**Opis Przedmiotu Zamówienia**

**zaprojektowanie, budowa i wdrożenie systemu teleinformatycznego Krajowego Rejestru Mediatorów**

**realizowanego w ramach projektu pn. *Upowszechnienie alternatywnych metod rozwiązywania sporów poprzez podniesienie kompetencji mediatorów, utworzenie Krajowego Rejestru Mediatorów (KRM) oraz działania informacyjne***

Spis treści

1. [Kontekst zamówienia 3](#_Toc93330595)
2. [Przedmiot zamówienia 8](#_Toc93330597)
3. [Szczegółowe warunki realizacji zamówienia 9](#_Toc93330598)
4. [Etap I – Analiza Przedwdrożeniowa dla KRM 1.0 i KRM 2.0 – działania: 13](#_Toc93330599)
5. [Opracowanie i dostarczenie Planu Szkoleń: 14](#_Toc93330600)
6. [Opracowanie i dostarczenie Planu testów . 16](#_Toc93330601)
7. [Przeprowadzanie testów 17](#_Toc93330602)
8. [Wytworzenie i wdrożenie Systemu na środowiskach: automatycznej kompilacji, deweloperskim (wytwórcze), testowym. System działający na środowisku testowym zgodnym z wymaganiami Umowy oraz wymaganiami wynikającymi z przepisów prawa 20](#_Toc93330603)
9. [Wdrożenie Systemu na środowiskach przedprodukcyjnym i produkcyjnym. System działający na środowisku przedprodukcyjnym i produkcyjnym zgodny z wymaganiami umowy oraz wymaganiami wynikającymi z przepisów prawa. Przeprowadzenie testów. 23](#_Toc93330604)
10. [Przeprowadzenie audytu bezpieczeństwa –( Etap IVa – KRM 1.0, Etap IVb – KRM 2.0) 25](#_Toc93330605)
11. [Odbiór dokumentacji (Etap VIa – KRM 1.0, Etap Vb – KRM 2.0) 27](#_Toc93330606)
12. [Szczegółowe warunki realizacji zamówienia określonego w Fazie 2 29](#_Toc93330607)
13. [Świadczenia usług utrzymania i rozwoju Systemu teleinformatycznego MS 29](#_Toc93330608)
14. [Ogólne zasady realizacji Usług: 30](#_Toc93330609)
15. [Procedura realizacji Zgłoszeń: 35](#_Toc93330610)
16. [Usługa Modyfikacji Systemu: 37](#_Toc93330611)
17. [Procedura zlecania Modyfikacji 39](#_Toc93330612)
18. [Procedura odbioru Modyfikacji 42](#_Toc93330613)
19. [Szczegółowe zasady realizacji usługi gwarancyjnej: 45](#_Toc93330614)
20. [Zarządzanie realizacją przedmiotu zamówienia 46](#_Toc93330615)
21. [Kary umowne 48](#_Toc93330616)

# Kontekst zamówienia

Zamówienie realizowane jest w ramach prowadzonego przez Ministra Sprawiedliwości projektu pn. *Upowszechnienie alternatywnych metod rozwiązywania sporów poprzez podniesienie kompetencji mediatorów, utworzenie Krajowego Rejestru Mediatorów (KRM) oraz działania informacyjne* współfinansowanego ze środków Unii Europejskiej w ramach Programu Operacyjnego Wiedza Edukacja Rozwój.

Założenia projektu:

Obecnie brak jest systemu ułatwiającego nadzór nad mediatorami wpisanymi na listy stałych mediatorów, a także jednolitych standardów szkoleń. Powyższe problemy, utrudniają potwierdzenie kompetencji i kwalifikacji mediatorów, a także prawidłowe ustalenie liczby aktywnych zawodowo mediatorów na rynku w określonej kategorii spraw. Dotychczas przyjęta praktyka, przewiduje prowadzenie list stałych mediatorów przez prezesów sądów okręgowych przy SO w danym regionie, ale nie jest to ujednolicony, ogólnopolski rejestr i znaczna część mediatorów wpisuje się na listy mediatorów w różnych województwach, co utrudnia oszacowanie rzeczywistej liczby mediatorów aktywnych na rynku. Ponadto, brak jest systemu umożliwiającego nadzór nad działalnością zawodową mediatorów, co pozwala na generowanie tzw. „martwych dusz” - nieaktywnych zawodowo mediatorów. W trakcie dotychczasowych działań w obszarze interwencji publicznej wnioskodawca podejmował działania związane z propagowaniem mediacji sądowej oraz pozasądowej, a także podnoszeniem kompetencji mediatorów i świadomości społecznej w zakresie mediacji, przebiegu postępowania mediacyjnego oraz korzyści z mediacji. Dotychczasowe działania potwierdziły istnienie potrzeby podejmowania dalszych inicjatyw i prac w celu zwiększenia liczby spraw kierowanych do mediacji.

1. **Cel biznesowy Systemu**

Głównym zadaniem systemu teleinformatycznego Krajowego Rejestru Mediatorów (dalej również jako „System” lub „KRM”) jest gromadzenie i przetwarzanie informacji o osobach mediatorów:

1. sądowych,
2. pozasądowych.

Przedmiot zamówienia zakłada utworzenie ogólnopolskiej bazy mediatorów tj. listy mediatorów udostępnionej w systemie teleinformatycznym – na stronie internetowej   
z wyszukiwarką, zakładkami i informacjami dodatkowymi (komponent zewnętrzny, KRM 1.0).

System powinien uwzględniać możliwość rozwoju w kierunku zapewnienia dwustronnej komunikacji pomiędzy sądem a mediatorem (komponent wewnętrzny systemu, KRM 2.0).

Otoczenie prawne:

1. Rozporządzenie Ministra Sprawiedliwości *w sprawie prowadzenia listy stałych mediatorów* z dnia 20 stycznia 2016 r. (Dz. U. z 2016 r. 122),

2. Ustawa *Prawo o ustroju sądów powszechnych* z dnia 27 lipca 2001 r. (t.j. Dz.U. 2020 poz. 2072),

3. Ustawa *Kodeks postępowania cywilnego* z dnia 17 listopada 1964 roku (t.j. Dz.U. 2021 r. poz. 1805),

4. Rozporządzenie Ministra Sprawiedliwości *Regulamin urzędowania sądów powszechnych* z dnia 18 czerwca 2019 r. (Dz.U. z 2021 r. poz. 2046),

5. Ustawa *o informatyzacji działalności podmiotów realizujących zadania publiczne* z dnia 17 lutego 2005 roku (t.j. Dz.U. z 2021 r. poz. 2070),

6. Rozporządzenie Rady Ministrów *w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych* z dnia 12 kwietnia 2012 roku (t.j. Dz.U. z 2017 r. poz. 2247),

7. Ustawa *o krajowym systemie cyberbezpieczeństwa* z dnia 5 lipca 2018 roku (t.j. Dz.U. z 2020 r. poz. 1369),

**Słownik pojęć**

| **Pojęcie / skrót** | **Definicja** |
| --- | --- |
| **Administrator Systemu** | Pracownik administrujący systemem, w tym bazami danych lub aplikacją. |
| **Infrastruktura centralna** | Infrastruktura na której posadowiony jest System. |
| **Infrastruktura systemowa** | Całokształt rozwiązań sprzętowo - programowych  stanowiących podstawę wdrożenia i eksploatacji Systemu. |
| **Modyfikacje** | Zmiany w Systemie obejmujące zarówno zmiany w istniejących komponentach, jak i budowa nowych komponentów, projektowanie nowych procesów, budowa środowisk technologicznych. |
| **MS** | Ministerstwo Sprawiedliwości. |
| **Równoważność** | lub rozwiązanie równoważne o odpowiednich parametrach i możliwościach.  Ilekroć w treści OPZ użyte są znaki towarowe, patenty lub pochodzenie, źródła lub szczególne procesy,  a także normy, Zamawiający dopuszcza rozwiązanie równoważne. Przez produkt równoważny dla wyspecyfikowanego przedmiotu zamówienia rozumie się produkt o parametrach i wymaganiach minimalnych wyszczególnionych (wymienionych), które są równoważne dla wskazanego produktu.  W przypadku dostarczenia rozwiązania równoważnego, Wykonawca jest zobowiązany do zapewnienia kompatybilności z posiadanymi przez Zamawiającego licencjami lub wymienić posiadane przez Zamawiającego licencje oraz dostosować systemy informatyczne współpracujące przy zachowaniu ciągłości pracy, wszystkich danych oraz wydajności systemu. Zamawiający posiada kompetencje związane z eksploatacją posiadanego systemu, jeżeli oferowanym rozwiązaniem będzie inne niż wskazane przez Zamawiającego, Wykonawca zobowiązany jest do zapewnienia w ramach oferty stosownych szkoleń dla operatorów systemu w siedzibie Zamawiającego (nie mniej niż dla 5 osób i nie więcej niż dla 10 osób) z dostarczanego rozwiązania, w wymiarze nie mniejszym niż 8h szkoleń do wykorzystania na żądanie Zamawiającego w terminie obowiązywania Umowy. |
| **Oprogramowanie** | Oprogramowanie Systemu, w tym oprogramowanie systemowe i bazodanowe lub oprogramowanie aplikacji, do którego Zamawiający posiada autorskie prawa majątkowe. |
| **Oprogramowanie Osób Trzecich (OOT)** | Oprogramowanie inne niż będące własnością Zamawiającego, dostarczone przez Wykonawcę, konieczne do realizacji przedmiotu Umowy. |
| **OPZ** | Opis Przedmiotu Zamówienia w niniejszym postępowaniu. |
| **System/KRM** | Krajowy Rejestr Mediatorów. |
| **Usługa** | Usługa wsparcia technicznego i serwisu, Usługa Modyfikacji oraz Usługa realizacji szkoleń/warsztatów dla Administratorów Systemu. |
| **Użytkownik wewnętrzny** | Sędziowie, Referendarze, Pracownicy sądów powszechnych oraz mediatorzy. |
| **Użytkownik zewnętrzny** | Każdy użytkownik części zewnętrznej Systemu np. obywatele. |
| **Wada** | Nieprawidłowości związane z funkcjonowaniem Systemu. |
| **WF** | Wymagania funkcjonalne. |
| **WNF** | Wymagania niefunkcjonalne. |
| **Zgłoszenie** | Zgłoszenie Wady za pośrednictwem Serwisu zgłoszeniowego. |
| **Zlecenie** | Zlecenie Modyfikacji. |
| **Zamawiający** | Ministerstwo Sprawiedliwości. |

# Przedmiot zamówienia

Przedmiotem zamówienia jest zaprojektowanie, budowa oraz wdrożenie i rozwój wraz z integracją z istniejącymi rozwiązaniami systemu teleinformatycznego – Krajowego Rejestru Mediatorów (KRM) wraz ze świadczeniem usługi utrzymania i rozwoju.

Zakres zamówienia, określonego w pkt 1 obejmuje realizację prac w dwóch etapach:

Etap I - utworzenie ogólnopolskiej bazy mediatorów tj. listy mediatorów udostępnionej w systemie teleinformatycznym – na stronie internetowej z wyszukiwarką, zakładkami i informacjami dodatkowymi (komponent zewnętrzny, KRM 1.0),

Etap II - w dwóch Fazach:

rozwój KRM 1.0 obejmujący zapewnienie dwustronnej komunikacji pomiędzy sądem a mediatorem (komponent wewnętrzny systemu, KRM 2.0).

1. **Faza 1 Zaprojektowanie, budowa i wdrożenie** **obejmująca m.in.:**

Wykonawca zobowiązany jest uwzględnić wszystkie usługi niezbędne do zaprojektowania, zbudowania, wdrożenia, uruchomienia i późniejszej eksploatacji Systemu o deklarowanej funkcjonalności, a także usługę utrzymania i rozwoju w szczególności:

* 1. Przygotowanie Analizy Przedwdrożeniowej, obejmującej, co najmniej szczegółowy opis realizacji przez System funkcji określonych w Załączniku nr 1 do Opisu Przedmiotu Zamówienia oraz przygotowanie Projektu Technicznego Systemu,
  2. Opracowanie i dostarczenie Planu Szkoleń,
  3. Opracowanie Planu Testów,
  4. Wytworzenie i wdrożenie Systemu na środowiskach: automatycznej kompilacji, deweloperskim (wytwórcze), testowym. System działający na środowisku testowym zgodnym wymaganiami wynikającymi z przepisów prawa określonych powyżej. Przeprowadzanie testów,
  5. Wdrożenie Systemu na środowiskach przedprodukcyjnym i produkcyjnym. System działający na środowisku przedprodukcyjnym i produkcyjnym zgodny z wymaganiami Umowy oraz wymaganiami wynikającymi z przepisów prawa określonych powyżej,

1. przeniesienie autorskich praw majątkowych do Systemu (KRM 1.0 oraz KRM 2.0);
2. instalację oprogramowania Systemu na wskazanej przez Zamawiającego infrastrukturze sprzętowej;
3. wykonanie wszelkich czynności mających na celu instalację, wdrożenie, konfigurację, rozszerzenie, uruchomienie i integrację wszystkich elementów funkcjonalnych Systemu;
   1. zaplanowanie, przygotowanie i przeprowadzenie audytu bezpieczeństwa
   2. Przygotowanie materiałów szkoleniowych i szkoleń dla administratorów i użytkowników kluczowych Systemu;
   3. Opracowanie i dostarczenie wymaganej dokumentacji projektowej (przedwdrożeniowej i powykonawczej) w tym dokumentacji technicznej (projekt techniczny, analiza biznesowa), użytkowej i administracyjnej w języku polskim
   4. udzielenie gwarancji i rękojmi na dostarczone produkty i wykonane usługi na okres 36 miesięcy
4. **Faza 2 - Świadczenia usług utrzymania i rozwoju Systemu teleinformatycznego MS , tj.:**
   1. zapewnienie serwisu utrzymaniowego przez okres 36 miesięcy od odbioru produktu końcowego projektu,
   2. udzielenie gwarancji i rękojmi na dostarczone produkty i wykonane usługi na okres   
      36 miesięcy od daty odbioru produktu końcowego projektu.

