

OPIS PRZEDMIOTU ZAMÓWIENIA (OPZ)

1. Przedmiot zamówienia:

- 1.1 Przedmiotem zamówienia jest dostawa, wdrożenie oraz utrzymanie systemu IT w modelu chmurowym (SaaS), przeznaczonego do obsługi procesów konkursowych i naboru wniosków przez okres 36 miesięcy od dnia zawarcia umowy, w szczególności:
- a) licencja na Aplikację na okres obowiązywania umowy - dostarczenie licencji, uruchomienie środowiska aplikacyjnego i zapewnienie dostępu dla Zamawiającego nastąpi w terminie do 5 dni roboczych od dnia zawarcia umowy,
 - b) wdrożenie modułów Aplikacji - uruchomienie systemu, konfiguracja startowa, asysta techniczna oraz przeszkolenie personelu Zamawiającego i użytkowników zewnętrznych. Wdrożenie poszczególnych modułów Aplikacji będzie realizowane etapowo (do ustalenia w terminie do 5 dni roboczych od dnia zawarcia umowy), z zastrzeżeniem, że wdrożenie modułu dotyczącego realizacji otwartych konkursów ofert oraz trybu 19a (zakres wynikający z ustawy o działalności pożytku publicznego i o wolontariacie), nastąpi w terminie do 30 dni od daty zawarcia umowy. Wykaz zakresów działania Urzędu planowanych do wdrożenia stanowi załącznik do niniejszego OPZ,
- 1.2 System umożliwi obsługę procesów konkursowych i nabory wniosków realizowanych na podstawie właściwych przepisów prawa, w szczególności:
- a) ustawy o działalności pożytku publicznego i o wolontariacie (w tym trybu 19a, otwartych konkursów ofert oraz naboru członków do komisji konkursowych, oceniających oferty w otwartych konkursach ofert),
 - b) ustawy o zdrowiu publicznym (obejmującej konkursy ofert oraz konkursy wieloletnie),
 - c) uchwał jednostki samorządu terytorialnego, m.in w zakresie programów stypendialnych, programów dotacyjnych, przyznawania nagród indywidualnych/zbiorowych ogłaszanych na podstawie wewnętrznych regulaminów.

2. Opis wymagań systemowych:

- 2.1 Architektura systemu oraz jego główne komponenty
- System winien składać się z modułów wspierających realizację poszczególnych etapów procesu konkursowego:
- 1) ogłaszanie konkursów:
 - a) umożliwienie tworzenia i publikacji nowych naborów wniosków,
 - b) automatyczne przygotowywanie oraz udostępnianie ogłoszeń wraz z dokumentacją konkursową, w oparciu o wcześniej zdefiniowany harmonogram;
 - 2) nabór wniosków:
 - a) zapewnienie elektronicznego składania wniosków przez uprawnione podmioty,

- b) walidacja poprawności i kompletności danych na etapie składania formularzy,
 - c) automatyczne nadawanie unikalnych numerów ewidencyjnych dla zgłoszeń,
 - d) generowanie potwierdzeń złożenia wniosków;
- 3) ocena wniosków:
- a) wsparcie elektronicznej oceny formalnej i merytorycznej wniosków,
 - b) możliwość śledzenia statusu i postępu prac oceniających,
 - c) konfigurowanie kryteriów oceny wraz z możliwością generowania kart i protokołów;
- 4) tworzenie umów:
- a) automatyczne przygotowywanie projektów umów na podstawie danych zawartych we wnioskach,
 - b) obsługa zmian w umowach, w tym aneksów;
- 5) sprawozdawczość:
- a) umożliwienie składania sprawozdań z realizacji zadań,
 - b) obsługa dołączania załączników,
 - c) weryfikacja oraz zatwierdzanie sprawozdań przez przedstawicieli Zamawiającego;
- 6) statystyki - generowanie automatycznych raportów statystycznych, obejmujących m.in. liczbę wniosków, zawartych umów, wysokość przyznanych środków, obszary tematyczne oraz liczbę uczestników działań;
- 7) komunikacja:
- a) wewnętrzny moduł komunikacji obejmujący powiadomienia i wiadomości;
 - b) rejestrowanie historii wymiany informacji pomiędzy wnioskodawcami a Zamawiającym,
 - c) wysyłka powiadomień (systemowych i mailowych) związanych ze zmianami statusu spraw,
 - d) wypełnianie przez wnioskodawców ankiet współpracy zdefiniowanych przez Zamawiającego;
- 8) archiwizacja - zapewnienie bezpiecznego i uporządkowanego przechowywania danych dotyczących konkursów, wniosków, umów oraz sprawozdań, przez cały okres obowiązywania umowy.

