*Załącznik nr 1 do SIWZ*

*Załącznik nr 1 do Umowy nr CSIOZ/…./2020*

**Opis przedmiotu zamówienia**

***Przedmiotem zamówienia jest usługa Integracji Systemu e-PLOZ z Węzłem Krajowym na potrzeby zapewnienia weryfikacji i identyfikacji użytkowników w systemach i rejestrach Zamawiającego za pośrednictwem Systemu e-PLOZ.***

1. **Przedmiot zamówienia**

W ramach realizacji przedmiotu zamówienia, Wykonawca zrealizuje Integrację Systemu e-PLOZ z systemem Węzła Krajowego, gdzie System e-PLOZ będzie występował w roli Dostawcy Usługi (zgodnie z dokumentacją Węzła Krajowego umieszczoną w Biuletynie Informacji Publicznej Ministerstwa Cyfryzacji pod adresem <https://mc.bip.gov.pl/wezel-krajowy/wezel-krajowy-dokumentacja-dotyczaca-integracji-z-wezlem-krajowym.html>).

System „Elektroniczna platforma logowania ochrony zdrowia” (e-PLOZ) jest systemem odpowiadającym za proces autentykacji, autoryzacji i uwierzytelnienia dla systemów i rejestrów medycznych obsługiwanych w CSIOZ. Zbudowany jest w oparciu o Keycloak w wersji 8.0.1, którego kod został zmodyfikowany na potrzeby projektu, zainstalowany na systemie operacyjnym CentOS 8. Baza danych użyta dla e-PLOZ to PostgreSQL ver 10.10. System e-PLOZ będzie umożliwiał zalogowanie za pomocą Węzła Krajowego.

1. **Definicje**

|  |  |
| --- | --- |
| **Pojęcie** | **Definicja** |
| Dokumentacja | wszelka dokumentacja dotycząca rezultatów prac Wykonawcy, która powstanie w ramach realizacji Umowy. Dokumentacja obejmuje w szczególności: dokumentację przeznaczoną dla administratora, dokumentację techniczną, dokumentację użytkową (podręcznik użytkownika) |
| eIDAS | Rozporządzenie Parlamentu Europejskiego i Rady (UE) Nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE |
| System e-PLOZ lub System | Elektroniczna platforma logowania ochrony zdrowia – system autoryzacyjny dla systemów i rejestrów medycznych obsługiwanych w CSIOZ, realizowany przez oprogramowanie Keycloak |
| Integracja | proces skutkujący zespoleniem Systemu e-PLOZ z WK, w celu uwierzytelniania użytkowników systemów CSIOZ  |
| Kod źródłowy | zestaw plików zawierających nieskompilowany kod oprogramowania napisany w języku programowania, wynikający z przyjętej technologii rozwiązania oraz w formie czytelnej dla człowieka, normalnie używanej dla umożliwienia wprowadzania modyfikacji (w tym również komentarze oraz kody proceduralne, takie jak skrypty w języku opisu prac i skrypty do sterowania kompilacją i instalowaniem), jak również dokumentacja niezbędna do użycia takiego Kodu Źródłowego |
| Naprawa | trwałe przywrócenie w pełni prawidłowego funkcjonowania Systemu lub jego elementu, poprzez, między innymi: 1. usunięcie Błędu,
2. doprowadzenie do działania Systemu zgodnie z Dokumentacją lub innymi uzgodnieniami pomiędzy Stronami
 |
| Oprogramowanie open source | oprogramowanie komputerowe dystrybuowane na warunkach tzw. licencji otwartych, tj. zgodnie z definicją wskazaną pod adresem internetowym: <https://opensource.org/faq#osd> |
| Repozytorium Zamawiającego/Repozytorium GitHub | narzędzie informatyczne przeznaczone do przechowywania Kodu Źródłowego wskazane przez Zamawiającego, w tym konkretnym przypadku jest to [hostingowy](https://pl.wikipedia.org/wiki/Hosting) [serwis internetowy](https://pl.wikipedia.org/wiki/Serwis_internetowy) przeznaczony dla projektów [programistycznych](https://pl.wikipedia.org/wiki/Programowanie_komputer%C3%B3w) wykorzystujących [system kontroli wersji](https://pl.wikipedia.org/wiki/System_kontroli_wersji) [Git](https://pl.wikipedia.org/wiki/Git_%28oprogramowanie%29) |