Realizacja Zamówienia będzie następować w podziale na etapy określone w rozdziale 3.

# Szczegółowe warunki realizacji zamówienia

* 1. Faza I - KRM 1.0.

Zgodnie z art. 157b i 157c ustawy z dnia 27 lipca 2001 r. – Prawo o ustroju sądów powszechnych (t.j. Dz. U. z 2020 r. poz. 2072 ze zm.) wpisu/skreślenia na listę stałych mediatorów dokonuje prezes sądu okręgowego w drodze decyzji wydawanej na wniosek osoby ubiegającej się o wpis. Zgodnie z art. 157d prezes sądu okręgowego prowadzi listę stałych mediatorów dla obszaru właściwości danego okręgu sądowego. Na liście stałych mediatorów zamieszcza się następujące dane dotyczące stałego mediatora: imię i nazwisko oraz rok urodzenia, adres do korespondencji, informację dotyczącą wykształcenia i odbytych szkoleń, informacje dotyczące specjalizacji. Na liście, o której mowa w § 2, na wniosek stałego mediatora, zamieszcza się: numer telefonu stałego mediatora, adres poczty elektronicznej stałego mediatora, informację o wpisie na listę mediatorów, o której mowa w [art. 1832 § 3](https://sip.lex.pl/#/document/16786199?unitId=art(183(2))par(3)&cm=DOCUMENT) ustawy z dnia 17 listopada 1964 r. - Kodeks postępowania cywilnego. Prawomocna decyzja o wpisie na listę stałych mediatorów stanowi podstawę do wpisania mediatora na listę stałych mediatorów prowadzoną w innym sądzie okręgowym, na wniosek mediatora złożony do prezesa tego sądu. Stały mediator zawiadamia prezesa sądu okręgowego o każdej zmianie imienia lub nazwiska oraz danych lub informacji, o których mowa w § 2 pkt 2-4 oraz § 3, o okolicznościach, o których mowa w art. 157c § 1 pkt 3 i 4 p.u.s.p., umieszczeniu na liście mediatorów prowadzonej w sądzie okręgowym - w terminie 14 dni od dnia zaistnienia zdarzenia powodującego obowiązek zawiadomienia. Zgodnie z art. 157e prezes sądu okręgowego udostępnia sądom oraz innym podmiotom w siedzibie sądu oraz zamieszcza w Biuletynie Informacji Publicznej na stronie podmiotowej sądu aktualną listę stałych mediatorów, sposób prowadzenia listy stałych mediatorów, tryb wpisywania i skreślania z listy, zamieszczania na liście i aktualizacji danych i informacji.

Sposób potwierdzania spełnienia warunków wpisywania na listę, wzór formularza wniosku o wpis na listę stałych mediatorów, a także rodzaje dokumentów załączanych do wniosku, uwzględniając potrzebę zapewnienia wiarygodnej i aktualnej informacji o stałych mediatorach, jednolitości wniosków i sprawnego przebiegu procedury wpisu na listę stałych mediatorów reguluje Rozporządzenie Ministra Sprawiedliwości z dnia 20 stycznia 2016 r. w sprawie prowadzenia listy stałych mediatorów (Dz. U. poz. 122 ze zm.). Zgodnie z przywołanym Rozporządzeniem prezes sądu okręgowego prowadzi listę w formie tabelarycznej w postaci pisemnej i elektronicznej. Nagłówek tabeli stanowią rubryki określające poszczególne rodzaje danych i informacji, o których mowa w [art. 157d § 2](https://sip.lex.pl/#/document/16909701?unitId=art(157(d))par(2)&cm=DOCUMENT) i [3](https://sip.lex.pl/#/document/16909701?unitId=art(157(d))par(3)&cm=DOCUMENT) ustawy z dnia 27 lipca 2001 r. - Prawo o ustroju sądów powszechnych. Wpisy dotyczące poszczególnych mediatorów oddziela się od siebie pogrubioną linią poziomą. Wpisy zamieszcza się w porządku alfabetycznym. Wniosek o wpis na listę składa się do prezesa wybranego sądu okręgowego na urzędowym formularzu. Wzór formularza jest określony w załączniku do rozporządzenia. Osoba ubiegająca się o wpis na listę potwierdza spełnienie warunków wpisania na listę przez złożenie stosownych oświadczeń potwierdzonych czytelnym podpisem oraz oryginałów lub kopii dokumentów. Do wniosku dołącza się kopie dokumentów potwierdzających wiedzę i umiejętności w zakresie prowadzenia mediacji, którymi są: informacje o liczbie przeprowadzonych mediacji, spis wydanych publikacji na temat mediacji, opinie ośrodków mediacyjnych lub osób fizycznych o posiadanej wiedzy i umiejętnościach w zakresie mediacji, dokumenty poświadczające posiadane wykształcenie, odbyte szkolenia z zakresu mediacji oraz określające specjalizację. Prezes sądu okręgowego w razie wątpliwości co do treści lub autentyczności załączonych dokumentów może żądać okazania oryginałów dokumentów załączonych do wniosku. Wpisu na listę dokonuje się po sprawdzeniu spełnienia przez osobę ubiegającą się o wpis warunków, o których mowa w [art. 157a pkt 1-5](https://sip.lex.pl/#/document/16909701?unitId=art(157(a))pkt(1)&cm=DOCUMENT) ustawy pusp, oraz sprawdzeniu, czy zostały załączone oświadczenia i dokumenty, o których mowa w [art. 157b § 2](https://sip.lex.pl/#/document/16909701?unitId=art(157(b))par(2)&cm=DOCUMENT) i [3](https://sip.lex.pl/#/document/16909701?unitId=art(157(b))par(3)&cm=DOCUMENT) ustawy pusp. Osobę wpisaną na listę prowadzoną w innym sądzie okręgowym wpisuje się na listę na podstawie załączonej do wniosku decyzji. Wpisu na listę danych i informacji, o których mowa w [art. 157d § 2](https://sip.lex.pl/#/document/16909701?unitId=art(157(d))par(2)&cm=DOCUMENT) i [3](https://sip.lex.pl/#/document/16909701?unitId=art(157(d))par(3)&cm=DOCUMENT) ustawy pusp, dokonuje się na podstawie ostatecznej decyzji, o której mowa w [art. 157b § 1](https://sip.lex.pl/#/document/16909701?unitId=art(157(b))par(1)&cm=DOCUMENT) ustawy pusp, lub decyzji o wpisie na listę wydanej przez prezesa innego sądu okręgowego. Aktualizacji danych i informacji, o których mowa w [art. 157d § 2](https://sip.lex.pl/#/document/16909701?unitId=art(157(d))par(2)&cm=DOCUMENT) i [3](https://sip.lex.pl/#/document/16909701?unitId=art(157(d))par(3)&cm=DOCUMENT) ustawy pusp, dokonuje się po złożeniu wniosku stałego mediatora w tym przedmiocie. Dane dotychczas umieszczone na liście zastępuje się aktualnymi danymi. W razie ujawnienia okoliczności wskazującej, że zamieszczone na liście dane i informacje, o których mowa w [art. 157d § 2](https://sip.lex.pl/#/document/16909701?unitId=art(157(d))par(2)&cm=DOCUMENT) i [3](https://sip.lex.pl/#/document/16909701?unitId=art(157(d))par(3)&cm=DOCUMENT) ustawy pusp, są nieaktualne, na liście umieszcza się o tym wzmiankę.

System KRM 1.0 w momencie odbioru produktu końcowego powinien uwzględniać przepisy regulujące sposób prowadzenia listy i obejmować obsługę procesów:

* 1. wpis na listę stałych mediatorów przez Prezesa SO,
  2. zmianę wpisu na listę stałych mediatorów przez Prezesa SO,
  3. skreślenie wpisu na listę stałych mediatorów przez Prezesa SO,
  4. udostępnianie listy stałych mediatorów pracownikom sądów powszechnych,
  5. udostępnianie listy mediatorów użytkownikom zewnętrznym,
  6. architektura systemu KRM 1.0. powinna uwzględniać ograniczenia związane z przetwarzaniem danych osobowych i dostępem do danych osobowych przez poszczególne podmioty, tj. MS, sądy okręgowe, pozostałe sądy powszechne, użytkownicy zewnętrzni,
  7. Posiadać API (Interfejs Programowania Aplikacji) umożliwiające integrację z innymi systemami obsługującymi sądy i postępowania sądowe.
  8. **Faza II - KRM 2.0**

W założeniu projektodawców KRM 2.0 ma umożliwiać komunikację elektroniczną pomiędzy mediatorami a sądem powszechnym:

1. Komunikacja wewnętrzna w zakresie wpisu/zmiany wpisu na listę zgodnie z Rozporządzeniem Ministra Sprawiedliwości z dnia 20 stycznia 2016 r. w sprawie prowadzenia listy stałych mediatorów (Dz. U. poz. 122 ze zm.), a także skreślenia, przy czym na moment ogłoszenia szacowania nie są prowadzone zmiany przepisów w tym zakresie. W przypadku braku zmiany przepisów w ramach ogłoszenia postępowania, Zamawiający odstąpi od realizacji KRM 2.0 w tym zakresie. Na potrzeby szacowania należy przyjąć, że:
2. Mediatorzy komunikują się z sądem w zakresie wpisu wyłącznie elektronicznie;
3. Mediatorzy mają założone indywidualne konta w systemie KRM 2.0;
4. Logowanie do systemu KRM 2.0 następuje za pomocą profilu zaufanego ePUAP, certyfikowanego podpisu lub loginu i hasła;
5. Osoby, które pierwszy raz komunikują się z sądem mają utworzone konto tymczasowe do czasu wpisu na listę mediatora, po wpisie na listę mediatorów, takie osoba otrzymuje konto mediatora;
6. Konto zintegrowane jest z podpisem osobistym, podpisem kwalifikowanym, podpisem weryfikowanym profilem zaufanym ePUAP;
7. System umożliwia załączanie skanów dokumentów w formatach prawem przewidzianym;
8. System generuje urzędowe potwierdzenie przedłożenia (UPP);
9. System obsługuje doręczenia elektroniczne;
10. System generuje elektroniczne potwierdzenie odbioru (EPO);
11. System prezentuje wnioski w formacie xml, umożliwiające ich wypełnienie on-line (wnioski uwzględniają autouzupełnienie oraz walidację danych).
12. System generuje edytowalne szablony dokumentów związanych z postępowaniem mediacyjnym np. protokół z mediacji, wniosek o mediację, itp.
13. System jest zintegrowany ze wszystkimi systemami repertoryjno – biurowymi w sądach. Zamawiający informuje, że w sądach znajdują się różne systemy, które są licencjonowane.
14. System obejmuje import danych z systemów repertoryjno – biurowych.
15. Mediatorzy komunikują się w zakresie obsługi spraw z sądem i z obywatelami w zakresie prawem przewidzianym. Na potrzeby szacowania należy przyjąć:
16. sądy informują o przydzieleniu sprawy do mediacji za pośrednictwem systemu KRM 2.0
17. mediator uzgadnia z sądem udostępnienie akt na potrzeby mediacji komunikując się za pośrednictwem systemu teleinformatycznego
18. mediator przekazuje produkty mediacji drogą elektroniczną (należy przyjąć, że przepisy przewidują możliwość zawarcia ugody w formie elektronicznej),
19. system KRM 2.0 będzie posadowiony na wskazanej przez Zamawiającego infrastrukturze sprzętowej.

Wykonawca w trakcie realizacji umowy zobowiązany jest do oznaczenia wszystkich składowych produktów projektu znakiem Funduszy Europejskich, barwami RP, logotypem zamawiającego (Ministerstwo Sprawiedliwości) i znakiem Unii Europejskiej.

1. **Etapy i terminy realizacji Przedmiotu Zamówienia.**

Prace polegające na realizacji Przedmiotu Zamówienia zostaną zrealizowane w następujących Etapach:

1. Etap I – Analiza Przedwdrożeniowa dla KRM 1.0 i KRM 2.0 – działania:
   1. Opracowanie Projektu Technicznego Systemu - zostanie opracowany przez Wykonawcę na postawie zatwierdzonych przez Zamawiającego wyników analizy biznesowej i systemowej, w tym opracowanych modeli procesowych, dalej: Analiza Przedwdrożeniowa. Analiza Przedwrożeniowa obejmować musi kompleksowo wszystkie zagadnienia funkcjonalne i techniczne projektowanego rozwiązania.