2.2 Użytkownicy, role oraz zakres uprawnień

- 1) system winien zapewniać obsługę co najmniej dwóch podstawowych kategorii użytkowników:
- a) użytkownicy zewnętrzni:
 - wnioskodawcy – możliwość zakładania kont i logowania, przygotowywania oraz składania wniosków, przekazywania sprawozdań z realizacji zadań, prowadzenia komunikacji w ramach sprawy, a także dostęp do dokumentów i informacji o statusie procesów,
 - członkowie komisji konkursowych - możliwość zakładania kont i logowania, składanie oświadczeń, podgląd wniosków, przeprowadzanie oceny wniosków;
 - b) użytkownicy wewnętrzni (personel Zamawiającego) – tworzenie i prowadzenie naborów, konfiguracja formularzy oraz reguł walidacyjnych, przeprowadzanie oceny wniosków,

generowanie dokumentów, obsługa sprawozdań, prowadzenie korespondencji, realizacja działań kontrolnych oraz przygotowywanie raportów;

- 2) system winien umożliwiać zarządzanie dostępami użytkowników wewnętrznych w oparciu o model kontroli dostępu opartej na rolach RBAC (Role-Based Access Control), w tym przypisywanie ról oraz definiowanie uprawnień ograniczających dostęp do danych i funkcjonalności zgodnie z zakresem obowiązków użytkownika;

2.3 Wymagania funkcjonalne

1) konta użytkowników i proces rejestracji:

- a) system winien umożliwiać tworzenie kont przez wnioskodawców oraz ich uwierzytelnianie z wykorzystaniem adresu e-mail i hasła,
- b) w trakcie rejestracji system winien zapewniać prezentację oraz akceptację regulaminów, oświadczeń i klauzul informacyjnych związanych z ochroną danych osobowych,
- c) należy zapewnić mechanizmy bezpieczeństwa w obszarze logowania, w szczególności blokowanie konta po określonej liczbie nieudanych prób dostępu oraz opcję wymuszenia zmiany hasła,
- d) system winien rejestrować historię kluczowych zdarzeń związanych z kontem użytkownika, takich jak logowania, zmiany hasła czy aktualizacje danych kontaktowych,
- e) administrator ze strony Zamawiającego winien mieć możliwość zakładania kont dla użytkowników wewnętrznych oraz przypisywania im odpowiednich ról i zakresów uprawnień;

2) nabory:

- a) system winien zapewniać możliwość publikowania ogłoszeń o naborach wraz z pełną dokumentacją (w tym załącznikami) oraz parametrami takimi jak terminy, kryteria oceny, dostępna alokacja środków oraz poziom dofinansowania,
- b) system winien udostępniać narzędzie do konfiguracji naboru (kreator), pozwalające na definiowanie formularzy i ich pól, reguł walidacyjnych oraz przebiegu etapów procesu,
- c) system winien umożliwiać równoległą obsługę wielu naborów oraz ich prezentację z podziałem na aktualny status lub fazę realizacji,
- d) system winien rejestrować historię zmian w konfiguracji naboru, w tym prowadzić dziennik modyfikacji,
- e) system winien umożliwiać tworzenie nowych naborów w oparciu o już istniejące, poprzez kopiowanie ich konfiguracji,
- f) system winien zapewniać możliwość publikowania treści informacyjnych dostępnych po zalogowaniu (m.in. aktualności), zarządzanych przez Zamawiającego,
- g) system winien umożliwiać ograniczenie widoczności naboru i jego udostępnienie wyłącznie wybranym podmiotom poprzez bezpośredni link, o ile Zamawiający przewidzi taki sposób dystrybucji;

3) wnioski:

- a) system winien udostępniać elektroniczny formularz wniosku dostosowany do wymagań Zamawiającego, wyposażony w mechanizmy walidacji danych oraz funkcje automatycznych wyliczeń,

- b) system winien umożliwiać zarówno ręczne zapisywanie postępów pracy, jak i automatyczne zapisywanie wersji roboczych formularza,
- c) system winien uniemożliwiać złożenie wniosku, który nie spełnia zdefiniowanych reguł walidacyjnych,
- d) system winien zapewniać możliwość dołączania załączników do składanych wniosków,
- e) każdy wniosek winien otrzymywać unikalny identyfikator (numer sprawy) oraz sumę kontrolną dokumentu,
- f) system winien prowadzić wersjonowanie wniosków wraz z pełną historią zmian, obejmującą informacje o użytkowniku dokonującym modyfikacji oraz czasie ich wprowadzenia,
- g) system winien umożliwiać stosowanie reguł definiowanych przez Zamawiającego, m.in. ograniczenia liczby składanych wniosków w ramach jednego naboru dla danego podmiotu,
- h) system winien oferować możliwość generowania podglądu oraz wersji do wydruku (m.in. w formatach PDF lub RTF), a także eksportu danych do plików wymiany (m.in. CSV),
- i) system winien umożliwiać wyszukiwanie i filtrowanie wniosków według wybranych kryteriów, takich jak frazy, tytuł, identyfikator czy status;