| Symulator Ministerstwa Cyfryzacji lub Środowisko Integracyjnie  Ministerstwa Cyfryzacji | infrastruktura sprzętowo-systemowa, będąca własnością Skarbu Państwa Ministra Cyfryzacji, przeznaczona do realizacji określonych prac w ramach zamówienia. |
| Węzeł Krajowy lub WK lub login.gov.pl | rozwiązanie organizacyjno-techniczne, które zapewnia funkcjonowanie krajowego schematu identyfikacji elektronicznej oraz stanowi punkt przyłączenia akredytowanych systemów identyfikacji elektronicznej (DT) Węzeł krajowy umożliwia uwierzytelnienie w celu realizacji usług online z wykorzystaniem środka identyfikacji elektronicznej wydanego w ramach akredytowanego systemu identyfikacji elektronicznej. Węzeł Krajowy o którym mowa w ustawie z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz.U. z 2019 r. poz.162)  |
| Zgłoszenie | informacja Zamawiającego o wystąpieniu w Systemie e-PLOZ Błędu zgodna z opisem przewidzianym w umowie |
| CSIOZ | Centrum Systemów Informacyjnych Zdrowia, zwane Zamawiającym lub Stroną |
| Błąd | funkcjonowanie Integracji niezgodne z opisem w Dokumentacji, które powoduje zatrzymanie lub spowolnienie pracy Systemu e-PLOZ, wprowadza niespójność w bazie danych lub zaburzenia w integralności danych |
| Dzień roboczy | od poniedziałku do piątku z wyłączeniem dni ustawowo wolnych od pracy oraz dni wolnych u Zamawiającego, w godzinach od 8:00 do 17:00 |

1. **Zakres prac i warunki realizacji**
2. **Etap I - Integracja Systemu e-PLOZ z systemem Węzła Krajowego:**
	1. W ciągu 3 Dni Roboczych od daty podpisania umowy, Strony uzgodnią szczegółowy harmonogram realizacji etapu, przy czym termin jego realizacji wynosi zgodnie ze złożoną ofertą, nie krócej niż 20 dni roboczych lecz nie dłużej niż 43 dni roboczych od dnia podpisania umowy.
	2. W ciągu jednego Dnia Roboczego od podpisania umowy Wykonawca przekaże Zamawiającemu listę osób ze strony Wykonawcy realizujących zamówienie, dla których Zmawiający założy konta w środowiskach Systemu e-PLOZ.
	3. Zadaniem Wykonawcy będzie przeprowadzenie skutecznej Integracji Systemu e-PLOZ ze środowiskiem integracyjnym Węzła Krajowego, w szczególności:
		1. Budowa dostawcy tożsamości w Systemie e-PLOZ (Identity Provider) obsługującego integrację z Węzłem Krajowym. Przygotowane rozwiązanie musi obsługiwać w szczególności:
	4. Obsługę szyfrowania komunikatów do/z Węzła Krajowego zgodnie ze specyfikacją Węzła Krajowego;
	5. Zarządzanie certyfikatami klienta Węzła Krajowego z poziomu panelu administratora Systemu e-PLOZ;
	6. Wsparcie dla eIDAS SAML Attribute Profile;
	7. Mapowanie atrybutów eIDAS do profilu użytkownika Systemu e-PLOZ;
	8. Obsługa wylogowania (Single Logout Service) za pomocą SOAP binding (tzw. Back-channel logout);
	9. Pozostałe wymagania zgodne z dokumentem „Instrukcja integratora Dostawcy Usług (DU)” ze strony bip: <https://mc.bip.gov.pl/wezel-krajowy/wezel-krajowy-dokumentacja-dotyczaca-integracji-z-wezlem-krajowym.html>;
	10. Dodanie obsługi błędów zwracanych przez system Węzła Krajowego w postaci zrozumiałej dla użytkownika końcowego oraz administratora Systemu e-PLOZ (system powinien mapować kody błędów na komunikaty dla użytkownika).