Produkt: Analiza biznesowa i systemowa

Produkt: Analiza Przedwdrożeniowa

Aktualność produktów utrzymywana jest do czasu odebrania systemu KRM 2.0.

* 1. W Projekcie Technicznym Systemu zostanie opisany szczegółowo sposób konfiguracji Systemu w organizacji Zamawiającego oraz w sądach powszechnych, określając przy tym sposób realizacji każdego z wymagań zdefiniowanych w OPZ i w Analizie Przedwdrożeniowej.

Projekt Techniczny Systemu musi zostać opracowany na poziomie szczegółowości gwarantującym jednoznaczność opisu sposobu działania Systemu oraz sposobu jego konfiguracji (w tym fizycznych komponentów rozwiązania np.: konfiguracji sieciowych, planów adresacji, środowiskowych, plików i parametrów konfiguracyjnych, ścieżek, mechanizmów dot. niezawodności i bezpieczeństwa działania, modeli wymiany danych w ramach mechanizmów integracyjnych, opisu działania i wywoływania poszczególnych funkcji, projektów widoków poszczególnych ekranów w systemie, formatów danych wprowadzanych, pól, walidacji, filtracji, sortowania itp.).

W Projekcie Technicznym Systemu wymagane jest opisanie zagadnień   
m.in. w zakresie:

1. przedmiotu wdrożenia,
2. celów, założeń, zależności i ograniczeń,
3. funkcjonalności Systemu,
4. opisu i specyfikacji wymagań,
5. aktorów, uprawnień i ról,
6. przypadków użycia Systemu opisanych stosownymi scenariuszami,
7. opisu sposobu realizacji poszczególnych przypadków użycia w Systemie,
8. modeli struktur danych,
9. schematów przepływu danych,
10. interfejsu użytkownika,
11. interfejsów integracyjnych (wewnętrznych i zewnętrznych),
12. modelu wymiany danych,
13. szczegółowego opis konfiguracji poszczególnych komponentów Systemu składające się na projekt architektury logicznej i fizycznej tworzonego rozwiązania.

Opisany w Projekcie Technicznym Systemu projekt infrastruktury, jej minimalnych wymagań oraz środowiska musi uwzględniać podział środowisk na, co najmniej: produkcyjne i testowe.

Produkt: Projekt Techniczny Systemu Aktualność produktów utrzymywane jest do czasu odebrania systemu KRM 2.0.

1. Opracowanie i dostarczenie Planu Szkoleń:
2. Wykonawca zobowiązany jest do przygotowania Planu Szkoleń zarówno dla Systemu KRM 1.0 jak i 2.0. Dokument ten powinien precyzować szczegółowo nie tylko aspekty organizacyjne realizacji szkoleń, harmonogram szkoleń, ale również zawierać merytoryczne aspekty szkoleń jak agendy poszczególnych szkoleń, program szkoleń i materiały szkoleniowe.
3. Rozpoczęcie realizacji szkoleń warunkowane jest akceptacją przez Zamawiającego Planu szkoleń przygotowanego przez Wykonawcę.
4. Zamawiający zakłada przeprowadzenie szkolenia e-learningowego dla użytkowników systemu oraz szkolenia dla administratorów i użytkowników wewnętrznych Systemu.

**Zamawiający zakłada następujące wymagania co do szkoleń:**

**[Szkolenia e-learningowe]**

* 1. Wykonawca przygotuje materiały szkoleniowe do szkoleń e-learningowych użytkowników wewnętrznych Systemu w platformie SAP LSO (zwane dalej „Materiałami szkoleniowymi”)
  2. Dla szkoleń e-learningowych Wykonawca zapewni profesjonalne Materiały szkoleniowe, zawierające część teoretyczną oraz ćwiczenia pozwalające na aktywne zdobywanie wiedzy w zakresie obsługi systemu KRM
  3. Szkolenia e-learningowe muszą być interaktywne. Nie jest akceptowalna forma prezentacji zawierającej jedynie screeny z ekranu. Uczestnik szkolenia musi mieć możliwość nawigacji. Elementem szkoleń e-learningowych powinny być scenki i filmiki wspomagające przyswajanie wiedzy jak również wypełniane aktywnie formularze ekranowe i egzamin ze zdobytej wiedzy.
  4. Materiały szkoleniowe wykonane mają być w języku polskim w postaci elektronicznej.
  5. Materiały szkoleniowe przygotowane mają być w formacie SCORM 2004, do publikacji materiałów w formacie HTML5
  6. Warunkiem przystąpienia do realizacji Materiałów szkoleniowych jest akceptacja Planu Szkoleń przez Zamawiającego
  7. Projekt Materiałów szkoleniowych powinien zawierać co najmniej informacje o sposobie przekazania wiedzy, plan szkolenia, podział na bloki tematyczne, informacje o formie sprawdzenia i utrwalenia wiedzy, informacje o wykorzystanych funkcjach i dodatkach (np. zdjęcia, zapisy audio lub audio-wideo), które mają przyczynić się do uatrakcyjnienia szkolenia, formę sprawdzenia nabytej wiedzy, sposób stylizacji slajdów, projekt wizualno-funkcjonalny szkolenia w postaci reprezentatywnych ekranów szkolenia (prototyp szkolenia zawierający do kilkunastu ekranów szkolenia ujmujący wszystkie typy ekranów i formy dydaktyczne zaplanowane w szkoleniu oraz umożliwiające prezentację nawigacji i narracji), wkład merytoryczny (wszelkie treści dydaktyczne, które będą składały się na przygotowane szkolenia w postaci tekstowej gotowe do przetworzenia na postać szkolenia e-learningowego).
  8. W ramach projektu Materiałów szkoleniowych Wykonawca przedstawi projekt docelowego szkolenia e-learningowego, które Zamawiający zaimplementuje na platformie SAP LSO celem weryfikacji treści merytorycznej i zastosowanej formy graficznej.
  9. Wykonawca przekaże materiały szkoleniowe do akceptacji Zamawiającego na 3 tygodnie przed rozpoczęciem szkoleń.
  10. Wykonawca przekaże pliki źródłowe Materiałów szkoleniowych wraz z przeniesieniem wszelkich praw autorskich.

1. [Wymagania ogólne dla szkoleń online]
   1. Szkolenia muszą być zrealizowane w języku polskim.
   2. Szkolenia obejmować będą wyłącznie zakres funkcjonalności rozwiązania, który przeszedł pozytywne testy akceptacyjne Zamawiającego.
   3. Szkolenie dot. administracji zrealizowane zostanie w zakresie, który zagwarantuje Zamawiającemu samodzielne zarządzanie wdrożonym systemem.
   4. Wykonawca zapewni asystę zdalną trenera odpowiadającego na pytania uczestników szkolenia (drogą elektroniczną) przez okres do 2 tygodni po zakończeniu ostatniego ze szkoleń.
   5. Szkolenia odbywają się online
   6. Na potrzeby szacowania należy założyć, że Wykonawca zapewni 10 terminów szkoleń odpowiednio na etapie przed wdrożeniem KRM 1.0, jak i przed wdrożeniem KRM 2.0. Czas trwania szkolenia to 4 godziny szkoleniowa (godzina szkoleniowa = 45 min)
   7. Wszystkie szkolenia będą rejestrowane w formie audiowizualnej i po zakończeniu szkoleń zostaną one przesłane Zamawiającemu w formie elektronicznej.
   8. Po zakończeniu szkoleń oraz asysty Wykonawca przygotuje raport podsumowujący wyniki szkoleń i asysty.

Produkt: Plan szkoleń

1. Opracowanie i dostarczenie Planu testów .

**Plan testów** obejmuje w szczególności: Scenariusze Testowe będące podstawą weryfikacji poprawności działania rozwiązania i jego zgodności z założeniami opisanymi w Projekcie Technicznym Systemu. Plan Testów regulował będzie również szczegółowe założenia i procedury realizacji testów – musi zawierać w tym zakresie:

1. cel przeprowadzenia testu,
2. metodę̨ przeprowadzenia testów,
3. zasady organizacyjne, podział zadań,
4. oprogramowanie wspomagające testy,
5. harmonogram testów,
6. macierz pokrycia wymagań i przypadków użycia scenariuszami testowymi,
7. opis i konfigurację środowiska testowego,
8. wykaz danych testowych niezbędnych do wykonania testów.

**Scenariusze Testowe** muszą pokrywać wszystkie zdefiniowane w Projekcie Technicznym przypadki użycia rozwiązania oraz zawierać w każdym teście poza ścieżką podstawową co najmniej jedną ścieżkę alternatywną realizacji pracy. Scenariusze Testów zawierać będą co najmniej dane w zakresie:

1. Nr scenariusza,
2. Nr kroku testowego,
3. Opis czynności do wykonania,
4. Dane testowe,
5. Użytkownik wykonujący (rola w Systemie),
6. Oczekiwany rezultat,
7. Odnotowanie uzyskanego w teście rezultatu,
8. Uwagi.

Scenariusze testowe muszą być przygotowane przez Wykonawcę dla każdego z objętych projektem rodzajów testów. Scenariusze testowe muszą być możliwe do zaimportowania w oprogramowaniu TestFLO Test Management for JIRA i HP ALM, które są w posiadaniu Zamawiającego.

Scenariusze Testowe podlegają akceptacji Zamawiającego.

1. Przeprowadzanie testów

Wykonawca jest zobligowany do przygotowania środowiska testowego zgodnie z zatwierdzonym przez Zamawiającego Planem Testów.

Wykonawca zobligowany jest do uczestnictwa w prowadzonych przez Zamawiającego testach i bieżącego wsparcia zespołu Zamawiającego w toku realizowanych testów. Wersja systemu dostarczona przez Wykonawcę Zamawiającemu powinna przejść uprzednio pozytywnie testy wewnętrzne w organizacji Wykonawcy, a przy kolejnej korekcyjnej iteracji testów również stosowne testy regresyjne. Przed przystąpieniem Zamawiającego do testów Wykonawca przedstawi wyniki testów wewnętrznych (dotyczy również testów regresji w kolejnych iteracjach) oraz dostarczy kompletne i aktualne skrypty testów automatycznych pokrywających pełną funkcjonalność Systemu Zamawiający w toku testów, poza weryfikacją Systemu na bazie Scenariuszy Testowych przygotowanych przez Wykonawcę, może tworzyć i realizować własne scenariusze testowe oraz dokonywać testów rozwiązania ad-hoc (bez użycia scenariuszy).

W projekcie wymagana jest realizacja Testów Akceptacyjnych Zamawiającego (TAZ), realizowanych przez Wykonawcę, w tym:

1. testów funkcjonalnych – testy poszczególnych funkcji Systemu w ramach obszaru wdrożenia.
2. testów pokrycia – realizowanych dla identyfikacji wszystkich przypadków testowych,
3. testów wydajnościowych – testy polegające na określeniu czasu odpowiedzi systemu w dialogowym trybie pracy dla określonej liczby jednocześnie pracujących użytkowników i czasu realizacji w systemie określonych procesów. Testowane będą różne poziomy obciążenia oraz sytuacja przeciążenia systemu. Zamawiający wymaga sprawnego działania systemu przy obciążeniu na poziomie 300 równoległych sesji. Wymagany scenariusz testów wydajnościowych został opisany w sekcji poniżej.
4. testów integracyjnych – test realizacji procesów zaimplementowanych w systemie, a wymagających wymiany danych z systemami współpracującymi z projektowanym rozwiązaniem (jeżeli dotyczy).
5. testów jednostkowych – w zakresie testów poszczególnych elementów składających się na rozwiązanie
6. testów bezpieczeństwa – w szczególności w zakresie analizy zgodności konfiguracji i sposobu funkcjonowania urządzeń oraz analizy podatności aplikacji.
7. testów użyteczności – testy te zrealizowane zostaną z zaangażowaniem użytkowników końcowych systemu, obejmują weryfikację interakcji użytkowników z systemem w zakresie badania poprawności budowy interfejsu użytkownika w tym jego intuicyjności i przyjazności oraz zgodności z wymaganymi w tym zakresie standardami.
8. testów akceptacyjnych - dot. poprawności konfiguracji infrastruktury serwerowej, w tym testów ciągłości działania.
9. testów dostępności systemu- celem testu jest weryfikacja zastosowanych w portalu rozwiązań dostosowania do wymogów WCAG 2.1/ 2.2

Testy wydajnościowe powinny zostać zrealizowane z uwzględnieniem poniższych wymagań dot. scenariusza testów:

1. Testy odbędą się w środowisku preprodukcyjnym (przed uruchomieniem produkcyjnym) z poziomu sieci lokalnej Zamawiającego.
2. Przedmiotem testu będą symulowane operacje użytkowników na Systemie produkcyjnym.
3. Na test składały się będą skrypty automatyczne odzwierciedlające przejście przez wybrane moduły/podstrony Systemu.
4. Zamawiający wskaże reprezentatywne moduły/podstrony wytworzonego Systemu, które wejdą w skład testu, przy założeniu, że merytoryczna zawartość informacyjnej treści tekstowej (tzn. zawartość strony poza znacznikami HTML, skryptami, arkuszami stylów, ilustracjami i innymi elementami strony HTML nie stanowiącymi zawartości merytorycznej) serwowanej przez poszczególne podstrony nie przekroczy 500kB.
5. W trakcie testu użytkownicy, po zalogowaniu się, przechodzą między modułami wykonując operacje odczytu i zapisu do bazy.
6. Obciążenie systemu symulowane będzie poprzez inicjację 300 równoczesnych sesji użytkowników w systemie.
7. Użytkownicy inicjowani będą stopniowo z użyciem losowego czasu reakcji pomiędzy transakcjami, aby warunki testu były jak najbardziej zbliżone do rzeczywistych.
8. Co 5 sekund loguje się kolejnych 10 użytkowników. Łącznie ramp-up zajmuje 25 minut.
9. Czas reakcji użytkownika przyjęto jako wartość losową z zakresu między 10, a 15 sekund.
10. Po przejściu ścieżki scenariusza użytkownicy powtarzają pełną ścieżkę scenariusza.
11. Oczekiwany rezultat, którego spełnienie warunkuje spełnienie wymagań wydajnościowych nałożonych przez Zamawiającego:
    1. Średni czas załadowania testowanej strony systemu nie może być dłuższy niż 5 sekund.
    2. Średni czas transakcji zapisu do bazy nie może być dłuższy niż 5 sekund.