4) ocena wniosków:

- a) system winien prezentować zestawienia wniosków przypisanych do poszczególnych etapów oceny oraz umożliwiać zarządzanie ich przepływem poprzez odpowiednie statusy,
- b) system winien wspierać proces przypisywania wniosków do oceniających – zarówno w trybie ręcznym, jak i automatycznym (m.in. losowym) - oraz obsługiwać ocenę wieloetapową,
- c) system winien umożliwiać definiowanie kryteriów oceny oraz rejestrowanie odpowiedzi wraz z uzasadnieniami,
- d) system winien zapewniać możliwość zwrócenia wniosku do poprawy (wezwania do uzupełnień), wraz z zapisaniem przyczyny oraz przekazaniem stosownej informacji do wnioskodawcy,
- e) system winien umożliwiać generowanie kart ocen oraz zestawień (m.in. w formatach PDF i CSV), a także – w razie potrzeby – ograniczenie ich widoczności dla wnioskodawcy,
- f) system winien zapewniać funkcjonalność anonimizacji danych ekspertów oceniających (m.in. imię, nazwisko, adres e-mail) w zakresie informacji udostępnianych wnioskodawcom;

5) inna dokumentacja (umowy, aneksy, pisma):

- a) system winien zapewniać możliwość wykorzystania szablonów dokumentów (m.in. umów, decyzji, pism), w tym ich utrzymywania oraz wersjonowania,
- b) system winien umożliwiać automatyczne uzupełnianie dokumentów danymi pochodzącymi z wniosków oraz innych informacji dostępnych w procesie,
- c) system winien oferować możliwość pobierania wygenerowanych dokumentów zarówno w formatach edytowalnych, jak i nieedytowalnych (m.in. RTF oraz PDF),
- d) system winien wspierać proces przygotowania dokumentów do podpisu, w tym zarządzanie statusami na poszczególnych etapach ich opracowania i podpisywania,
- e) system winien obsługiwać proces tworzenia aneksów w sposób analogiczny do obsługi umów, w tym w zakresie generowania dokumentów, wersjonowania, zarządzania statusami oraz archiwizacji,

- f) system winien umożliwiać przygotowywanie dodatkowych dokumentów wymaganych przez Zamawiającego (m.in. zaświadczeń), zgodnie z przekazanymi wzorami oraz obowiązującymi uregulowaniami;
- 6) sprawozdania:
- a) system winien umożliwiać składanie sprawozdań częściowych oraz końcowych w formie elektronicznej, zgodnie z wymaganiami określonymi przez Zamawiającego,
 - b) system winien zapewniać automatyczne pobieranie danych z wniosku i umowy, a także realizację automatycznych obliczeń i walidacji,
 - c) system winien umożliwiać zarówno ręczny zapis postępu pracy, jak i automatyczne zapisywanie wersji roboczych sprawozdań,
 - d) system winien uniemożliwiać złożenie sprawozdania niespełniającego zdefiniowanych reguł walidacyjnych,
 - e) system winien zapewniać możliwość dołączania załączników do sprawozdań,
 - f) system winien obsługiwać statusy sprawozdań oraz umożliwiać wnioskodawcy dostęp do historii złożonych przez niego sprawozdań,
 - g) system winien nadawać sprawozdaniom unikalny identyfikator oraz sumę kontrolną dokumentu;
- 7) korespondencja i powiadomienia:
- a) system winien umożliwiać prowadzenie inicjowanej przez Zamawiającego korespondencji powiązanej z daną sprawą lub wnioskiem oraz zapewniać archiwizację jej historii;
 - b) system winien realizować automatyczną wysyłkę powiadomień (m.in. e-mailowych) informujących o istotnych zdarzeniach oraz zmianach statusu w procesie;
- 8) raportowanie i eksport danych:
- a) system winien zapewniać możliwość tworzenia raportów zarówno w ujęciu zbiorczym, jak i szczegółowym, w oparciu o dane gromadzone w systemie,
 - b) system winien umożliwiać określanie zakresu raportów, w szczególności poprzez wskazanie przedziału czasowego (od–do) oraz stosowanie filtrów według wybranych kryteriów,
 - c) system winien wspierać eksport danych do formatów wymiany (m.in. CSV) na potrzeby analiz, sprawozdawczości oraz działań kontrolnych,
 - d) system winien rejestrować działania użytkowników w sposób umożliwiający odtworzenie pełnej ścieżki audytu, obejmującej co najmniej identyfikator użytkownika lub jego rolę, typ wykonanej operacji, znacznik czasu oraz identyfikator obiektu, którego dotyczyła operacja,
 - e) system winien zapewniać administratorowi Zamawiającego dostęp do dzienników zdarzeń lub możliwość ich udostępnienia w uzgodnionym terminie;
- 9) podpis elektroniczny i weryfikacja podpisu:
- a) system winien umożliwiać dołączanie do spraw dokumentów opatrzonych podpisem elektronicznym,
 - b) system winien zapewniać funkcjonalność weryfikacji poprawności podpisu elektronicznego dla przekazanych plików, w tym kontrolę ważności certyfikatu na moment złożenia podpisu oraz integralności dokumentu;