		1. Przeprowadzenie testów rozwiązania zgodnie z treścią instrukcji: <https://mc.bip.gov.pl/wezel-krajowy/wezel-krajowy-dokumentacja-dotyczaca-integracji-z-wezlem-krajowym.html>, w szczególności:
3. Uruchomienie Integracji Systemu e-PLOZ na środowisku testowym CSIOZ z użyciem środowiska Symulatora Ministerstwa Cyfryzacji;
4. Uruchomienie Integracji Systemu e-PLOZ na środowisku testowym CSIOZ z użyciem Środowiska Integracyjnego Ministerstwa Cyfryzacji;
5. Testy każdego z etapów uruchomienia Integracji Systemu e-PLOZ (Środowisko Symulatora Ministerstwa Cyfryzacji, Środowisko Integracyjne Ministerstwa Cyfryzacji) kończyć będą się dostarczeniem przez Wykonawcę raportu z testów, realizowanych wg scenariuszy testowych dostarczonych przez Centralny Ośrodek Informatyki lub Zamawiającego;
6. Zamawiający zastrzega sobie prawo do przeprowadzenia na każdym etapie wdrożenia testów swoim zespołem w zakresie określonym scenariuszami testowymi dostarczonymi przez Centralny Ośrodek Informatyki lub Zamawiającego;
	* 1. Przeprowadzenie niezależnego audytu bezpieczeństwa kodu źródłowego użytego do integracji oraz testów bezpieczeństwa. Aplikacja powinna być przetestowana w oparciu o standardy OWASP (Open Web Application Security Project), a w szczególności o klasyfikację OWASP Top 10, OWASP ASVS (Application Security Verification Standard) oraz OWASP Testing Guide 4.0 (zawierający najlepsze praktyki w zakresie testów bezpieczeństwa). Przeprowadzone testy zostaną potwierdzone raportem składającym się z podsumowania oraz szczegółowego opisu wykrytych podatności oraz sposobów ich wyeliminowania. Wszystkie wykryte podatności zostaną usunięte przez Wykonawcę w terminie realizacji Etapu I i potwierdzone nowym raportem z testów. Zadanie zostanie przeprowadzone przez podmiot niezależny od Wykonawcy na jego koszt. Przynajmniej jeden członek zespołu wskazany przez Wykonawcę musi wykazać się posiadaniem certyfikatu poświadczającego umiejętności prowadzenia audytów i testów bezpieczeństwa: OCSP lub CEH[[1]](#footnote-1) lub CISSP[[2]](#footnote-2) lub równoważne.
		2. Dostarczenie zbudowanych elementów instalacyjnych (paczek) oraz umieszczenie kodu źródłowego, paczek oraz konfiguracji Systemu e-PLOZ w repozytorium GitHub znajdującym się w ramach organizacji CSIOZ.
		3. Dostarczenie przygotowanej dokumentacji wdrożeniowej w zakresie opisu Integracji wraz z pełną dokumentacją techniczną rozwiązania, dokumentacją administratora, a także dokumentacją użytkową (jeśli będzie wymagana).