Scenariusze testowe powinny być przygotowane przez Wykonawcę dla każdego z objętych projektem rodzajów testów. Scenariusze testowe muszą być możliwe do zaimportowania w oprogramowaniu TestFLO Test Management for JIRA i HP ALM, które są w posiadaniu Zamawiającego.

Produkt: Scenariusze testowe dla Systemu KRM 1.0 i KRM 2.0

1. Wytworzenie i wdrożenie Systemu na środowiskach: automatycznej kompilacji, deweloperskim (wytwórcze), testowym. System działający na środowisku testowym zgodnym z wymaganiami Umowy oraz wymaganiami wynikającymi z przepisów prawa

System KRM będzie wykorzystywał obecną infrastrukturę sprzętową wskazanego sądu apelacyjnego. System KRM będzie zainstalowany na wskazanej przez Zamawiającego infrastrukturze sprzętowej

**Główne założenia:**

W zakresie infrastruktury sprzętowej – platforma x86-64 wraz z zastosowaniem platformy wirtualizacji lub ewentualnie platformy do konteneryzacji usług. W zakresie sytemu przechowywania danych – macierze dyskowe z zastosowaniem zróżnicowanej wydajności.

Sieć i bezpieczeństwo - wykorzystanie: systemu wykrywania i zapobiegania włamaniom (Intrusion Prevention System, Intrusion Detection System ), systemu zapory sieciowej (FireWall). Systemy operacyjne serwerowe Windows Server, Linux (Red Hat Enterprise Linux, SUSE Linux Enterprise Server). Bazy danych MS SQL Server, IBM Db2. Serwery aplikacji - MS Internet Information Services, Red Hat JBoss Enterprise Application Platform, inne wykorzystywane w OCP. Platforma wirtualizacji: Vmware

1. Wytworzone i dostarczone Oprogramowanie Dedykowane w postaci kodów źródłowych i wersji skompilowanej,
2. Wytworzone i dostarczone Oprogramowanie wraz z licencjami, programami niezbędnymi do prawidłowego funkcjonowania Systemu oraz kodami źródłowymi i wersji skompilowanej dla Oprogramowania Dedykowanego. System ze wszystkimi funkcjonalnościami gotowy do uruchomienia i testów w środowisku testowym,
3. Dostosowanie, zainstalowanie, skonfigurowane i przetestowanie Systemu na infrastrukturze Zamawiającego,
4. Dostarczenie, instalacja i konfiguracja zoptymalizowanego Oprogramowania systemowo-narzędziowego,
5. Zamawiający wymaga aby Wykonawca przekazywał mu wytworzone produkty przyrostowo z częstotliwością określoną w Planie Kontraktu.
6. Zamawiający wymaga, aby Wykonawca tworzył produkty analityczne z wykorzystaniem oprogramowania Enterprise Architekt bądź równoważnym w wersji minimum takiej jak posiada aktualnie Zamawiający (wersji nie niższej niż v 13), zgodnego z modelem MDA oraz aktualną metodyką wytwarzania oprogramowania Ministerstwa Sprawiedliwości.
7. Zamawiający wymaga aby dostarczone kody źródłowe nie zawierały elementów składowych systemu tj. bibliotek, komponentów, kodów źródłowych, itp. firm trzecich jaki i „open source” bez praw do ich wykorzystania przez Zamawiającego w przekazanych produktach. Wszystkie elementy systemu, które Wykonawca będzie chciał użyć, muszą być wcześniej zatwierdzone przez Zamawiającego w zakresie wykorzystania, licencjonowania, oraz wsparcia technicznego producenta.
8. Zamawiający wymaga, aby Wykonawca zapewnił Zamawiającemu wszystkie wykorzystane licencje na oprogramowanie i biblioteki wykorzystywane w trakcie kompilacji, testów, instalacji i wdrożenia oprogramowania. Wykonawca musi zapewnić Zamawiającemu prawo do korzystania z nich przez okres od dnia dostarczenia licencji do upływu 3 lat po zakończeniu umowy z Zamawiającym. W przypadku licencji na użytkownika (programisty, wdrożeniowca, itd) Wykonawca musi zapewnić min 10 licencji dla Zamawiającego.
9. Zamawiający wymaga, aby w ramach dostarczanych produktów były:
10. Wyniki analiz, projekty architektury w formacie EAP (jeden plik rozwijany i wersjonowany).
11. Kody źródłowe, testy funkcjonalne, testy jednostkowe, testy integracji, scenariusze testowe, wraz z raportami wykonania.
12. Wykorzystywane biblioteki i licencje wystawione na rzecz Zamawiającego
13. Instrukcje instalacji, konfiguracji na środowisku deweloperskim, testowym i produkcyjnym, w szczególności konfigurację procesów Continuous Integration, Continuous Veryfication, Continuous Delivery na serwerze Bamboo z uwzględnieniem realizacji testów jednostkowych.
14. Zamawiający wymaga dostarczenia produktów na nośniku elektronicznym. Zamawiający nie udostępni Wykonawcy dostępu do środowiska Zamawiającego. Zamawiający dopuszcza ew. asystę personelu Wykonawcy w czynnościach mających na celu wgrywanie produktów na środowisko Zamawiającego.
15. Zamawiający wymaga, aby odbiór produktów odbywał się na środowisku Zamawiającego i poszczególne produkty będą deponowane w następujących miejscach:
16. Projekty analiz na bazie danych EA (MSSQL) projektu zawierającej wersjonowanie.
17. Kody źródłowe w repozytorium Bitbucket Zamawiającego dla danego projektu.
18. Testy funkcjonalne w oprogramowaniu HP ALM Zamawiającego.
19. Licencje, instrukcje w repozytorium SVN Zamawiającego.
20. Zamawiający wymaga, aby pokrycie kodu źródłowego testami jednostkowymi było na poziomie min. 80%.
21. Zamawiający wymaga przygotowania instrukcji konfiguracji serwera Bamboo Zamawiającego umożliwiającego minimum:
22. Zbudowanie aplikacji
23. Przeprowadzenie testów automatycznych: jednostkowych, regresji i integracyjnych.
24. Wdrożenie aplikacji na wyznaczonym przez Zamawiającego środowisku.
25. Zamawiający wymaga od Wykonawcy udostępnienia co najmniej 10 licencji dla użytkowników Zamawiającego do systemu zarządzania zadaniami Atlassian Jira Software utrzymywanego na zasobach Wykonawcy. Zamawiający wymaga, aby Wykonawca realizował projekt w oparciu o to oprogramowanie w taki sposób aby Zamawiający w każdym momencie miał wgląd do stanu zaawansowania prac. Na życzenie Zamawiającego Wykonawca przedstawi bądź też udostępni możliwość Zamawiającemu generowania raportów dot. procesu zaawansowania prac.
26. Zamawiający wymaga dostarczenia co najmniej 10 licencji na rzecz Zamawiającego dla oprogramowania Bitbucket i Bamboo bądź równoważny wraz z min. rocznym utrzymaniem w przypadku gdy wymagania licencyjne wykorzystywane do przeprowadzenia procesu budowania i testowania oprogramowania przekroczą możliwości licencyjne Zamawiającego.
27. Przygotowanie wszelkich niezbędnych procedur związanych z zarządzaniem uprawnieniami, wdrożeniem i utrzymaniem Systemu,
28. Plany testów, Raporty z wykonania testów,
29. Przeprowadzenie testów Systemu: bezpieczeństwa, akceptacyjnych, automatycznych, funkcjonalnych, użyteczności (interfejsu), instalacji (konfiguracji), modułowych (jednostkowych), regresyjnych, jednostykowych, integracyjnych, w zakresie procedur i mechanizmów backupowych, Testy instalacji.
30. Wdrożenie Systemu na środowiskach przedprodukcyjnym i produkcyjnym. System działający na środowisku przedprodukcyjnym i produkcyjnym zgodny z wymaganiami umowy oraz wymaganiami wynikającymi z przepisów prawa. Przeprowadzenie testów.

**Etap II – Wytworzenie i wdrożenie Systemu na środowiskach: automatycznej kompilacji, deweloperskim (wytwórcze), testowym. System działający na środowisku testowym zgodnym z wymaganiami (Etap IIa – KRM 1.0, KRM IIb – KRM 2.0)**

Główne działania:

1. Dostarczone Oprogramowanie Systemu wraz z ewentualnymi licencjami, programami niezbędnymi do prawidłowego funkcjonowania Systemu oraz kodami źródłowymi i wersji skompilowanej.
2. Dostosowanie, zainstalowanie, skonfigurowane i przetestowanie Systemu na infrastrukturze Zamawiającego ,
3. Przygotowanie procedur związanych z zarządzaniem uprawnieniami, wdrożeniem i utrzymaniem Systemu,
4. Przeprowadzanie testów,
5. Wykonawca zobowiązany jest przenieść autorskie prawa majątkowe do Systemu na Zamawiającego. Wykorzystanie licencjonowanego oprogramowania lub usług typu XaaS możliwe jest tylko za wyłączną zgodą Zamawiającego wyrażoną w sposób jednoznaczny w ramach Etapu I.

**Przeprowadzanie testów**

1. Testy odbędą się w środowisku testowym (przed uruchomieniem produkcyjnym) z poziomu sieci lokalnej Zamawiającego.
2. Przedmiotem testu będą symulowane operacje użytkowników na Systemie produkcyjnym.
3. Na test składały się będą skrypty automatyczne odzwierciedlające przejście przez wybrane moduły/podstrony Systemu.
4. Zamawiający wskaże reprezentatywne moduły/podstrony wytworzonego Systemu Raporty z testów: Testy akceptacyjne, Testy automatyczne, Testy funkcjonalne, Testy instalacji (konfiguracji), Testy integracyjne, Testy modułowe (jednostkowe), Testy wydajnościowe,
5. Przetestowanie z sukcesem w zakresie zgodności implementacji procesów biznesowych i funkcjonalności Systemu oraz potwierdzenie w zakresie zgodności Systemu z wymaganiami WCAG 2.1./2.2 oraz zgodności Systemu z wytycznymi określonymi w Załączniku nr 4 do Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z dn. 15 maja 2012 r., poz. 526). oraz wymienionymi w Krajowych Ramach Interoperacyjności zaleceniami norm: PN-ISO/IEC 27001, PN-ISO/IEC 27002, PN-ISO/IEC 27005, PN-ISO/IEC 24762S oraz zaleceniami normy ISO 22301. Spełnienie wymagań RODO, ustawy o ochronie danych osobowych,
6. Dostarczenie oświadczenia potwierdzającego zgodność Systemu z WCAG 2.1/2.2
7. Przeprowadzenie z sukcesem testów Systemu: obciążeniowych, wydajnościowych, bezpieczeństwa, akceptacyjnych, automatycznych, funkcjonalnych, użyteczności (interfejsu), instalacji (konfiguracji), modułowych (jednostkowych), regresyjnych, jednostykowych, integracyjnych, w zakresie procedur i mechanizmów backupowych,
8. Plany testów, Raporty z wykonania testów.

**Etap III - wdrożenie Systemu na środowiskach przedprodukcyjnym i produkcyjnym. System działający na środowisku przedprodukcyjnym i produkcyjnym zgodny z wymaganiami Umowy oraz wymaganiami wynikającymi z przepisów prawa (Etap IIIa – KRM 1.0, Etap IIIb – KRM 2.0)**

1. Dostarczone Oprogramowanie wraz z licencjami, programami niezbędnymi do prawidłowego funkcjonowania Systemu oraz kodami źródłowymi i wersji skompilowanej dla Oprogramowania dedykowanego.
2. Dostosowanie, zainstalowanie, skonfigurowane i przetestowanie Systemu na infrastrukturze Zamawiającego ,
3. Przygotowanie procedur związanych z zarządzaniem uprawnieniami, wdrożeniem i utrzymaniem Systemu,
4. Przeprowadzanie testów,
5. Raport z testów
6. Przeprowadzenie audytu bezpieczeństwa –( Etap IVa – KRM 1.0, Etap IVb – KRM 2.0)

Wykonawca zobowiązany jest do przeprowadzenia audytu bezpieczeństwa wytworzonego Systemu na środowisku przedprodukcyjnym.

