytułu Modyfikacji Zamawiający ma prawo skorzystać z usług zastępczych na koszt i ryzyko Wykonawcy bez utraty praw z tytułu związanych z Gwarancją.
6. Modyfikacje będą wykonywane na podstawie pisemnych Zleceń wystawianych przez Zamawiającego, zgodnie z niniejszym paragrafem. Wzór formularza zlecenia stanowi Załącznik nr 8 „Formularz Zlecenia” do Umowy.
7. Jednostką rozliczeniową Zlecenia będzie jedna Roboczogodzina. Maksymalne wynagrodzenie należne Wykonawcy za wykonanie pełnego Zlecenia rozumiane jest jako iloczyn liczby całkowitej Roboczogodzin wskazanych w podpisanym Zleceniu i wynagrodzenia za jedną Roboczogodzinę wskazanego w Umowie.
8. Czas dojazdu do siedziby Zamawiającego lub innego wyznaczonego przez Zamawiającego miejsca realizacji Zlecenia nie jest zaliczany na poczet czasu realizacji Zlecenia.
9. Realizacja Modyfikacji odbywać się będzie na podstawie Zlecenia podpisanego przez upoważnionych przedstawicieli Stron.
10. Przekazanie i przyjmowanie Zleceń będzie odbywało się według następujących zasad:
	1. Zamawiający przekaże Wykonawcy propozycję treści Zlecenia zgodnie z „Formularzem Wstępnego Zlecenia”, którego wzór stanowi Załącznik nr 7 do Umowy , określając w nim temat i zakres Zlecenia oraz termin, miejsce i sposób jego realizacji. Wraz z propozycją Zlecenia Zamawiający przekaże Wykonawcy inne niezbędne dla realizacji Zlecenia informacje, w zakresie w jakim Zamawiający takimi informacjami dysponuje;
	2. w terminie 5 Dni Roboczych od dnia przekazania propozycji Zlecenia Wykonawca przekaże Zamawiającemu analizę zlecenia zgodnie ze wzorem stanowiącym Załącznik nr 8 „ Wzór Formularza Zlecenia ” do Umowy, zawierającą ewentualne uwagi oraz uzupełnienia do treści propozycji Zlecenia, określenie szczegółowego zakresu przedmiotu Zlecenia, oferowany termin realizacji Zlecenia oraz proponowaną maksymalną liczbę Roboczogodzin – w przypadku Modyfikacji Wykonawca przedstawia w ramach analizy zlecenia:
	- szczegółowy zakres prac składających się na Modyfikację wraz z koncepcją rozwiązania oferowanego w wyniku Modyfikacji,

- opis efektu, jaki przyniesie Modyfikacja w Systemie,

- szczegółowy opis zmiany i realizacji przez System danej potrzeby biznesowej, a także informacją o wpływie Modyfikacji na działanie Systemu w części niepodlegającej Modyfikacji;