		4. Dostarczenie instrukcji instalacji paczek instalacyjnych oraz instrukcji ich budowania.
	1. Wymagania niefunkcjonalne wobec rozwiązania dostarczanego przez Wykonawcę:
		1. Rekonfiguracja integracji nie wymaga przerwania pracy Systemu e-PLOZ;
		2. Rozwiązanie dostarczane przez Wykonawcę ma umożliwić Systemowi e-PLOZ zapisywanie faktu wysłania i odebrania każdego komunikatu (wywołania usługi) w ramach komunikacji Systemu e-PLOZ z WK oraz zapewnić uprawnionemu użytkownikowi prezentację zapisanych informacji;
		3. Forma prezentacji informacji, o których mowa w pkt 1.4.2, powinna zapewniać, że  wszystkie komunikaty i błędy generowane w trakcie komunikacji z WK (np. błędy pobrań, wysyłki komunikatów) będą zrozumiałe dla administratorów Zamawiającego;
		4. Rozwiązanie wytworzone przez Wykonawcę w Systemie e-PLOZ powinno wykorzystywać interfejsy komunikacyjne zdefiniowane w WK;
		5. W ramach komunikacji Systemu e-PLOZ z WK, System e-PLOZ pełni rolę klienta;
		6. Wszystkie połączenia pomiędzy Systemem e-PLOZ-em a WK muszą być szyfrowane;
		7. Rozwiązanie musi wykorzystywać szyfrowanie podczas komunikacji pomiędzy wszystkimi komponentami. Szyfrowanie musi być zrealizowane w oparciu o rozwiązania zapewniające poziom bezpieczeństwa co najmniej równy temu jaki zapewniają protokoły SSL/TLS lub VPN;
		8. Rozwiązanie musi spełniać wymogi krajowych i unijnych przepisów w zakresie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych;
		9. Wszystkie komponenty (z wyjątkiem skryptów, plików edytowalnych) muszą być podpisane zaufanym certyfikatem;
		10. System e-PLOZ musi obsłużyć co najmniej 100 jednoczesnych logowań w czasie nie dłuższym niż 2 sekundy, liczone od momentu wysłania żądania autoryzacji do WK do momentu przetworzenia przez e-PLOZ odpowiedzi z WK na wysłane żądanie, bez wliczania w to czasu przetwarzania żądania przez WK;
		11. Na potrzeby Integracji Wykonawca bez zgody Zamawiającego nie może wykonywać ani proponować zmian w kodzie źródłowym (core) oprogramowania Keycloak;
		12. Zamawiający dopuszcza możliwość podniesienia wersji Keycloak do wersji wyższej niż obecnie użytkowana przez Zamawiającego, ale każdorazowo za zgodą Zamawiającego. Powyższe nie może mieć wpływu na wysokość wynagrodzenia Wykonawcy oraz na uzgodniony harmonogram.
	2. W ramach realizacji Etapu I Wykonawca przeprowadzi dla nie więcej niż 4 osób, w miejscu wskazanym przez Zamawiającego, dwudniowe warsztaty (16 godzin roboczych), których celem jest przedstawienie przygotowanego w ramach Zamówienia rozwiązania technicznego, aspektów dotyczących administracji tym rozwiązaniem oraz możliwości jego skalowania. Co najmniej 2 dni robocze przed warsztatami Wykonawca dostarczy Zamawiającemu wszelkie materiały, prezentacje, przykładowe skrypty, dla osób korzystających z rozwiązania z zakresu dostarczonego rozwiązania.
	3. Wykonawca do uruchomienia Integracji nie może się posłużyć oprogramowaniem objętym komercyjną licencją Wykonawcy lub podmiotów trzecich. W przypadku wykorzystania oprogramowania typu Opensource stosuje się zapisy pkt. 4.4.
	4. Zamawiający zastrzega sobie prawo do realizacji testów wydajnościowych oraz testów bezpieczeństwa w trakcie trwania Etapu I, własnym zespołem lub zlecając je podmiotowi zewnętrznemu. W przypadku wystąpienia nieprawidłowości, Wykonawca zobowiązany jest do ich usunięcia.