10) dostępność i kompatybilność:

- a) system musi spełniać wymagania dostępności cyfrowej określone w ustawie z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych oraz być zgodny z wytycznymi WCAG 2.1 na poziomie co najmniej AA,
- b) system winien zapewniać poprawne działanie w aktualnych wersjach najpopularniejszych przeglądarek internetowych (m.in. Chrome, Edge, Firefox, Safari), bez konieczności instalowania dodatkowego oprogramowania lub rozszerzeń;

11) integracje z usługami zewnętrznymi:

- a) system winien umożliwiać integrację z funkcjonującym u Zamawiającego systemem EZD, wykorzystywanym do obsługi obiegu dokumentów, obejmującą co najmniej przekazywanie metadanych spraw,
- b) w przypadku braku możliwości realizacji bezpośredniej integracji, system winien przewidywać alternatywne mechanizmy wymiany danych, w szczególności poprzez eksport i import plików w uzgodnionym formacie, umożliwiające skuteczne przekazywanie informacji pomiędzy systemami.

2.4 Infrastruktura i hosting

Zamawiający dopuszcza realizację rozwiązania w oparciu o infrastrukturę udostępnioną przez Wykonawcę oraz/lub z wykorzystaniem usług chmurowych dostarczanych przez podmioty trzecie. Wykonawca winien stosować rozwiązania technologiczne zapewniające odpowiedni poziom stabilności, wydajności, skalowalności oraz bezpieczeństwa systemu. Zastosowane komponenty infrastrukturalne winny być należycie udokumentowane oraz pochodzić z rozwiązań sprawdzonych i powszechnie wykorzystywanych w środowiskach produkcyjnych IT.

1) odrębna instancja:

- a) system winien być uruchomiony jako dedykowana instancja dla Zamawiającego, zapewniająca separację zasobów oraz konfiguracji, w szczególności poprzez wydzieloną bazę danych, konta użytkowników oraz ustawienia systemowe,
- b) instancja winna umożliwiać samodzielne zarządzanie treściami, szablonami dokumentów, słownikami oraz politykami bezpieczeństwa i uprawnień,
- c) system winien zapewniać możliwość konfiguracji warstwy prezentacyjnej, zarówno w części publicznej, jak i dostępnej po zalogowaniu, w tym w zakresie treści oraz elementów identyfikacji wizualnej właściwych dla Zamawiającego;

2) dostępność usługi i skalowalność:

- a) usługa hostingu winna być dostępna w trybie ciągłym, tj. 24 godziny na dobę, 7 dni w tygodniu,
- b) wymagana miesięczna dostępność systemu winna wynosić co najmniej 99%, z wyłączeniem uprzednio uzgodnionych okien serwisowych,
- c) zastosowana infrastruktura winna gwarantować stabilne działanie również w okresach podwyższonego obciążenia, a system winien być przystosowany do jednoczesnej obsługi minimum 500 użytkowników;

- 3) kopie zapasowe, odtwarzanie i retencja:
 - a) system winien realizować automatyczne wykonywanie kopii zapasowych, przy czym okres ich przechowywania winien obejmować co najmniej kopie codzienne utrzymywane przez minimum 30 dni,
 - b) infrastruktura winna być zaprojektowana zgodnie z zasadą „3-2-1”, tj. uwzględniać co najmniej trzy kopie danych przechowywane na minimum dwóch różnych nośnikach, w tym jedną kopię zlokalizowaną w odrębnym środowisku,
 - c) Wykonawca winien zapewnić procedury pozwalające na odtworzenie danych po awarii oraz możliwość przywrócenia działania systemu;
- 4) ograniczenia geograficzne przetwarzania danych:
 - a) infrastruktura fizyczna oraz lokalizacje przechowywania kopii zapasowych winny być zlokalizowane na obszarze Unii Europejskiej lub państw Europejskiego Obszaru Gospodarczego,
 - b) stosowane procedury techniczne i organizacyjne, w tym związane z zapewnieniem ciągłości działania, nie powinny przewidywać transferu danych Zamawiającego poza obszar Unii Europejskiej lub państw Europejskiego Obszaru Gospodarczego;
- 5) procedura zakończenia świadczenia usługi (Plan Wyjścia):