**Wymagania dla audytu bezpieczeństwa:**

1. Usługę przeprowadzenia testów bezpieczeństwa/penetracyjnych dla powstałego Systemu powstałego Systemu.
2. Zakres minimalny testów:
3. dla aplikacji Web / interfejsu API Systemu:
4. Testy aplikacji WWW według standardu OWASP ASVS 4.0 Level 1 – Greybox (bez dostępu do systemu operacyjnego i kodu źródłowego) (Załącznik Nr 1 - Testy aplikacji WWW według standardu OWASP ASVS 4 do OPZ)Wymagania standardów i metodyk:

Wykonawca zobowiązany jest stosować co najmniej następujące metody i standardy lub inne odpowiednie do analizowanego elementu Systemu w porozumieniu z Zamawiającym:

* 1. Wykorzystanie baz danych o znanych podatnościach i słabościach bezpieczeństwa:
     1. SAN Top 20 Critical Security Controls lub równoważne,
     2. Common Vulnerabilities and Exposures lub równoważne,
     3. WASC (Web Application Security Consortium) Threat Classifications lub równoważne,

Przy czym za równoważne Zamawiający uzna, takie bazy danych, które stanowią aktualne źródło informacji o lukach bezpieczeństwa:

* 1. są publikowane i utrzymywane przez którekolwiek państwo będące członkiem paktu NATO lub
  2. są stworzone i utrzymywane przez organizacje, niezależnie od ich form (komercyjna, non-profit w tym zorganizowana społeczność internetowa) których celem działalności jest zapewnienie bezpieczeństwa systemów i rozwiązań informatycznych, Zamawiający nie dopuszcza zastosowania baz, których wiarygodność została podważona w zakresie ich wykorzystania przez administracje publiczną tych Państw, 2) Odpowiednio do zakresu, zastosowanie list kontrolnych udostępnianych przez organizacje pracujące na rzecz bezpieczeństwa systemów IT do projektowania i oceny bezpieczeństwa systemów operacyjnych, baz danych, tj.:
     1. National Security Agency (NSA) lub równoważne,
     2. Center for Internet Security (CIS) lub równoważne.

Przy czym za równoważne Zamawiający uzna, takie listy kontrolne, które opisują całość procesów audytu systemów oraz rozwiązań informatycznych w niemniejszym zakresie, z niemniejszą szczegółowością i systematyką wykonywania audytu.

1. Zastosowanie do testów bezpieczeństwa, odpowiednio do zakresu, jednego ze standardów:
   1. OWASP (Open Web Application Security Project) ASVS 20141 lub równoważne,
   2. Open Source Security Testing Methodology Manual (OSSTMM) lub równoważne,
   3. Penetration Testing Execution Standard (PTES) lub równoważne.

Za równoważne Zamawiający uzna standardy opisujące cały przebieg procesu testowania bezpieczeństwa systemów IT oraz obszary systemowe, które muszą podlegać weryfikacji, w niemniejszym zakresie, z niemniejszą szczegółowością i systematyką wykonywania audytu niż wymienione.

1. Wymagania w zakresie realizacji audytu muszą zawierać co najmniej następujące czynności:
   1. harmonogram audytu – nie dłużej niż 30 dni kalendarzowych;
   2. ustalenie zakresu docelowego – ustalenie charakteru i zasięgu testów;
   3. gromadzenie informacji – zbieranie informacji na temat obiektu testów;
   4. mapowanie podatności – poszukiwanie podatności w elementach Systemu;
   5. docelowe wykorzystanie podatności – stworzenie wektora inicjalizującego atak, który ma na celu ominąć zabezpieczenia w celu naruszenia poufności, integralności oraz dostępności danych osobowych, przejęcia systemów, odcięcia Systemu od sieci zewnętrznej, utraty danych; zatrzymania eksploatacji Systemu, itp.
   6. eskalacja uprawnień – zwiększenie uprawnień w Systemie i przeniesienie kontroli na kolejne usługi lub systemy;
   7. zapewnienie ciągłości uzyskanego dostępu wynikającego z przełamania zabezpieczeń, w tym weryfikacja możliwości zainstalowania oprogramowania typu „tylna furtka” lub rootkit-ów, lub innego złośliwego oprogramowania;
   8. dokumentacja i raportowanie – raport powinien zawierać informacje o znalezionych podatnościach oraz zauważonych problemach;
   9. realizacja retestów (ponowna próba odnalezionych podatności pod kątem ich występowania) w terminie wskazanym przez Zamawiającego oraz sporządzenie raportu z retestu.
2. Odbiór dokumentacji (Etap VIa – KRM 1.0, Etap Vb – KRM 2.0)
3. Wykonawca przygotuje oraz stosownie zaktualizuje zgodnie z ogólnie akceptowalnymi standardami w dziedzinie dokumentowania, następujące rodzaje dokumentacji bezpośrednio związanej z przedmiotem zamówienia:
4. Dokumentację Projektu Technicznego Systemu (Projekt techniczny),
5. Dokumentację utrzymaniową,
6. Dokumentację w zakresie instrukcji użytkownika,
7. Dokumentację powykonawczą.
8. Wykonawca zobowiązuje się do opracowania każdej z wymienionych wyżej dokumentacji w języku polskim w jednym wydrukowanym egzemplarzu oraz w wersji elektronicznej w formacie doc i formacie PDF na nośniku elektronicznym.
9. Wszystkie dokumenty tworzone w ramach realizacji przedsięwzięcia charakteryzowały się będą wysoką jakością, na którą będą miały wpływ, takie czynniki jak:
10. czytelna i zrozumiała struktura zarówno poszczególnych dokumentów jak i całej dokumentacji z podziałem na rozdziały, podrozdziały i sekcje,
11. zachowanie standardów, a także sposób pisania, rozumianych jako zachowanie jednolitej i spójnej struktury, formy i sposobu prezentacji treści poszczególnych dokumentów oraz fragmentów tego samego dokumentu, jak również całej dokumentacji,
12. kompletność dokumentu, rozumiana jako pełne, bez wyraźnych, ewidentnych braków przedstawienie omawianego problemu obejmujące całość opisu rozpatrywanego zagadnienia. Oznacza to w szczególności jednoznaczne i wyczerpujące przedstawienie wszystkich zagadnień w odniesieniu do systemu,
13. spójność i niesprzeczność dokumentu, rozumianych jako zapewnienie wzajemnej zgodności pomiędzy wszystkimi rodzajami informacji umieszczonymi w dokumencie, jak i brak logicznych sprzeczności pomiędzy informacjami zawartymi we wszystkich przekazanych dokumentach oraz we fragmentach tego samego dokumentu.
14. Dokumentacja Techniczna Systemu będzie aktualizowana przez Wykonawcę odpowiednio do zmian lub modyfikacji wprowadzanych według zaleceń Zamawiającego w terminie do 14 dni kalendarzowych od wdrożenia zmian w ramach realizacji usługi rozwoju Systemu. Oznacza to, że Zamawiający wymaga, by zmiany wprowadzane w poszczególnych dokumentach były analizowane przez Wykonawcę przez pryzmat ich wpływu na zapisy innych dokumentów, a w razie ich zidentyfikowania ‑ Wykonawca zobowiązany jest do wprowadzenia wymaganych zmian we wszystkich dokumentach powiązanych.
15. Wykonawca przeniesie na Zamawiającego całość majątkowych praw autorskich do stworzonej w toku projektu dokumentacji.

**Dokumentacja utrzymaniowa:**

1. Dokumentacja utrzymaniowa, musi zawierać co najmniej:
2. procedury administracyjne,
3. procedury zabezpieczeń (backup’owe),
4. procedury awaryjne,
5. procedury użytkownika.
6. Każda z procedur wymienionych w ustępie 1, muszą zawierać, co najmniej następujące informacje:
7. identyfikator i nazwę procedury,
8. rodzaj procedury,
9. data utworzenia i zatwierdzenia oraz wersja procedury,
10. cel i zakres procedury,
11. warunki uruchomienia procedury i oczekiwany rezultat jej wykonania,
12. dane osób, które opracowały procedurę, sprawdziły, zaakceptowały i zatwierdziły,
13. działania, które występują jedno po drugim, jakie należy wykonać, aby osiągnąć postawiony cel, w tym informacja o osobie (zgodnie z zaproponowanymi rolami), która powinna wykonać dane czynności.

**Dokumentacja w zakresie instrukcji**

1. Podręczniki opracowane zostaną przez Wykonawcę dla każdej z ról przewidzianych w systemie.
2. Podręcznik może zawierać zrzuty ekranów (opatrzone krótkimi opisami tekstowymi) demonstrujące oczekiwane stany Systemu.
3. W szczególności powinny zostać dostarczone podręczniki:
4. podręcznik systemu standardowego (jeżeli taki system jest składową oferowanego rozwiązania) tj. systemu w wersji przed aplikacją w nim zmian specyficznych dla wdrożenia w organizacji Zamawiającego,
5. podręcznik dla użytkownika zgodny z wypracowaną w toku projektu koncepcją wdrożenia systemu w organizacji Zamawiającego, umożliwiający samodzielne i sprawne wykonywanie wszelkich operacji w systemie przez użytkowników.

**Dokumentacja powykonawcza:**

Dokumentację powykonawczą systemu stanowić będzie zaktualizowana dokumentacja techniczna Systemu uzupełniona o opis wykonanych w toku prac wraz z informacjami o parametrach i sposobie konfiguracji, instrukcje techniczno‑instalacyjne, instrukcje obsługi oprogramowania oraz inne dokumenty producentów, o ile zostaną one dostarczone przez Wykonawcę, a także materiały szkoleniowe w zakresie dotyczącym systemu.

W szczególności w ramach dokumentacji powykonawczej wymagana jest aktualizacja:

* 1. Projektu technicznego,
  2. diagramów ze strukturami danych,
  3. dokumentacji interfejsów systemu,
  4. kodów źródłowych i dokumentacji tych kodów.

# Szczegółowe warunki realizacji zamówienia określonego w Fazie 2

1. Świadczenia usług utrzymania i rozwoju Systemu teleinformatycznego MS

Wykonawca zobowiązuje się do świadczenia usługi utrzymania systemu (Krajowy Rejestr Mediatorów) i wsparcia Zamawiającego w okresie trzydziestu sześciu (36) miesięcy liczonych od dnia podpisania Protokołu Odbioru Systemu KRM. Serwis zostanie uruchomiony pod wdrożeniu Systemu KRM 1.0 (Etap VIIa), przy czym do czasu uruchomienia KRM 2.0 Wykonawca oszacuje i wskaże swoje wynagrodzenie z tytułu Serwisu Utrzymaniowego (Zamawiający na etapie ogłoszenia zamówienia określi udział procentowy na podstawie danych z szacowania). Uruchomienie Serwisu dla KRM 2.0 – Etap VIIb.

1. Ogólne zasady realizacji Usług:
   1. Wykonawca świadczy Usługi dla Zamawiającego oraz Użytkowników Końcowych.
   2. Usługi obejmują: (do czasu uruchomienia KRM 2.0, Usługa obejmuje wyłącznie KRM 1.0)
      1. wszystkie komponenty Systemu KRM,
      2. systemy operacyjne, w oparciu o które funkcjonuje System KRM,
      3. zadania administracji wszystkimi komponentami Systemu w Infrastrukturze systemowej,
      4. obsługę kopii zapasowych baz danych Systemu i ich odtwarzania zgodnie z procedurami tworzenia kopii zapasowych (backup),
      5. usuwanie Wad Systemu oraz skutków Wad Systemu, a także wszelkich negatywnych skutków spowodowanych korzystaniem z wadliwie działających wersji Systemu we wszystkich lokalizacjach funkcjonowania Systemu,
      6. realizację Konfiguracji Systemu we wszystkich lokalizacjach funkcjonowania Systemu,
      7. odtworzenie Systemu i przywrócenie do pełnej funkcjonalności w tym po Katastrofie (pod pojęciem Katastrofy Zamawiający rozumie uszkodzenie lub całkowite zniszczenie komponentu istniejącej Infrastruktury systemowej, kiedy do przywrócenia sprawności Systemu niezbędne są działania związane z odtwarzaniem zniszczonych zasobów sprzętowych «Wykonawca nie jest zobowiązany do dostarczenia nowej Infrastruktury sprzętowej» i danych – w zakresie związanym z Systemem),
      8. monitorowanie i rekomendowanie Zamawiającemu konieczności zainstalowania poprawek i nowych wersji, na poszczególnych elementach Systemu
   3. Realizacja Usług będzie wykonywana w sposób niezakłócający normalnego funkcjonowania Zamawiającego i Użytkowników Końcowych pomiędzy godziną 7:00 a 18:00 w Dni robocze.
   4. Wykonawca zapewnia obsługę Wad, niemożliwych do zdiagnozowania   
      i usunięcia w sposób zdalny (za pośrednictwem łącza VPN lub telefonicznie), na miejscu u Zamawiającego przez specjalistę ze strony Wykonawcy.
   5. Wykonawca zobowiązany jest przedstawiać wraz z Protokołem odbioru wsparcia technicznego i serwisu za dany miesiąc Raport zawierający informację o zamkniętych w danym miesiącu zgłoszeniach wraz z wyjaśnieniem przekroczeń czasu ich realizacji (o ile dotyczy), zgodny ze wzorem ustalonym w porozumieniu z Zamawiającym w ciągu 30 dni od dnia zawarcia Umowy.
   6. Zamawiający zastrzega sobie prawo do modyfikacji Systemu KRM przez Zamawiającego lub przez podmiot trzeci. Zamawiający każdorazowo po wprowadzeniu modyfikacji poinformuje Wykonawcę o wykonanych zmianach i przekaże aktualny kod źródłowy Systemu KRM do wdrożenia przez Wykonawcę.
   7. W trakcie realizacji Usług, Wykonawca jest uprawniony do wykorzystywania OOT, w szczególności, gdy OOT staje się trwałym składnikiem Systemu, pod warunkiem, że Zamawiający wyraził na to zgodę, co zostało uwzględnione w treści Zlecenia lub Zgłoszenia. Wykonawca zobowiązuje się i gwarantuje, że udziela Zamawiającemu, o ile zajdzie taka potrzeba, licencji lub zgody na korzystanie na wszelkie elementy OOT zapewnione przez Wykonawcę w ramach realizacji Usług. Wykonawca zobowiązuje się i gwarantuje, że udzielone Zamawiającemu licencje na używanie OOT będą obejmowały wszystkie konieczne do realizacji funkcji i celu OOT pola eksploatacji, w tym w szczególności: wprowadzanie i zapisywanie w pamięci komputerów i w sieciach multimedialnych, instalowanie i deinstalowanie, przekazywanie, przechowywanie, utrwalanie, wyświetlanie, stosowanie.
   8. Wykonawca odpowiada za optymalizację baz danych.
   9. Wykonawca przygotuje i dostarczy Zamawiającemu Plan ciągłości działania Systemu obejmujący, co najmniej:
   10. analizę BIA (*Business Impact Analysis*),
   11. analizę ryzyka,
   12. określenie działań,
   13. procedury odtworzeniowe,
   14. testy ciągłości działania,
   15. procedurę wykonywania testów,
   16. BCP (*Business continuity planning*).
   17. Wykonawca przeprowadzi co 12 miesięcy test planu ciągłości działania Systemu, przy czym pierwszy test odbędzie się w terminie nie później niż 30 dni od dnia odebrania przez Zamawiającego Planu ciągłości działania, o którym mowa w pkt 1, a działania będą prowadzone w sposób minimalizujący wpływ testu na system produkcyjny.
       1. **Rodzaje środowisk technologicznych**