	5. Na zakończenie etapu, Strony podpiszą Protokół odbioru Etapu I, przy założeniu spełnienia następujących warunków :
		1. Pozytywna decyzja Ministerstwa Cyfryzacji o przejściu testów integracyjnych i podłączeniu Systemu e-PLOZ do Węzła Krajowego na środowisku produkcyjnym;
		2. Przekazanie Zamawiającemu kompletu kodów źródłowych oraz pozostałych komponentów jak biblioteki itd. niezbędnych do prawidłowego działania rozwiązania,
		3. Przekazanie Zamawiającemu Dokumentacji składającej się z pełnej dokumentacji technicznej rozwiązania, dokumentacji użytkownika, dokumentacji administratora;
		4. Przekazanie zaakceptowanych przez Zamawiającego raportów z audytu bezpieczeństwa kodu oraz testów bezpieczeństwa rozwiązania;
		5. Skuteczne uruchomienie przez Zamawiającego Integracji środowiska produkcyjnego Systemu e-PLOZ z środowiskiem produkcyjnym WK zakończone potwierdzeniem przez Ministerstwo Cyfryzacji lub Centralny Ośrodek Informatyki o pozytywnym przejściu testów zgodnie z Instrukcją integratora Dostawcy Usług dostępną na Biuletynie Informacji Publicznej Ministerstwa Cyfryzacji;
		6. Przekazaniu Zamawiającemu wykazu wszystkich licencji oprogramowania typu Opensource użytych do realizacji Etapu I.
	6. W ramach odbioru Etapu I:
		1. Strony uzgodnią wersję oprogramowania, która zostanie wgrana na środowisko produkcyjne e-PLOZ lub środowisko zintegrowane z e-PLOZ;
		2. Zamawiający jest odpowiedzialny za zapewnienie dostępów do środowiska odbiorczego (Symulator Ministerstwa Cyfryzacji, Środowisko Integracyjne Ministerstwa Cyfryzacji );
		3. Zamawiający w ciągu jednego Dnia Roboczego od otrzymania paczek instalacyjnych przystąpi do samodzielnej instalacji paczek na środowisku produkcyjnym Zamawiającego na podstawie Instrukcji instalacji dostarczonej przez Wykonawcę, pod nadzorem Wykonawcy w miejscu wskazanym przez Zamawiającego;
		4. W przypadku gdy podczas instalacji paczek na środowisku produkcyjnym oraz produkcyjnego uruchamiania rozwiązania Zamawiający wykryje błąd w przekazanym kodzie, Wykonawca usunie ten błąd w ciągu maksymalnie 8 godzin roboczych od momentu zgłoszenia;
7. **Etap II – Stabilizacja**
	1. Wykonawca będzie świadczył 20-dniowy (Dni robocze) okres stabilizacji liczony od daty podpisania Protokołu odbioru Etapu I, polegający na rozwiązywaniu Błędów, przekazywanych Wykonawcy w ramach Zgłoszenia przez Zamawiającego drogą mailową, zgodnie z następującymi czasami ich rozwiązania.
	2. Sposób realizacji obsługi Błędów będzie następujący.
		1. Zamawiający dla celów odbiorów i zgłoszeń Błędów ustala następujące kategorie Błędów:
			1. Błąd kategorii A – błąd uniemożliwiający użytkowanie Integracji spowodowany wadliwym działaniem rozwiązania dostarczonego przez Wykonawcę, objawiające się brakiem możliwości skutecznego zalogowania się użytkownika Systemu e-PLOZ z wykorzystaniem WK lub logowanie się użytkownika Systemu e-PLOZ z  wykorzystaniem WK przekracza czas określony w pkt 1.4.10.
			2. Błąd kategorii B – błąd polegający na co najmniej jednym z poniższych:
				1. Główne elementy powodowane wadliwym działaniem rozwiązania dostarczonego przez Wykonawcę funkcjonują w sposób niezgodny z Dokumentacją;
				2. Występują istotne ograniczenia w działaniu Integracji Systemu e-PLOZ z WK, ale niepowodujące braku możliwości zalogowania się użytkownika Systemu e-PLOZ z wykorzystaniem WK, powodowane wadliwym działaniem rozwiązania dostarczonego przez Wykonawcę;
				3. Użytkownik nie może korzystać z elementów Integracji Systemu e- PLOZ z WK, co spowodowane jest wadliwym działaniem rozwiązania dostarczonego przez Wykonawcę ale uzyskanie oczekiwanych efektów jest możliwe w inny sposób).