System musi umożliwiać bezpłatne wyeksportowanie całości danych, (wnioski, umowy, sprawozdania, logi) w formacie otwartym i ustrukturyzowanym (np. w postaci rzutu bazy danych (dump bazy danych), plików JSON (JavaScript Object Notation) lub CSV (Comma-Separated Values), wraz ze słownikiem danych na wypadek zakończenia obowiązywania umowy.
- 6) zgodność z przepisami dotyczącymi dostawców wysokiego ryzyka:
 - a) oferowane w ramach zamówienia produkty ICT, usługi ICT oraz procesy ICT nie mogą być objęte zakazem wprowadzania do użytkowania, o którym mowa w art. 67c ust. 1 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa,
 - b) Wykonawca zobowiązany jest zapewnić, że produkty ICT, usługi ICT oraz procesy ICT objęte przedmiotem zamówienia nie są dostarczane przez dostawcę uznanego za dostawcę wysokiego ryzyka, w zakresie objętym decyzją, o której mowa w art. 67b ust. 15 ustawy o krajowym systemie cyberbezpieczeństwa,
 - c) w przypadku gdy w okresie realizacji zamówienia produkt ICT, usługa ICT lub proces ICT zostanie objęty zakazem, o którym mowa w ust. 1, Wykonawca zobowiązany jest niezwłocznie poinformować o tym Zamawiającego oraz zapewnić rozwiązanie zgodne z obowiązującymi przepisami, umożliwiające dalszą realizację przedmiotu zamówienia.

2.5 Wymagania bezpieczeństwa

- 1) uwierzytelnianie, autoryzacja i kontrola dostępu:
 - a) system winien wykorzystywać bezpieczne mechanizmy uwierzytelniania oraz zarządzania sesją lub tokenami, z uwzględnieniem ochrony ich integralności oraz ograniczonego czasu ważności,
 - b) system winien zapewniać mechanizmy autoryzacji oparte na rolach oraz szczegółowych uprawnieniach, determinujące dostęp użytkowników do danych i dostępnych operacji,
 - c) system winien umożliwiać zastosowanie uwierzytelniania wieloskładnikowego,

- d) system winien zawierać mechanizmy zabezpieczające przed atakami typu brute force, takie jak ograniczanie liczby prób logowania, czasowe blokady kont oraz rejestrowanie zdarzeń związanych z próbami dostępu,
 - e) system winien umożliwiać definiowanie i egzekwowanie polityki haseł zgodnej z wymaganiami Zamawiającego, w tym konfigurację parametrów dotyczących długości hasła (minimalnej i maksymalnej) oraz wymagań dotyczących jego złożoności (m.in. użycie małych i wielkich liter, cyfr oraz znaków specjalnych);
- 2) ochrona przed typowymi atakami na aplikacje webowe:
- a) system winien zapewniać zabezpieczenia przed najczęściej występującymi podatnościami aplikacji webowych, w szczególności w obszarach takich jak kontrola dostępu, podatności typu injection, XSS, nieprawidłowa konfiguracja bezpieczeństwa oraz wykorzystanie nieaktualnych komponentów,
 - b) system winien stosować walidację danych wejściowych oraz wykorzystywać bezpieczne mechanizmy komunikacji z bazą danych zgodne z dobrymi praktykami,
 - c) system winien ograniczać ryzyko ataków typu CSRF poprzez zastosowanie odpowiednich mechanizmów ochrony żądań, takich jak tokeny anty-CSRF, a także właściwie zaprojektowany model uwierzytelniania,
 - d) infrastruktura winna być zabezpieczona poprzez mechanizmy filtrowania ruchu oraz rozwiązania ograniczające skutki ataków typu DDoS, a także zaporę sieciową (firewall) działającą zgodnie z zasadą minimalnych uprawnień dostępu;
- 3) szyfrowanie i ochrona danych:
- a) komunikacja pomiędzy użytkownikiem a systemem winna być realizowana z wykorzystaniem protokołu HTTPS, przy zastosowaniu aktualnych wersji TLS (co najmniej TLS 1.2),
 - b) hasła użytkowników winny być przechowywane w postaci nieodwracalnych skrótów (hash), z użyciem aktualnych, bezpiecznych algorytmów oraz odpowiednio dobranych parametrów zwiększających odporność na ataki,
 - c) dane przechowywane w systemie winny być zabezpieczone poprzez szyfrowanie na poziomie bazy danych i/lub warstwy dyskowej, adekwatnie do przyjętej architektury oraz modelu utrzymania,
 - d) system winien zapewniać logiczną separację danych pomiędzy użytkownikami oraz prowadzonymi sprawami, zgodnie z przypisanymi uprawnieniami dostępu;
- 4) aktualizacje i zarządzanie podatnościami:
- a) Wykonawca winien zapewniać regularne aktualizowanie komponentów systemu oraz infrastruktury w celu ograniczania ryzyka wynikającego ze znanych podatności,
 - b) Wykonawca winien stosować uporządkowany proces zarządzania podatnościami, obejmujący ich identyfikację, ocenę poziomu ryzyka oraz podejmowanie działań naprawczych.