Wykonawca wytworzy środowiska technologiczne w ramach niniejszego zamówienia.

Lista środowisk technologicznych może ulec poszerzeniu w wyniku realizacji Modyfikacji Systemu.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Nazwa środowiska technologicz-nego** | **Rodzaj danych** | **Wersja aplikacji** | **Dla kogo i komu służy** | **Kto zapewnia infrastrukturę** | **Kto może korzystać ze środowiska** |
| Produkcyjne | Dane produkcyjne | Wersja produkcyjna | Użytkownicy | Zamawiający | Zamawiający i Wykonawca |
| Testowe | Dane testowe  lub przeniesione z produkcji | Wersja testowa lub produkcyjna | Wsparcie Użytkowników (służy do sprawdzenia nowych wersji aplikacji, która rozwiązuje zauważone błędy) | Zamawiający | Zamawiający  i Wykonawca |
| Developerskie  Wykonawcy | Dane testowe | Wersja implementowana (programowana) przez programistów | Pracownicy Wykonawcy | Wykonawca | Wykonawca |

**2. Rodzaje i kwalifikacje Zgłoszeń oraz czas ich realizacji:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Rodzaj problemu** | **Opis** | **Priorytet** | **Czas usunięcia Wady** |
| Awaria | Zatrzymanie eksploatacji Systemu, brak dostępności lub miejsca na zasobie w Infrastrukturze centralnej, wyciek danych, utrata danych lub naruszenie ich spójności, w wyniku której niemożliwe jest prowadzenie bieżącej działalności Systemu. Za Awarie uznawane jest również jednoczesne wystąpienie szeregu Błędów Krytycznych w przypadku kiedy można wykazać, że ich wystąpienie ma ten sam skutek. | Wysoki | Do 8 godzin od Zgłoszenia przez Zamawiającego. |
| Błąd  Krytyczny | Błąd uniemożliwiający poprawne wykorzystanie Systemu lub jego istotnej funkcjonalności do realizacji procesów biznesowych. Zakłócenie pracy Systemu polegające na ograniczeniu realizacji lub uciążliwości w realizacji jednej z funkcji Systemu. Działanie Systemu prowadzące do otrzymywania błędnych wyników przetwarzania danych lub praca Systemu niezgodna z Dokumentacją.  Po udostępnieniu rozwiązania czasowego pozwalającego na realizację błędnie działającej usługi (wdrożeniu obejścia) Błąd Krytyczny staje się Błędem Niekrytycznym.  Jako Błąd Krytyczny rozumiemy również błąd mogący powodować lub powodujący przełamanie zabezpieczeń związanych z poufnością, integralnością i dostępnością Systemu i danych oraz niezgodność z Dokumentacją bezpieczeństwa, w tym w szczególności System Zarządzania Bezpieczeństwem Informacji wdrożony u Zamawiającego. | Wysoki | Do 48 godzin od Zgłoszenia przez Zamawiającego |

|  |  |  |  |
| --- | --- | --- | --- |
| Błąd  Niekrytyczny | Zakłócenie pracy Systemu mogące mieć wpływ na jego funkcjonalność, natomiast nieograniczające zdolności operacyjnych Systemu w obrębie obsługi i wspomagania procesów biznesowych, niebędące Awarią, ani Błędem Krytycznym.  Błędy drobne, błędy ergonomiczne lub kosmetyczne błędy (np. format pól, brak walidacji, literówki, błędne nazwy, konieczność zbędnych „kliknięć” w celu uzyskania pożądanego przez użytkownika rezultatu, itp.). | Średni | Do siedmiu dni roboczych od daty Zgłoszenia przez Zamawiającego |
| Konfiguracja | 1. Dostosowanie Systemu z uwagi na:    1. zmiany przepisów prawa;    2. zmiany organizacyjno - administracyjne sądów, w tym w szczególności utworzenie nowego sądu, likwidacja sądu, utworzenie nowego wydziału, likwidacja wydziału, dodanie lub usunięcie repertorium/wykazu, zmiana zakresu publikacji,    3. zmiany w środowisku teleinformatycznym Użytkownika Końcowego i Zamawiającego,    4. zmiany w konfiguracji sieci WAN w oparciu, o którą funkcjonuje System,    5. aktualizacje przeglądarek internetowych, prawidłowe wyświetlanie i funkcjonowanie na aktualnej stabilnej i jednej poprzedzającej ją wersji dla przeglądarek internetowych: Firefox, Opera, Safari, Chrome, Edge.    6. zgodność z aktualną wersją WCAG lub zastosowanie odstępstwa po uwzględnieniu przez Zamawiającego uzasadnienia,    7. błędy w interfejsie użytkownika dotyczące istniejących funkcjonalności biznesowych powodujące ograniczenie wydajności i ergonomii pracy użytkownika (m.in.: zbyt mała lub duża długość pola, nieposortowane wartości list rozwijanych, brak możliwości sortowania i filtrowania po istniejących atrybutach, korekta etykiet, korekta nazw atrybutów, korekta wartości słownikowych, złe linkowanie opcji w aplikacji, braki komunikatów, nadmiarowe komunikaty, korekta treści komunikatów, obsłużenie błędów wewnętrznych właściwym komunikatem). 2. Instalacja poprawek i nowych wersji do środowiska technologicznego Systemu. 3. Analiza i przeciwdziałanie zagrożeniom wynikającym z podatności komponentów Systemu lub systemów operacyjnych w Infrastrukturze Centralnej na cyberprzestępczość. 4. Optymalizacja funkcjonowania Systemu w uzgodnieniu z Zamawiającym, obejmująca optymalizację kodu źródłowego Systemu, systemu baz danych w Infrastrukturze Centralnej, serwerów aplikacyjnych. 5. Instalacja usług, konfigurację serwera i systemu operacyjnego, konfiguracja dostępu do lokalnych i sieciowych zasobów dyskowych, macierzy, baz danych. 6. Aktualizacja Dokumentacji i kodów źródłowych.   Obejmuje działania wyłącznie zaplanowane i związane z uruchomieniem nowych usług oraz funkcjonalności. Nie obejmuje usług utrzymania i serwisu związanego z Wadami wynikającymi z nieprzewidzianych i nieuzgodnionych zmian środowiska i plików konfiguracyjnych po stronie lokalnej w systemach zintegrowanych i po stronie centralnej, które powodują brak lub częściowy brak zasilania systemu danymi. | Niski | W terminie siedmiu Dni roboczych lub innym terminie wnioskowanym przez Wykonawcę i potwierdzonym przez Zamawiającego. |
| Wniosek o informację | Udzielenie informacji dotyczącej funkcjonowania Systemu w części lokalnej i centralnej lub dotyczącej realizacji przedmiotu Umowy | Niski | W terminie siedmiu dni roboczych lub innym terminie wnioskowanym przez Wykonawcę i potwierdzonym przez Zamawiającego. |

1. Procedura realizacji Zgłoszeń:
2. Zamawiający przewiduje następujące kanały komunikacji - za pośrednictwem:
   1. systemu zgłoszeniowego udostępnionego przez Zamawiającego (podstawowy), zwany dalej „Systemem Zgłoszeniowym”. W przypadku Zgłoszeń typu Awaria Zamawiający zastrzega sobie prawo dodatkowego opcjonalnego zgłoszenia telefonicznego lub sms-owego na całodobowy numer wskazany przez Wykonawcę;
   2. dodatkowe kanały komunikacji wykorzystywane będą po uzgodnieniu z Wykonawcą w przypadku niedostępności kanału podstawowego;
   3. Zamawiający zastrzega sobie możliwość zmiany Systemu Zgłoszeniowego w trakcie trwania Umowy.
3. Nazwy „Rodzajów problemów” mogą być podczas trwania Umowy dostosowywane do użytkowanego Systemu Zgłoszeniowego, ale nie będą powodowały zmian „Czasów usunięcia Wad” oraz określonych Opisem definicji poszczególnych rodzajów problemów.
4. Zamawiający kategoryzuje Zgłoszenia na formularzu zgłoszenia zgodnie z kwalifikacją określoną w tabeli zawierającej rodzaje kwalifikacji Zgłoszeń (pkt 2).
5. Po zmianie kategorii Zgłoszenia, jego sposób realizacji określany jest przez nową kategorię Zgłoszenia, a czas realizacji w przypadku zmiany kategorii na wyższą liczony jest od momentu poinformowania Wykonawcy o zmianie kategorii w Systemie Zgłoszeniowym.
6. Za realizację Zgłoszenia uważa się dostarczenie poprawki na środowisko technologiczne, którego dotyczy Wada, chyba, że Zamawiający w treści Zgłoszenia wskaże inne środowisko technologiczne lub Wykonawca wskaże, że wgranie poprawki wymaga okna serwisowego.
7. Wykonawca jest uprawniony do trzykrotnego zwrócenia się do Użytkownika Końcowego o udzielenie wyjaśnień. Czas odpowiedzi Użytkownika Końcowego nie jest w takim wypadku wliczany do czasu realizacji Zgłoszenia.
8. Prawidłowa realizacja Zgłoszenia, musi być odnotowana w Systemie Zgłoszeniowym. Zamawiającemu lub Użytkownikowi Końcowemu przysługuje prawo do zgłoszenia reklamacji prawidłowości rozwiązania. Czas poświęcony na weryfikację Zgłoszenia (od zamknięcia Zgłoszenia do otwarcia w wyniku reklamacji) nie jest wliczany w czas jego realizacji przez Wykonawcę. Reklamacje w zakresie prawidłowości rozwiązania Zgłoszenia mogą być zgłaszane w terminie 30 dni kalendarzowych od zamknięcia Zgłoszenia. W przypadku ponownego otwarcia Zgłoszenia w wyniku reklamacji Zamawiającego lub Użytkownika kary umowne w przypadku zwłoki Wykonawcy nalicza się w podwójnej wysokości.
9. Wykonawca zaktualizuje Dokumentację jeżeli w wyniku realizacji Zgłoszenia jest to wymagane w terminie 7 dni roboczych od zamknięcia Zgłoszenia.
10. W sytuacji kiedy rozwiązanie Zgłoszenia wymaga zainstalowania Modyfikacji Systemu, Strony ustalają w drodze porozumienia indywidualny termin realizacji Zgłoszenia. Nie dotyczy Awarii.
11. Uwagi zgłoszone przez Użytkowników Końcowych bezpośrednio do Wykonawcy, dotyczące funkcjonowania i funkcjonalności, a skutkujące Modyfikacjami Systemu, będą niezwłocznie, tj. nie później niż w ciągu 2 dni roboczych przekazywane do Zamawiającego za pośrednictwem uzgodnionego między Stronami kanału komunikacyjnego.