		2. Zamawiający pod pojęciem czasu Naprawy rozumie czas pomiędzy potwierdzeniem przyjęcia zgłoszenia o Błędzie przez Wykonawcę, a dostarczeniem przez Wykonawcę do Repozytorium Zamawiającego poprawki usuwającej Błąd wraz z instrukcja opisującą sposób wdrożenia Naprawy;
		3. Wykonawca wskaże adres e-mail, na który Zamawiający będzie przekazywał zgłoszenia Błędów oraz otrzymywał potwierdzenie ich usunięcia. Uprawnionymi osobami do przekazania zgłoszenia Błędu będą pracownicy Zamawiającego lub podmioty trzecie działające w imieniu Zamawiającego, posiadające odpowiednie upoważnienie do zgłaszania Błędów.
		4. Błąd uznaje się za usunięty po otrzymaniu przez Wykonawcę potwierdzenia Zamawiającego o skuteczności dostarczonej poprawki.
		5. Zamawiający wymaga, aby czas reakcji na zgłoszenie Błędu, rozumiany jako czas potwierdzenia przyjęcia zgłoszenia przez Wykonawcę wynosił maksymalnie do 1 godziny (w Dni Robocze), liczone od zgłoszenia Błędu Wykonawcy przez Zamawiającego .
		6. Zamawiający wymaga, aby czas Naprawy nie przekroczył:
			1. dla Błędu kategorii A –nie dłużej niż 4 godziny w Dni Robocze,
			2. dla Błędu kategorii B –nie dłużej niż 2 Dni Robocze;
		7. W przypadku ujawnienia się Błędów kat. A lub kat. B, Zamawiający wezwie Wykonawcę do ich usunięcia w terminach wskazanych w pkt 2.2.6, a Wykonawca zobowiązany jest do usunięcia tych Błędów. W przypadku nie usunięcia zgłoszonych Błędów kat. A lub kat. B z przyczyn leżących po stronie Wykonawcy lub braku potwierdzenia przyjęcia zgłoszenia o którym mowa w punkcie 2.2.5 Zamawiający będzie uprawniony do naliczenia kar umownych lub odstąpienia w całości lub w części od Umowy, lub  wypowiedzenia Umowy.
	3. Zamawiający zastrzega sobie prawo do realizacji testów wydajnościowych oraz testów bezpieczeństwa w trakcie trwania Etapu II, własnym zespołem lub zlecając je podmiotowi zewnętrznemu. W przypadku wystąpienia nieprawidłowości, Wykonawca zobowiązany jest do ich usunięcia.
	4. Na zakończenie etapu, Strony podpiszą Końcowy Protokół Odbioru Umowy, przy założeniu spełnienia następujących warunków :
		1. Na zakończenie okresu stabilizacji brak będzie otwartych zgłoszeń Błędów. W przypadku występowania na koniec Etapu II otwartych zgłoszeń Błędów, Wykonawca usunie je zgodnie z czasami określonymi w punkcie 2.2.6. Końcowy Protokół Odbioru zostanie podpisany po skutecznej Naprawie Błędów zgłoszonych w Etapie II.
8. **Termin realizacji Zamówienia**
	1. Umowa zostanie zrealizowana w terminie nie dłuższym niż ……… (suma dni roboczych z Etapu I i II zgodnie z ofertą Wykonawcy, nie dłużej niż 63 Dni robocze) od momentu podpisania Umowy, z zastrzeżeniem ust. 3.2 i 3.3.
	2. Etap I zostanie zrealizowany w terminie ………. dni roboczych (zgodnie ze złożoną ofertą, nie krócej niż 20 Dni roboczych lecz nie dłużej niż 43 Dni roboczych) od momentu podpisania Umowy.