3. Przeszkolenie z wdrażanych modułów aplikacji

- 1) Wykonawca winien zapewnić przeprowadzenie co najmniej dwóch szkoleń przy wdrażaniu poszczególnych modułów aplikacji dla pracowników Zamawiającego odpowiedzialnych za obsługę systemu.

Szkolenie winno obejmować w szczególności:

- a) obsługę procesów realizowanych w systemie,
- b) korzystanie z kluczowych funkcjonalności,
- c) podstawowe czynności administracyjne i konfiguracyjne,
- d) obsługę sytuacji typowych oraz najczęstszych problemów;

Szkolenia winny zostać przeprowadzone w formie uzgodnionej z Zamawiającym (zdalnej lub stacjonarnej). Wykonawca winien przekazać materiały szkoleniowe w formie elektronicznej;

- 2) Wykonawca winien zapewnić przeprowadzenie co najmniej dwóch szkoleń (zdalnie lub stacjonarnie) dla użytkowników zewnętrznych przed uruchomieniem produkcyjnym systemu oraz na żądanie Zamawiającego po wdrożeniu nowych funkcjonalności lub modułów. Ponadto Wykonawca zapewni przygotowanie materiałów szkoleniowych (instrukcje użytkownika) w formie elektronicznej dla użytkowników zewnętrznych do każdego z wdrażanych modułów aplikacji.

4. Usługa utrzymania i wsparcia

Wykonawca w trakcie obowiązywania umowy, zobowiązany jest do wykonywania prac związanych z bieżącym funkcjonowaniem oraz utrzymaniem systemu. Wykonawca winien zapewnić ciągłość działania rozwiązania, w szczególności poprzez bieżące usuwanie awarii i usterek oraz świadczenie wsparcia dla użytkowników po stronie Zamawiającego.

- 1) zakres usługi:

- a) analiza zgłoszeń obejmująca ich przyjmowanie, rejestrowanie oraz klasyfikację wraz z nadawaniem odpowiednich priorytetów,
- b) usuwanie błędów oraz implementacja poprawek – zarówno w ramach planowanych wydań, jak i w trybie pilnym w przypadku incydentów o charakterze krytycznym,
- c) zapewnienie rozwiązań tymczasowych (obejść) w sytuacjach, gdy natychmiastowe usunięcie problemu nie jest możliwe,
- d) świadczenie wsparcia technicznego (helpdesk) w uzgodnionych godzinach dostępności oraz bieżąca współpraca i koordynacja działań z Zamawiającym,
- e) udzielanie wsparcia w zakresie awaryjnego odtwarzania systemu oraz danych – na żądanie Zamawiającego,
- f) monitorowanie środowiska oraz instalacja krytycznych aktualizacji bezpieczeństwa;

- 2) testowanie i wdrażanie zmian:

- a) Wykonawca winien przeprowadzać testy wszystkich wprowadzanych modyfikacji (zarówno funkcjonalnych, jak i konfiguracyjnych) przed ich wdrożeniem do środowiska produkcyjnego,
- b) Wykonawca winien zapewnić przeprowadzanie testów przez co najmniej 1 osobę posiadającą co najmniej roczne doświadczenie w realizacji testów systemów informatycznych, w zakresie dotyczącym realizacji otwartych konkursów ofert oraz trybu 19a (zakres wynikający z ustawy o działalności pożytku publicznego i o wolontariacie),