**Procedura zgłaszania Zamawiającemu konieczności zainstalowania poprawek i nowych wersji poszczególnych elementów Systemu KRM dla środowisk technologicznych:**

1. Wykonawca przedstawia listę poprawek do zainstalowania do każdego środowiska technologicznego. Zamawiający zawsze może żądać dodatkowego (ponad listę poprawek przedstawioną przez Wykonawcę) wykonania poprawek, lecz nie więcej niż raz na miesiąc.
2. Zamawiający wymaga, aby poprawki bezpieczeństwa systemów operacyjnych były instalowane w ciągu maksymalnie 7 dni od ich wydania przez producenta systemu operacyjnego.
3. Zamawiający w terminie 7 dni roboczych od dnia dostarczenia listy poprawek do zainstalowania informuje Wykonawcę, które ze zgłoszonych poprawek będą podlegać realizacji.
4. Wykonawca przeprowadza wdrożenie poprawek podlegających realizacji w terminie 14 dni roboczych od dnia przekazania zatwierdzenia ich przez Zamawiającego.
5. Za nieterminowe wdrożenie poprawek podlegających realizacji naliczone zostaną kary umowne jak za Błąd Niekrytyczny.
6. Z realizacji zgłoszenia poprawek Wykonawca sporządza raport zgłoszenia.
7. Usługa Modyfikacji Systemu:

Szczegółowe zasady realizacji usługi Modyfikacji Systemu oraz przygotowania dokumentów analitycznych i innych dokumentów oraz projektów zmian w Systemie.

**Zakres usługi Modyfikacje Systemu**

Usługa Modyfikacji Systemu obejmuje:

1. Modyfikacje Systemu;
2. Przygotowywanie dokumentów analitycznych i innych dokumentów oraz projektów zmian w Systemie, w tym również aktualizacja Dokumentacji, przygotowywanie opinii na temat wykorzystania w Systemie nowych technologii lub sprzętu (dalej: „Prace analityczne”).

Zamawiający może zlecić w ramach puli Roboczogodzin przeznaczonych na Modyfikacje Systemu Prace analityczne. Procedury zlecenia i odbioru Modyfikacji Systemu stosuje się odpowiednio do zlecenia i odbioru Prac analitycznych.

**Zasady realizacji usługi Modyfikacje Systemu**

1. Realizacja Usługi Modyfikacje Systemu następuje na podstawie zleceń (dalej: „Zlecenie”).
2. Dla Zlecenia i odbiór Prac analitycznych stosuje się odpowiednio zapisy dotyczące Modyfikacji.
3. Zamawiający może zlecić Wykonawcy Modyfikacje Systemu oraz Prace analityczne w okresie trwania Usługi wsparcia technicznego i serwisu. Termin realizacji danego Zlecenia nie może wykraczać poza okres obowiązywania Umowy. Jeżeli w wyniku zwłoki Wykonawcy lub z innych przyczyn niezależnych od Wykonawcy lub Zamawiającego termin realizacji Zlecenia miałby ulec wydłużeniu i być dłuższy niż okres obowiązywania Umowy, Zamawiający dokonuje odbioru Zlecenia według stanu na ostatni dzień obowiązywania Umowy i dokonuje rozliczenia z Wykonawcą w oparciu o procentowany stan zaawansowania prac oraz nalicza kary umowne w przypadkach prawem przewidzianych. W przypadkach szczególnie uzasadnionych, w szczególności, gdy do wydłużenia terminu doszło z winy Zamawiającego lub wskutek działania Siły wyższej, lub zlecona usługa Modyfikacji ma istotne znaczenie dla Zamawiającego lub Użytkowników końcowych, odbiór Modyfikacji/Prac analitycznych może nastąpić po wygaśnięciu Umowy.
4. Dla każdej Modyfikacji Wykonawca przygotowuje projekt Modyfikacji zawierający elementy wskazane przez Zamawiającego, a w przypadku Modyfikacji o pracochłonności większej niż 400 Roboczogodzin dodatkowo harmonogram realizacji Modyfikacji.
5. Modyfikacja Systemu powoduje zmianę wartości major lub minor numeru wersji Systemu oraz konieczność instalacji nowej wersji Systemu zgodnie z procedurą opisaną w OPZ. Instalacja nowej wersji Systemu następuje na środowisku (lub środowiskach) wskazanym przez Zamawiającego w Zleceniu.
6. Do odbioru Modyfikacji Wykonawca zobowiązany jest przedstawić wszystkie wymagane przez Zamawiającego produkty, w tym zaktualizowaną Dokumentację.
7. Odbiór Modyfikacji/Prac analitycznych nastąpi Protokołem Odbioru Modyfikacji.
8. Procedura zlecania Modyfikacji
9. Modyfikacje/Prace analityczne zlecane są za pośrednictwem wskazanego przez Zamawiającego Systemu Zgłoszeniowego (kanał podstawowy). Dodatkowe kanały komunikacji wykorzystywane będą po uzgodnieniu z Wykonawcą tylko i wyłącznie w przypadku niedostępności kanału podstawowego.
10. Komunikacja Stron w zakresie realizacji Usługi Modyfikacja (dla Modyfikacji/Prac analitycznych) odbywa się w formie dokumentowej (w tym również oświadczenia Zamawiającego w zakresie akceptacji lub odrzucenia.
11. Procedura zgłaszania Zleceń Modyfikacji:
12. Zamawiający rejestruje w Systemie Zgłoszeniowym zgłoszenie wykonania usługi Modyfikacji wraz z podaniem wymagań oraz ewentualnie pożądanym terminem realizacji (dalej „Zlecenie”). Zamawiający w Zlecenie określa na jakim środowisku technologicznym nastąpi odbiór nowej wersji Systemu. Zamawiający może też wskazać szacowaną przez niego liczbę Roboczogodzin potrzebnych na realizację prac.
13. W ramach Zlecenia Modyfikacji Zamawiający może zażądać od Wykonawcy, co zostanie uwzględnione w treści Zlecenia, dodatkowo zestawu wymagań biznesowych oraz przypadków testowych z odpowiednią matrycą pokrycia wymagań przypadkami testowymi. Zarówno wymagania, jak i przypadki testowe zostaną dostarczone przez Wykonawcę w formacie umożliwiającym ich import do narzędzia wskazanego przez Zamawiającego; testy manualne i automatyczne.
14. W odpowiedzi Wykonawca przedstawia Projekt Techniczny Modyfikacji (dalej „PTM”), w którym szczegółowo określa w szczególności termin realizacji Modyfikacji, szacowaną liczbę Roboczogodzin, zakres koniecznych zmian w Systemie oraz zakres niezbędnej Dokumentacji do wykonania/uzupełnienia. W przypadku realizacji usługi Prace analityczne Wykonawca określa szacowaną liczbę Roboczogodzin oraz zakres niezbędnej Dokumentacji do wykonania/uzupełnienia.
15. Od momentu przedstawienia Zlecenia Wykonawca zobowiązany jest w terminie wskazanym przez Zamawiającego, nie krótszym niż 3 dni robocze, przedstawić PTM, przy czym termin wykonania Modyfikacji powinien uwzględniać również czas potrzebny do przygotowania projektu Modyfikacji, harmonogramu realizacji Modyfikacji jeżeli jest wymagany, przeprowadzenia testów Modyfikacji oraz procedurę odbiorową. Zamawiający ma prawo wyznaczyć Wykonawcy ostateczny termin przedstawienia PTM, w przypadku naruszenia którego, zostaną naliczone stosowne kary umowne zgodnie z postanowieniami Umowy.
16. Zamawiający zastrzega sobie prawo żądania szczegółowych wyjaśnień do przedstawionej wyceny pracochłonności oraz sposobu implementacji. Wykonawca zobowiązany jest do przedstawienia wyjaśnień w następnym Dniu Roboczym po otrzymaniu żądania. Na uzasadniony wniosek Wykonawcy termin ten może zostać wydłużony.
17. Strony ustalają w drodze porozumienia ostateczną pracochłonność   
    i termin wykonania Modyfikacji. W przypadku braku porozumienia, po dwukrotnej nieudanej próbie uzgodnienia pomiędzy Stronami, Zamawiający ma prawo wybrać podmiot zewnętrzny, który dokona oceny pracochłonności z uwzględnieniem proponowanego terminu wykonania i zakresu Dokumentacji. Strony przyjmą tak określoną pracochłonność   
    i termin, a koszty dokonania wyceny i opracowania opinii przez podmiot zewnętrzny pokryją w równych częściach Zamawiający i Wykonawca.
18. Zamawiający w terminie nie dłuższym niż 14 dni roboczych potwierdza Zlecenie Modyfikacji lub rezygnuje z niego. Brak odpowiedzi Zamawiającego uznać należy za bezterminowe zawieszenie realizacji Modyfikacji.
19. W przypadku rezygnacji ze Zlecenia Modyfikacji lub bezterminowego zawieszenia realizacji Modyfikacji za wykonane przez Wykonawcę czynności Strony rozliczają jak za usługę Prace analityczne, przy czym maksymalna kwota wynagrodzenia nie może być wyższa niż 20% szacowanej pracochłonności realizacji danej Modyfikacji.
20. Potwierdzenie Zlecenia Modyfikacji Systemu oznacza uzgodnienie przez Strony zakresu oraz terminu wykonania Modyfikacji, jej pracochłonności, wymaganej Dokumentacji oraz kryteriów jakościowych. Datą od której jest liczony termin realizacji Modyfikacji jest data potwierdzenia Zlecenia w Systemie Zgłoszeniowym. Na uzasadniony wniosek Wykonawcy termin realizacji Modyfikacji może zostać wydłużony. Zamawiający może również wstrzymać wykonanie Modyfikacji ze względu na pojawienie się innych priorytetowych Modyfikacji. Zamawiający może zrezygnować z dalszej realizacji Modyfikacji w przypadku ustania potrzeby wykonania tej Modyfikacji, a rozliczenie Modyfikacji nastąpi na podstawie wykonanych i odebranych prac.
21. Po potwierdzeniu Zlecenia przez Zamawiającego, ale przed przystąpieniem do wykonania Modyfikacji Systemu, Wykonawca przedstawia Zamawiającemu do akceptacji projekt Modyfikacji z elementami wskazanymi przez Zamawiającego. Zamawiający dokona akceptacji projektu Modyfikacji lub zgłosi uwagi w terminie nie dłuższym niż 7 dni roboczych od dnia przedstawienia projektu. W przypadku zgłoszenia uwag, Wykonawca przedstawi ponownie projekt do akceptacji w terminie nie dłuższym niż 2 dni robocze.
22. W przypadku oszacowania Modyfikacji, której oszacowana pracochłonność przekraczająca 400 Roboczogodzin przed przystąpieniem do wykonania Modyfikacji Wykonawca oprócz projektu Modyfikacji przedstawia harmonogram realizacji Modyfikacji obejmujący wszystkie etapy realizacji z rozpisanymi zadaniami oraz wyszczególnionymi produktami i liczbą Roboczogodzin na poziomie zadań, który na żądanie Zamawiającego zostanie również przedstawiony za pomocą wykresu Gantta. W przypadku, gdy produkcyjne uruchomienie Modyfikacji będzie uzasadniało zwiększenie nakładów Wykonawcy na świadczenie Usługi wsparcia technicznego i serwisu Wykonawca przedkłada do Zamawiającego wniosek wraz z uzasadnieniem, przy czym jednorazowy wzrost miesięcznego ryczałtu nie może być wyższy niż 10% wartości Modyfikacji ustalonej między Stronami w Zleceniu. W przypadku, gdy produkcyjne uruchomienie Modyfikacji będzie uzasadniało zwiększenie nakładów Wykonawcy na świadczenie Usługi wsparcia technicznego i serwisu Wykonawca przedkłada do Zamawiającego wniosek wraz z uzasadnieniem, przy czym jednorazowy wzrost miesięcznego ryczałtu nie może być wyższy niż 10% wartości Modyfikacji ustalonej między Stronami w Zleceniu. Zamawiający dokona akceptacji harmonogramu realizacji Modyfikacji lub zgłosi uwagi w terminie nie dłuższym niż 15 dni roboczych od dnia przedstawienia harmonogramu. W przypadku zgłoszenia uwag, Wykonawca przedstawi ponownie harmonogram do akceptacji w terminie nie dłuższym niż 5 dni Roboczych.
23. Na uzasadniony wniosek Wykonawcy terminy wskazane w lit. j-k mogą zostać wydłużone.
24. Wykonawca przystępuje do wykonania Modyfikacji po akceptacji przez Zamawiającego projektu Modyfikacji/ harmonogramu realizacji Modyfikacji. Projekt Modyfikacji/harmonogram realizacji Modyfikacji podlegają na bieżąco aktualizacji zgodnie z procedurą powyżej.
25. Na każdym etapie realizacji Strony mogą w drodze porozumienia dokonać stosownej aktualizacji Zlecenia w Systemie Zgłoszeniowym, w tym wydłużyć termin realizacji, zwiększyć ilość Roboczogodzin oraz zmienić kryteria jakościowe Modyfikacji.
26. Procedura odbioru Modyfikacji
27. Procedura odbioru Modyfikacji:
28. W przypadku usługi Prace analityczne, akceptacja przez Zamawiającego przygotowanych przez Wykonawcę dokumentów stanowi podstawę do odbioru i zamknięcia Zgłoszenia.
29. W przypadku wykonania Modyfikacji, Wykonawca przedstawia Zamawiającemu nową wersję Systemu wraz z Dokumentacją oraz raport z testów Wykonawcy
30. Zamawiający w terminie do 14 dni roboczych weryfikuje przekazaną wersję sprawdzając, czy zostały uwzględnione wymagania określone w Zleceniu oraz w zaakceptowanym przez Zamawiającego projekcie Modyfikacji/harmonogramie realizacji Modyfikacji, a także czy przekazana wersja nie zawiera Wad, a Dokumentacja jest kompletna i spełnia kryteria jakościowe.
31. Wyniki weryfikacji Zamawiający przekazuje Wykonawcy drogą elektroniczną, w szczególności w postaci raportu z testowania wersji.
32. W przypadku zgłoszenia zastrzeżeń przez Zamawiającego względem dostarczonej Modyfikacji, Wykonawca dokona stosownych poprawek. Po ponownym dostarczeniu przez Wykonawcę Modyfikacji zostanie przeprowadzony jej odbiór zgodnie z procedurą opisaną w lit. b – d.
33. W przypadku spełnienia warunków określonych w Zleceniu oraz braku Wad Zamawiający dokonuje odbioru Modyfikacji.
34. Prawidłowość wykonania Modyfikacji zostanie potwierdzona podpisanym bez zastrzeżeń przez obie Strony Protokołem Odbioru Modyfikacji.
35. W przypadku, gdy Modyfikacja została zainstalowana na innym środowisku niż produkcyjne na zlecenie Zamawiającego w terminie przez niego wskazanym Wykonawca dokona instalacji Modyfikacji na środowisku wskazanym przez Zamawiającego. W przypadku zwłoki Wykonawcy Zamawiający naliczy kary umowne jak za Błąd Niekrytyczny.
36. Wynagrodzenie Wykonawcy za wykonanie Modyfikacji lub za Prace analityczne będzie stanowić iloczyn faktycznie wykorzystanej liczby Roboczogodzin, potwierdzonej przez Zamawiającego, i wynagrodzenia brutto za jedną Roboczogodzinę Modyfikacji.
37. Po dokonaniu odbioru Modyfikacji Zamawiający zamyka Zgłoszenie w Systemie Zgłoszeniowym.