	3. Etap II zostanie zrealizowany w terminie 20 Dni roboczych od dnia podpisania protokołu odbioru Etapu I.
9. **Wymagania ogólne**
	1. W razie wystąpienia uzasadnionej potrzeby, Zamawiający zapewni przedstawicielom Wykonawcy realizującym przedmiot zamówienia, dostęp do pomieszczeń Zamawiającego. Udostępnienie pomieszczeń odbędzie się z zachowaniem procedur i regulaminów obowiązujących u Zamawiającego.
	2. Wykonawca jest zobowiązany informować Zamawiającego o postępie prac oraz raportować ich realizację co najmniej dwa razy w tygodniu, poprzez dostarczenie raportu z wykonanych dotychczas prac, wraz ze wskazaniem ryzyk i problemów, które pojawiły się podczas realizacji prac. Raport będzie przekazywany do osób wskazanych jako osoby odpowiedzialne za realizację umowy.
	3. W ramach realizacji przedmiotu zamówienia, Wykonawca przeniesie na Zamawiającego autorskie prawa majątkowe do utworów wytworzonych lub dostarczonych w ramach Umowy.
	4. W przypadku wykorzystywania przez Wykonawcę w wytworzonym oprogramowaniu elementów na licencji typu Open Source, wykonawca zobowiązany jest wskazać te elementy Integracji, poinformować o tym fakcie Zamawiającego i dostarczyć treść licencji określającej dokładne warunki korzystania. Równocześnie Wykonawca jest zobowiązany zapewnić, że wykorzystanie takiego oprogramowania Open Source będzie zgodne z postanowieniami odpowiednich licencji przypisanych do tego oprogramowania, jak również nie będzie ograniczać Zamawiającego w zakresie rozpowszechniania innego oprogramowania połączonego z oprogramowaniem Open Source, w tym nie może nakładać na Zamawiającego obowiązku rozpowszechniania takiego połączonego oprogramowania wraz z kodem źródłowym. W przypadku, w którym dana licencja uzależnia zakres takich obowiązków od sposobu połączenia oprogramowania Open Source z innym oprogramowaniem Wykonawca zobowiązany jest do zrealizowania takiego potencjalnego połączenia w sposób nienakładający na Zamawiającego obowiązku rozpowszechniania połączonego oprogramowania wraz z kodem źródłowym. Wykonawca gwarantuje, że licencja na oprogramowanie Open Source nie będzie nakładać na Zamawiającego obowiązku odprowadzania jakichkolwiek opłat lub wynagrodzenia na rzecz podmiotów uprawnionych do takiego oprogramowania przez 12  miesięcy od odebrania przedmiotu Umowy.
	5. W związku z tym, że Zamówienie jest realizowane ze środków publicznych Zamawiający zastrzega sobie możliwość udostępnienia wytworzonego kodu źródłowego innym instytucjom administracji publicznej lub realizującym zadania publiczne, w tym poprzez publikacje w publicznie dostępnych repozytoriach kodu źródłowego.
	6. Wykonawca zobowiązuje się, że osoby wykonujące usługi w zakresie czynności administracyjno-biurowych będą w okresie realizacji Umowy zatrudnione na podstawie umowy o pracę w rozumieniu przepisów ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (Dz.  U. z 2019 r. poz. 1040, z późn. zm.).
10. **Wymagania w zakresie tworzenia i aktualizacji Dokumentacji:**
	1. Zamawiający wymaga, aby dokumenty tworzone i modyfikowane w ramach realizacji zamówienia charakteryzowały się wysoką jakością, właściwą dla profesjonalnego charakteru świadczonych usług, na którą będą miały wpływ, takie czynniki jak:
		1. redakcja dokumentu:
			1. struktura dokumentu, rozumiana jako podział danego dokumentu na rozdziały, podrozdziały i sekcje w czytelny i zrozumiały sposób,
			2. sposób pisania rozumiany jako zachowanie spójnej struktury, formy i sposobu pisania dla poszczególnych dokumentów oraz fragmentów tego samego dokumentu,
			3. poprawność ortograficzna, gramatyczna i stylistyczna dokumentów,
			4. utrzymywanie aktualnych powiązań z innymi dokumentami.