* 1. zakres, termin oraz maksymalna liczba Roboczogodzin dla danego Zlecenia podlegają uzgodnieniu pomiędzy Stronami;
	2. W wyniku weryfikacji przez Zamawiającego przedstawionej przez Wykonawcę analizy zlecenia, Zamawiający może:
1. zamknąć Zlecenie, o czym poinformuje Wykonawcę,
2. zgłosić uwagi do analizy zlecenia i zobowiązać Wykonawcę do ponownej wyceny prac,
3. zażądać dodatkowych wyjaśnień od Wykonawcy dotyczących przedłożonej analizy zlecenia,
4. negocjować wycenę zakresu prac (liczbę Roboczogodzin),
5. negocjować termin wykonania Zlecenia;
	1. Zamawiający po przeprowadzeniu uzgodnień, zgodnie z pkt. 1) - 4):
6. potwierdzi udzielenie Wykonawcy Zlecenia i podpisze „Formularz Zlecenia”, lub
7. poinformuje Wykonawcę o odstąpieniu od udzielenia Zlecenia;
	1. Zamawiający ma możliwość udzielić Zlecenia w porozumieniu z Wykonawcą bez stosowania procedury określonej w punktach 1) – 4) poprzez podpisanie i przesłanie Wykonawcy Formularza Zlecenia, w szczególności w przypadku Zleceń, dla których przedmiot Zlecenia i Pracochłonność nie będą budzić jakichkolwiek wątpliwości dla obu Stron – w takim przypadku Zamawiający przekazuje Wykonawcy Zlecenie, które jest akceptowane przez Wykonawcę na warunkach określonych w tym Zleceniu poprzez wysłanie Zamawiającemu informacji zwrotnej o przyjęciu Zlecenia do realizacji.
8. Zamawiający zastrzega, iż rozliczeniu będą podlegały jedynie Zlecenia, zrealizowane na warunkach wynikających z ich treści, ustalonej z Zamawiającym.
9. Po wykonaniu Zlecenia Wykonawca przekazuje Zamawiającemu zestawienie prac wykonanych w ramach danego Zlecenia w formie tabelarycznej, z uwzględnieniem w szczególności następujących pozycji: Lp./ID pozycji, Nazwa i opis realizowanych prac, Pracochłonność poszczególnych pozycji i  Pracochłonność całkowita, okres realizacji (daty), miejsce realizacji prac - dokument podpisany elektronicznie lub tradycyjnie.
10. Na wniosek Zamawiającego podstawą odbioru modyfikacji będą testy prowadzone w oparciu o scenariusze testowe lub testy własne, w tym testy swobodne Zamawiającego i Partnerów, przy czym:
11. Testy przeprowadzane będą na infrastrukturze wskazanej przez Zamawiającego, a w przypadku niedostępności infrastruktury Zamawiającego będą realizowane na infrastrukturze Wykonawcy, którą ten zapewni, przy zachowaniu założeń wynikających ze scenariusza testowego. W trakcie realizacji testów na własnej infrastrukturze Wykonawca zobowiązany jest do utrwalenia i udostępnienia wyników testów Zamawiającemu;
12. W terminie co najmniej 5 Dni Roboczych przed wykonaniem danego Zlecenia, Wykonawca, po uzgodnieniach z Zamawiającym opracuje scenariusze testowe wraz z instrukcją przeprowadzenia testów akceptacyjnych, w oparciu o które zostaną przeprowadzone testy akceptacyjne. Zamawiający ma prawo zgłoszenia uwag to testów akceptacyjnych, które Wykonawca zobowiązany jest uwzględnić poprzez aktualizację opracowanych scenariuszy testowych;
13. Zamawiający zastrzega sobie prawo przeprowadzania testów przy udziale podmiotu trzeciego.
14. Prawidłowe zrealizowanie Zlecenia potwierdzone będzie przez Zamawiającego w „Protokole Odbioru Zlecenia” , którego wzór stanowi załącznik nr 9 do Umowy.
15. Jeżeli po podpisaniu Formularza Zlecenia wystąpią okoliczności, które powodują, że konieczna jest zmiana wymagań wskazanych w Zleceniu, Strony podpiszą aneks zmieniający do Zlecenia, uzgodniony przez Strony na warunkach wskazanych w ust. 10.
16. Inicjatywa dotycząca zmiany zakresu prac w ramach Zlecenia następuje ze strony Zamawiającego lub w odpowiedzi na uzasadniony wniosek Wykonawcy.

Dokumentacja

1. Wykonawca jest zobowiązany do wytworzenia i/lub zaktualizowania oraz przekazania Zamawiającemu kompletu dokumentacji wymienionej w ust. 6 niniejszego rozdziału w ramach rozliczenia Etapu I.
2. Wykonawca jest zobowiązany do utrzymania, bieżącego aktualizowania i udostępniania Dokumentacji wytworzonej i/lub aktualizowanej w trakcie realizacji Umowy przez cały okres jej trwania w odniesieniu do wszystkich produktów Przedmiotu Umowy.
3. Wytworzona i zaktualizowana Dokumentacja będzie udostępniana Zamawiającemu i Partnerom w repozytorium dokumentów, stanowiącym część ISZ.
4. Przed rozpoczęciem wykonywania testów Wykonawca przekaże Zamawiającemu aktualny Plan testów zawierający wszystkie informacje niezbędne do przeprowadzenia testów.
5. Po wykonaniu testów Wykonawca przekaże Zamawiającemu Raporty z przeprowadzonych testów.
6. Wykonawca zobowiązuje się przekazać Zamawiającemu następujące nowe lub zmodyfikowane dokumenty /produkty:

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Produkt**  |  |
| 1 | Plan testów | Plan testów obejmuje co najmniej:1) zakres testów,2) scenariusze testowe,3) przypadki testowe,4) procedurę obsługi błędów,5) opis środowiska testowego (konfiguracja środowiska, wykaz niezbędnych zasobów do przeprowadzenia testów),6) harmonogram testów.Scenariusze testowe dla testów akceptacyjnych muszą obejmować swoim zakresem całość Systemu.Zakłada się następujące rodzaje testów:1. testy funkcjonalne,
2. bezpieczeństwa,
3. wydajności,
4. integracji,
5. WCAG,
6. kodów źródłowych.
 |
| 2 | Raporty z przeprowa-dzonych Testów  | Raporty z przeprowadzonych testów obejmują co najmniej:1. zakres testów,
2. wyniki testów,
3. plan działań następczych związany z wynikami testów,
4. Raport z wdrożenia Systemu zawierający opis przeprowadzonego wdrożenia,
 |
| Dokumentacja powykonawcza  |
| 3 | Dokumentacja techniczna | Dokumentacja techniczna w tym: 1. aktualnej Dokumentacji deweloperskiej, w tym m.in.:
	* 1. opis kodu źródłowego systemu,
		2. sposób uruchamiania i kompilacji systemu,
		3. architekturę kodów źródłowych (diagram obrazujący powiązania pomiędzy plikami systemu);
2. procedury i harmonogramu tworzenia backupów;
3. opisu zastosowanej konfiguracji i parametryzacji
4. opisu Architektury Logiczną Systemu;
5. Opisu Konfigurację DNS i sposób udostępnienia usług Partnerom.
6. Procedury i harmonogramu tworzenia backupów;
7. Opisu zastosowanej konfiguracji i parametryzacji.
8. Analizy niezbędnej do wdrożenia rozwiązania infrastruktury IT Zamawiającego i Partnerów;
9. Opisu architektury technologicznej, w tym m.in.:
	* 1. wykaz zastosowanego oprogramowania (w tym nazwę i wersję produktu i producenta; rok produkcji (wydania); ogólny opis funkcjonalności, ze szczególnym uwzględnieniem proponowanej do wykorzystania w Systemach Dziedzinowych; opis powiązań z innymi elementami Oprogramowania Systemowego oraz Oprogramowania; inne istotne informacje dotyczące użytkowania; datę wsparcia w zakresie poprawek bezpieczeństwa dostarczanych przez producenta; zakres licencji i warunki licencyjne),
		2. opis infrastruktury wirtualizacyjnej,
		3. opis fizycznej infrastruktury sprzętowej,
		4. opis wymaganej do infrastruktury sieciowej,
		5. wymagania i wytyczne dotyczące Infrastruktury;
 |
| 4 | Dokumentacja funkcjonalna | Dokumentacja funkcjonalna obejmuje co najmniej:1. Model funkcjonalny (opis usług aplikacyjnych, tj. komponentów systemów informatycznych, realizujących określone funkcjonalności);
2. Analizę niezbędnej do wdrożenia rozwiązania infrastruktury IT Zamawiającego i Partnerów;
3. Katalog aktorów (zawiera m.in. opis aktorów systemu i usług aplikacyjnych z których korzystają aktorzy);
4. Listę i opis modułów systemu;
5. Opis zaproponowanych mechanizmów i ich implementacji zapewniających zgodność z wymaganiami bezpieczeństwa i wydajności oraz zgodność systemu z obowiązującymi przepisami prawa;
6. Opis mechanizmów integrujących;
7. Opis sposobu uwierzytelniania, w tym sposób podziału na Użytkowników i Administratorów oraz monitorowania i dostępu do danych dotyczących uwierzytelniania;
8. Projekty interfejsów Użytkowników (odrębnie dla każdego Aktora) obejmujące co najmniej:
9. opis usług z dostępem bezpośrednim dla Użytkowników poprzez interfejs graficzny;
10. listę elementów interfejsu Użytkownika oraz projekty graficzne poszczególnych elementów interfejsu Użytkownika,
11. opis głównych ścieżek przejść pomiędzy elementami interfejsu Użytkownika, zawierający diagram prezentujący powiązania pomiędzy elementami interfejsu Użytkownika,
12. diagram przepływu pokazujący interakcje pomiędzy poszczególnymi elementami interfejsu Użytkownika.
 |
| 5 | Podręcznik Regionalnego Administratora Systemu | Dokument zawiera minimum.:1. Opis Systemu;
2. Schemat logiczny Systemu;
3. Konfigurację Systemu;
4. Procedury instalacji Systemu;
5. Procedury odinstalowania Systemu;
6. Procedury i harmonogramu tworzenia backupów;
7. Opis zastosowanej konfiguracji i parametryzacji.
 |
| 6 | Podręcznik Lokalnego Administratora Systemu | Dokument zawiera minimum.:1. Opis Systemu;
2. Zasady administrowania poszczególnymi modułami (procedury administracyjne), w tym: procedury włączenia, wyłączenia, aktualizacji, sposobu postępowania w przypadku awarii i pojawiania się błędów w systemie, politykę i procedury wykonywania kopii zapasowych, politykę i procedury monitorowania;
3. Procedura tworzenia backupów;
4. Instrukcja zakładania kont użytkownikom i nadawania uprawnień:
5. sposób monitorowania aktywności,
6. zarządzanie użytkownikami,
7. opis zabezpieczenia przed nieautoryzowanym dostępem i nieautoryzowanym definiowaniem uprawnień,
8. procedury nadawania uprawnień.
 |
| 7 | Podręcznik Użytkownika | Dokument zawiera minimum.:1. informacje o rolach i uprawnieniach nadawanych w Systemie
2. zasady poruszania się w Systemie;
3. opis i graficzną prezentację funkcji Systemu i sposób korzystania z nich;
 |