- c) Wykonawca winien utrzymywać środowisko testowe umożliwiające weryfikację przygotowanych rozwiązań oraz przekazywać Zamawiającemu informacje o rezultatach przeprowadzonych testów,
 - d) Wdrożenia zmian na środowisko produkcyjne winny być realizowane w uprzednio uzgodnionych terminach, po uzyskaniu akceptacji Zamawiającego, o ile jest ona wymagana;
- 3) dokumentacja:
- a) dokumentacja tworzona oraz aktualizowana w trakcie realizacji umowy musi być sporządzana w języku polskim i przekazywana w formie elektronicznej (w formatach DOCX i/lub PDF),
 - b) dokumentacja winna zawierać tytuł, wykaz elementów składowych oraz ogólny opis zawartości,
 - c) Wykonawca winien na bieżąco aktualizować dokumentację w przypadku wprowadzania zmian odnoszących się do opisanych w niej obszarów,
 - d) na wniosek Zamawiającego Wykonawca winien przekazywać opis zrealizowanych prac w ramach obsługi zgłoszeń, wraz z informacją o sposobie rozwiązania danego problemu;
- 4) godziny gotowości i czasy reakcji:
- a) wsparcie systemu winno być realizowane zdalnie w dni robocze, tj. od poniedziałku do piątku, z wyłączeniem dni ustawowo wolnych od pracy, w godzinach od 8:00 do 16:00,
 - b) zgłoszenia winny być klasyfikowane według poziomu priorytetu, od którego uzależniony jest maksymalny czas przywrócenia podstawowej funkcjonalności systemu:
 - w przypadku incydentów o charakterze krytycznym, rozumianych jako awarie uniemożliwiające korzystanie z systemu lub realizację jego kluczowych funkcji (m.in. brak możliwości składania wniosków, brak dostępu do istotnych danych lub naruszenie spójności danych), przywrócenie podstawowej funkcjonalności winno nastąpić w czasie nie dłuższym niż 8 godzin roboczych od momentu zgłoszenia, w ramach godzin gotowości,
 - w przypadku zgłoszeń o charakterze zwykłym, dotyczących nieprawidłowości utrudniających korzystanie z systemu, ale nieblokujących jego podstawowych funkcji, czas przywrócenia podstawowej funkcjonalności nie powinien przekraczać 24 godzin roboczych od momentu zgłoszenia, również w ramach godzin gotowości,
 - c) niezależnie od priorytetów technicznych, Wykonawca zobowiązany jest do wydzielenia kategorii „Incydent Cyberbezpieczeństwa”, rozumianego jako zdarzenie mające niepożądany wpływ na bezpieczeństwo sieci i systemów informatycznych lub przetwarzanych w nich danych (w tym incydenty związane z poufnością, integralnością lub dostępnością danych)
 - Wykonawca ma obowiązek powiadomić Zamawiającego o wykryciu lub uzasadnionym podejrzeniu wystąpienia Incydentu Cyberbezpieczeństwa w czasie nie dłuższym niż 2 godziny od momentu jego wykrycia (7 dni w tygodniu, 24 godziny na dobę), w celu umożliwienia Zamawiającemu realizacji obowiązków sprawozdawczych wynikających z ustawy o Krajowym Systemie Cyberbezpieczeństwa (KSC),
 - czas podjęcia działań naprawczych przez Wykonawcę (mitygacja ryzyka lub usunięcie podatności) w przypadku Incydentu Cyberbezpieczeństwa wynosi maksymalnie 4 godziny od momentu wykrycia lub zgłoszenia.

5. Łańcuch dostaw

Oferowane rozwiązanie chmurowe oraz proces jego utrzymania nie mogą wykorzystywać komponentów, usług ani procesów ICT pochodzących od dostawców uznanych za dostawców wysokiego ryzyka w rozumieniu przepisów o Krajowym Systemie Cyberbezpieczeństwa. Wymagany jest ciągły monitoring podatności komponentów (w tym Open Source) i ich łatanie (podatności krytyczne do 72h od wydania poprawki). Zamawiający zastrzega możliwość weryfikacji struktury oprogramowania poprzez żądanie wykazu SBOM - Software Bill of Materials (wykaz składników oprogramowania).

6. Zgodność z przepisami i wytycznymi

Zarówno system, jak i proces jego wytwarzania oraz utrzymania winny być zgodne z obowiązującymi przepisami prawa oraz właściwymi wytycznymi, w szczególności w zakresie:

- a) ustawy z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych (Dz. U. z 2023 r., poz. 1440),
- b) Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 (RODO) oraz krajowych regulacji dotyczących ochrony danych osobowych,
- c) ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (w zakresie mającym zastosowanie) (Dz. U. z 2026 r., poz. 20, 252),
- d) przepisów określających minimalne wymagania dla systemów teleinformatycznych w administracji publicznej, w tym Krajowych Ram Interoperacyjności,
- e) innych przepisów prawa oraz regulacji mających wpływ na realizację umowy.