		2. kompletność dokumentu – pełne przedstawienie omawianego problemu obejmujące całość z danego zakresu rozpatrywanego zagadnienia;
		3. spójność i niesprzeczność dokumentu – zapewnienie wzajemnej zgodności pomiędzy wszystkimi rodzajami informacji umieszczonymi w dokumencie, brak logicznych sprzeczności pomiędzy informacjami zawartymi we wszystkich przekazanych dokumentach oraz fragmentach tego samego dokumentu;
		4. aktualność – uwzględnienie w dokumencie bieżących czynników i uwarunkowań, w tym aktualnie istniejącej dokumentacji;
		5. zachowanie ogólnie przyjętych norm, standardów i kryteriów jakości.
	2. Cała Dokumentacja powinna być opracowywana w języku polskim.
	3. Elementy Dokumentacji analitycznej, projektowej, wykonawczej i powykonawczej muszą być tworzone zgodnie z notacją BPMN, UML 2.0, lub ArchiMate 3.0 lub nowszym, odpowiednio w obszarach uzgodnionych z Zamawiającym.
	4. Dokumentacja musi obejmować między innymi opis wymagań i decyzji architektonicznych, przypadki użycia wraz z opisem, opis i modele warstwy logicznej aplikacji w tym komponenty oprogramowania i realizację przypadków użycia, opis i diagramy procesów systemu, modele danych: koncepcyjne, logiczne, fizyczne, ogólny opis architektury aplikacji, mapowanie wymagań na przypadki użycia.
	5. Dokumentacja w warstwie fizycznej musi obejmować między innymi opis oraz diagramy z charakterystyką platformy oprogramowania, diagram rozmieszczenia komponentów aplikacji.
	6. Cała Dokumentacja powinna być dostarczana w edytowalnej postaci elektronicznej, w formacie przetwarzanym przez MS Word, Excel (od wersji 2007) lub Enterprise Architect firmy Sparks Systems (od wersji 14).
1. Za certyfikat równoważny certyfikatowi OCSP lub CEH zostanie uznany każdy aktualny certyfikat wydany na podstawie pozytywnego wyniku sprawdzenia wiedzy (egzaminu) w zakresie metodyki przeprowadzania testów penetracyjnych w zakresie: Technik rekonesansu, wykorzystania podatności systemów, podsłuchiwania ruchu, przeprowadzania penetracji systemów informatycznych, wykorzystania podatności w bazach danych, omijania IDS, Firewall oraz HoneyPot, kryptografii, ukrywania śladów. Egzamin przeprowadzony został przez instytucję nie powiązaną kapitałowo ani osobowo z Wykonawcą zapewniającą porównywalność i obiektywizm wyników egzaminacyjnych, wykorzystuje jednolite zadania egzaminacyjne, kryteria oceniania i zasady przeprowadzania egzaminu, jest sprawdzany jest przez niezależnych od Wykonawcy egzaminatorów. [↑](#footnote-ref-1)
2. Za certyfikat równoważny certyfikatowi CISSP zostanie uznany każdy aktualny certyfikat wydany na podstawie pozytywnego wyniku sprawdzenia wiedzy (egzaminu) w zakresie eksperckim bezpieczeństwa systemów informatycznych w obszarach: Zarządzania bezpieczeństwem i ryzykiem systemów informatycznych, Ciągłość działania, Zapobieganie katastrofom, Zarządzanie cyklem życia systemów informatycznych, rozwiązań bezpieczeństwa. Egzamin przeprowadzony został przez instytucję nie powiązaną kapitałowo ani osobowo z Wykonawcą zapewniającą porównywalność i obiektywizm wyników egzaminacyjnych, wykorzystuje jednolite zadania egzaminacyjne, kryteria oceniania i zasady przeprowadzania egzaminu, jest sprawdzany jest przez niezależnych od Wykonawcy egzaminatorów. [↑](#footnote-ref-2)