Normy i standardy

* + - 1. W trakcie wykonywania Przedmiotu Umowy Wykonawca musi kierować się powszechnie obowiązującymi standardami określonymi w normach dotyczących bezpieczeństwa informatycznego, tj. odpowiednio:
1. ISO 27001/ISO 27002 – w odniesieniu do bezpieczeństwa informacji;
2. ISO 27005 – w odniesieniu do zarządzania ryzykiem;
3. ISO 22301 – w odniesieniu do zarządzania ciągłością działania;
4. ISO 20000-1 – w odniesieniu do zarządzania usługami IT.

Przepisy prawa

Wykonawca zobowiązuje się do działania zgodnie z obowiązującymi przepisami prawa, w tym:

* 1. Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j. Dz. U. z 2024 r. poz. 307 ze zm.);
	2. Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (t.j. Dz. U. z 2022 r. poz. 2509);
	3. Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (t.j. Dz. U. 2019 r. poz. 1781);
	4. Ustawa z dnia 5 czerwca 1998 r. o samorządzie województwa (t.j. Dz. U. z 2024 r. poz. 566);
	5. Ustawa z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (t.j. Dz. U. z 2024 r. poz. 572);
	6. Ustawa z dnia 23 kwietnia 1964 r. Kodeks Cywilny (t.j. Dz. U. z 2024 r. poz. 1061, ze zm.);
	7. Ustawa z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych (t.j.: Dz. U. 2023 poz. 1440);
	8. Ustawa z dnia 29 września 1994 r. o rachunkowości (tj. Dz. U. z 2023 r. poz. 120 ze zm.);
	9. Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz. U. z 2024 r. poz. 1077);
	10. Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (t.j. Dz. U. z 2024 r. poz. 422);
	11. Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (t.j. Dz. U. z 2020 r. poz. 344);
	12. Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (t.j. Dz. U. z 2024 r. poz. 34);
	13. Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (t.j. Dz. U. z 2024 r. poz. 632);
	14. Rozporządzenie Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (t.j. Dz. U. z 2024 r., poz. 773);
	15. Rozporządzenie Ministra Cyfryzacji z dnia 10 marca 2020 r. w sprawie szczegółowych warunków organizacyjnych i technicznych, które powinien spełniać system teleinformatyczny służący do uwierzytelniania użytkowników (Dz. U. z 2020 r., poz. 399);
	16. Rozporządzenie Ministra Cyfryzacji z dnia 4 grudnia 2019 r. w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo (Dz. U. z 2019 r. poz. 2479);
	17. 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 (Dz.Urz.UE.L. 119/1 z 04.05.2016);
	18. Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 18 stycznia 2007 r. w sprawie Biuletynu Informacji Publicznej (Dz. U. z 2077 r. nr 10, poz. 68);
	19. Rozporządzenie Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz. U. z 2018 r. poz. 1999).

Załączniki:

Załącznik nr 1 \_ Zasady opracowywania dokumentacji;

Załącznik nr 2\_ Procedura zgłaszania nieprawidłowości w działaniu Systemu;