Wszystkie wymagania określone w niniejszym Opisie Przedmiotu Zamówienia stanowią minimalne wymagania jakościowe odnoszące się do głównych elementów przedmiotu zamówienia. Oferowany system musi spełniać wszystkie wymagania określone w OPZ.

Wykaz zakresów działania UMWO planowanych do wdrożenia

Lp.	Zakres (obszar) działania	Podstawa prawna	Termin wdrożenia
1.	Otwarte konkursy ofert, tryb 19a (małe granty)	Ustawa z dnia 24 kwietnia 2003 r. o działalności pożytku publicznego i o wolontariacie	do 30 dni od dnia zawarcia umowy
2.	Nabór członków do komisji konkursowych - zgłoszenia przedstawicieli NGO jako kandydatów do komisji konkursowych oceniających oferty w otwartych konkursach ofert	Ustawa z dnia 24 kwietnia 2003 r. o działalności pożytku publicznego i o wolontariacie	
3.	Konkursy ofert	Ustawa o zdrowiu publicznym	
4.	Stypendia Marszałka Województwa Opolskiego dla osób zajmujących się twórczością artystyczną, upowszechnianiem kultury oraz opieką nad zabytkami - „Marszałkowskie Talenty”	Wewnętrzne regulacje prawne (uchwała jst)	
5.	Stypendia sportowe dla zawodników za osiągnięte wyniki sportowe	Wewnętrzne regulacje prawne (uchwała jst)	
6.	Marszałkowski Program Stypendialny dla uczniów szkół i placówek kształcenia ogólnego	Wewnętrzne regulacje prawne (uchwała jst)	
7.	Stypendia w dziedzinie zdrowia dla studentów kierunku lekarskiego	Wewnętrzne regulacje prawne (uchwała jst)	
8.	Program dotacyjny - Marszałkowska Inicjatywa Sołecka	Wewnętrzne regulacje prawne (uchwała jst)	
9.	Program dotacyjny - Program rozwoju infrastruktury sportowej w województwie opolskim	Wewnętrzne regulacje prawne (uchwała jst)	
10.	Dotacje celowe na prace konserwatorskie, restauratorskie lub roboty budowlane przy zabytkach wpisanych do rejestru zabytków lub znajdujących się w gminnych ewidencjach zabytków, znajdujących się na obszarze województwa opolskiego (na podstawie ustawy z dnia 23 lipca 2003 r. o ochronie zabytków i opiece nad zabytkami)	Wewnętrzne regulacje prawne (uchwała jst)	

11.	Konkurs "Opolska Niezapominajka"	Wewnętrzne regulacje prawne (uchwała jst)	
12.	Konkurs "Lew Opolskiej Turystyki"	Wewnętrzne regulacje prawne (uchwała jst)	
13.	Konkurs „Fundusz Sołecki -najlepsza inicjatywa"	Wewnętrzne regulacje prawne (uchwała jst)	
14.	Konkurs „Piękna Wieś Opolska"	Wewnętrzne regulacje prawne (uchwała jst)	
15.	Wojewódzki Konkurs Koron Dożynkowych	Wewnętrzne regulacje prawne (uchwała jst)	
16.	Nabór wniosków o przyznanie Nagród Marszałka Województwa Opolskiego dla Animatorów i Twórców Kultury	Wewnętrzne regulacje prawne (uchwała jst)	
17.	Nabór wniosków o przyznanie Nagród im. Karola Miarki	Wewnętrzne regulacje prawne (uchwała jst)	
18.	Nabór wniosków o przyznanie Nagród Marszałka Województwa Opolskiego za Wydarzenie Muzealne	Wewnętrzne regulacje prawne (uchwała jst)	
19.	Nabór wniosków o przyznanie Nagrody Marszałka Województwa Opolskiego „Zabytek na Medal"	Wewnętrzne regulacje prawne (uchwała jst)	
20.	Nabór wniosków o przyznanie nagród Marszałka Województwa Opolskiego w dziedzinie nauki, tj. Professor Opoliensis oraz Doctor Opoliensis	Wewnętrzne regulacje prawne (uchwała jst)	
21.	Nabór wniosków o przyznanie nagród Marszałka Województwa Opolskiego za szczególne osiągnięcia w dziedzinie upowszechniania i rozwoju edukacji	Wewnętrzne regulacje prawne (uchwała jst)	
22.	Nabór wniosków o przyznanie nagród Marszałka Województwa Opolskiego "Prymus Opolszczyzny" w kategorii wiedza i sztuka	Wewnętrzne regulacje prawne (uchwała jst)	
23.	Nabór wniosków o przyznanie nagrody Marszałka Województwa Opolskiego w dziedzinie sportu	Wewnętrzne regulacje prawne (uchwała jst)	