**Procedura autoryzacji Modyfikacji wykonanych przez Zamawiającego lub osoby trzecie działające w jego imieniu**

1. Zamawiający przedstawia Wykonawcy propozycję wykonania modyfikacji przez Zamawiającego lub osoby trzecie działające w jego imieniu (dalej: „Modyfikacja Zewnętrzna” lub „MZ”).
2. Wykonawca ma prawo w terminie 3 dni roboczych zgłosić uwagi do przedstawionej propozycji MZ.
3. Zamawiający może uwzględnić lub odrzucić uwagi Wykonawcy i zaproponowany sposób odbioru MZ.
4. Zamawiający lub osoby trzecie wykonuje/ją MZ.
5. Wykonawca instaluje MZ na środowisku testowym w terminie 1 dnia roboczego od przedstawienia jej przez Zamawiającego.
6. Zamawiający przeprowadza testy odbiorowe.
7. Jeśli Wykonawca uzna, iż przeprowadzone przez Zamawiającego testy nie są wystarczające, wówczas przeprowadza własne testy weryfikujące (na swój koszt) w terminie do 14 dni roboczych.
8. Pozytywny wynik weryfikacji jest równoznaczny z autoryzacją przez Wykonawcę MZ.
9. Jeśli wynik weryfikacji jest negatywny Wykonawca przedstawia Zamawiającemu wszystkie istotne powody, które składają się na ten wynik w terminie 1 dnia roboczego liczonego od dnia zakończenia testów weryfikujących przez Wykonawcę, o których mowa w pkt 7. Zamawiający ma prawo zadecydować czy MZ będzie wdrożona czy poprawiona. Zamawiający przekazuje Wykonawcy informację o podjętej decyzji. Polecenie wdrożenia MZ jest równoznaczne z autoryzacją przez Wykonawcę przedmiotowej MZ.
10. Wykonawca instaluje MZ na środowisku produkcyjnym w terminie wskazanym przez Zamawiającego.

**Procedura instalacji nowej wersji Systemu:**

1. Każdorazowo w przypadku powstania nowej wersji Systemu, jej instalacja na środowisku technologicznym następuje na zlecenie Zamawiającego na zasadach wskazanych w OPZ.
2. Wykonawca będzie prowadził ewidencję dostarczanych wersji Systemu, zawierającą:
   1. nazwa podsystemu
   2. numer wersji,
   3. datę wydania wersji,
   4. datę instalacji na środowiskach technologicznych,
   5. skrótowy opis zmian, które wersja uwzględnia, z odwołaniem do Zlecenia lub Zgłoszenia,
   6. ewentualne uwagi.
3. Wykonawca uzupełnia i przedstawia ewidencję, o której mowa w pkt 2 niezwłocznie po wydaniu nowej wersji (poprzez kanał uzgodniony w porozumieniu z Zamawiającym).
4. Na żądanie Zamawiającego Wykonawca przedstawi pakiet obejmujący kody źródłowe Systemu oraz instrukcję kompilacji i konsolidacji poszczególnych elementów Oprogramowania, a także wszystkie elementy dodatkowe służące kompilacji i konsolidacji, z uwzględnieniem wszystkich etapów tworzenia Oprogramowania na założonej linii technologicznej i udzieli odpowiedzi na ewentualne pytania Zamawiającego dotyczących sposobu kompilacji i uruchomienia przekazanych kodów.
5. Dystrybucja nowych wersji Systemu następuje według następującej procedury:
6. Wykonawca przekazuje kody źródłowe kanałem elektronicznym do repozytorium kodów źródłowych Zamawiającego lub jeżeli nie jest to możliwe w inny sposób zatwierdzony przez Zamawiającego,
7. Wykonawca instaluje nową wersję Systemu skompilowaną na ustalonym środowisku technologicznym i w terminach ustalonych z Zamawiającym.
8. Wraz z nową wersją Wykonawca zobowiązany jest dostarczyć Dokumentację wynikającą ze zmian w Systemie zrealizowanych przez Wykonawcę (aktualizacja Dokumentacji).
9. Zamawiający zastrzega sobie prawo do dokonywania zmian w Systemie przez inne podmioty niż Wykonawca działające na zlecenie Zamawiającego. W wypadku, gdy nowa wersja Systemu powstała na skutek wprowadzenia zmian w Systemie przez podmiot inny niż Wykonawca, Wykonawca na polecenie Zamawiającego dokonuje dystrybucji wersji zgodnie z pkt 5.

**Dokumentacja:**

1. Wykonawca zaktualizuje Dokumentację zgodnie z zaakceptowanymi przez Zamawiającego standardami w dziedzinie dokumentowania.
2. Wykonawca zobowiązuje się do opracowania Dokumentacji w języku polskim w wersji elektronicznej w formacie DOCX i formacie PDF w przypadku dokumentów tekstowych oraz innych formatach w przypadku diagramów oraz schematów drogą elektroniczną.
3. Wszystkie dokumenty, tworzone w ramach realizacji przedsięwzięcia, będą charakteryzowały się wysoką jakością, na którą będą miały wpływ, takie czynniki jak:
   1. Czytelna i zrozumiała struktura zarówno poszczególnych dokumentów jak i całej Dokumentacji z podziałem na rozdziały, podrozdziały i sekcje.
   2. Zachowanie standardów, a także sposób pisania, rozumianych jako zachowanie jednolitej i spójnej struktury, formy i sposobu prezentacji treści poszczególnych dokumentów oraz fragmentów tego samego dokumentu, jak również całej dokumentacji.
   3. Kompletność dokumentu, rozumiana jako pełne, bez wyraźnych, ewidentnych braków przedstawienie omawianego problemu obejmujące całość z danego zakresu rozpatrywanego zagadnienia. Oznacza to w szczególności jednoznaczne i wyczerpujące przedstawienie wszystkich zagadnień w odniesieniu do Systemu KRM.
   4. Spójność i niesprzeczność dokumentu, rozumianych jako zapewnienie wzajemnej zgodności pomiędzy wszystkimi rodzajami informacji umieszczonymi w dokumencie, jak i brak logicznych sprzeczności pomiędzy informacjami zawartymi we wszystkich przekazanych dokumentach oraz we fragmentach tego samego dokumentu.
4. W przypadku zmian w Systemie KRM wynikających z instalacji nowych wersji na skutek naprawy Wad lub Usług modyfikacji, Wykonawca dokona aktualizacji dokumentacji Systemu KRM.
5. Cała dokumentacja, o której mowa powyżej, podlegała będzie akceptacji Zamawiającego.
6. Szczegółowe zasady realizacji usługi gwarancyjnej:
7. Zakres usługi gwarancji obejmuje wszystkie wykryte podczas eksploatacji Systemu Wady.
8. W zakresie klasyfikacji Błędów Systemu, ewidencji Zgłoszeń, procedur odbioru, czasu realizacji zgłoszeń, odbioru usług, naliczania kar umownych mają zastosowanie postanowienie OPZ i Umowy.
9. W przypadku zmian w Systemie wynikających z instalacji nowych wersji na skutek naprawy Błędów lub Modyfikacji, Wykonawca dokona na żądanie Zamawiającego aktualizacji Dokumentacji.

**Tabela 1. Harmonogram Ramowy realizacji Przedmiotu Zamówienia**

**Harmonogram realizacji projektu**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Harmonogram realizacji projektu od momentu zawarcia umowy** | | | | | | | | | | | | | | | | |  |  |
|  | **Liczba miesięcy** | | | | | | | | | | | | | | | | | |
| **Etap** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | **11** | **12** | **13** | **14** | **15** | **16** | **17** | **18** |
| **Etap I**. Analiza przedwdrożeniowa (dotyczy **KRM 1.0 i KRM 2.0**). |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **Etap II a.** Wytworzenie i wdrożenie Systemu **KRM 1.0** na środowisku testowym. |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **Etap III a.** Wdrożenie Systemu **KRM 1.0** na środowiskach przedprodukcyjnym i produkcyjnym. System działający na środowisku przedprodukcyjnym i produkcyjnym zgodny z wymaganiami. |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **Etap VIIa.** Serwis utrzymaniowy |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **Etap Va**. Audyt bezpieczeństwa |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **Etap VI a.** W zakresie KRM 1.0 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **Etap II b.** Wytworzenie i wdrożenie Systemu KRM 2.0 na środowisku testowym |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **Etap IV b.** Przeprowadzenie szkoleń dla Administratorów i Użytkowników Kluczowych w zakresie **KRM 2.0** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **Etap IV b.** Szkolenia e- learningowe (**KRM 1.0**  i **KRM 2.0**) |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **Etap III b.** Wdrożenie systemu **KRM 2.0** na środowisku produkcyjnym i uruchomienie systemu |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **Etap Vb** Audyt bezpieczeństwa |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **Etap VIIb.** Serwis Utrzymaniowy |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

1. Zarządzanie realizacją przedmiotu zamówienia
2. Wykonawca odpowiedzialny jest za zarządzanie i koordynację prac zespołu Wykonawcy oraz koordynację współdziałania swojego zespołu z zespołem Zamawiającego w realizacji zobowiązań umownych. Dobór metod i technik pracy właściwych dla efektywnej realizacji przedmiotu zamówienia leży po stronie Wykonawcy, przy czym podlega on akceptacji Zamawiającego.
3. Wykonawca zobowiązany jest do realizacji prac inicjujących projekt obejmujących co najmniej organizację spotkania otwierającego projekt w siedzibie Zamawiającego w terminie nie późniejszym niż 20 dni kalendarzowych od zawarcia Umowy – celem spotkania jest dokonanie niezbędnych uzgodnień realizacyjnych. W trakcie spotkania inicjującego przedstawi co najmniej:
4. skład personelu kluczowego do realizacji Umowy zgodny z warunkami udziału,
5. opis struktury organizacyjnej zespołu Wykonawcy,
6. plan komunikacji pomiędzy stronami, zawierający kanały komunikacji oraz wykaz osób do kontaktu w poszczególnych zakresach tematycznych,
7. rejestr wymagań względem Wykonawcy,
8. harmonogram realizacji prac objętych rygorem terminu,
9. zagadnienia do ustalenia pomiędzy stronami,
10. sposób realizacji kluczowych elementów umowy (monitorowanie, modyfikacje, wdrożenie zmian, zarządzanie jakością, testowanie, dokumentacja),
11. pytania do Zamawiającego.
12. Wykonawca zobowiązany jest do organizowania cyklicznych spotkań przedstawicieli Personelu Podstawowego z zespołem utrzymaniowym Zamawiającego (nie rzadziej niż raz na tydzień w wymiarze 1-2h) w drodze wideokonferencji przy wykorzystaniu systemu udostępnionego w tym celu Wykonawcy przez Zamawiającego. O konieczności wyznaczenia spotkania oraz o terminie decyduje Zamawiający. Zamawiający wskazuje Wykonawcy członków Personelu Podstawowego, którzy są zobowiązani do wzięcia udziału w danym spotkaniu. Zamawiający może odstąpić od wyznaczenia spotkania. Wykonawca może wnioskować o wyznaczenie, odwołanie spotkania lub zmianę terminu. Wykonawca sporządzi i dostarczy Zamawiającemu w ciągu - 2 dni roboczych notatkę ze spotkania cyklicznego.
13. Na 6 miesięcy przed końcem Umowy Wykonawca przygotuje i przekaże Zamawiającemu szczegółową agendę zagadnień koniecznych do transferu wiedzy z poszczególnych obszarów utrzymania Systemu.
14. W ostatnim miesiącu trwania Umowy Wykonawca zobowiązany jest do transferu wiedzy Zamawiającemu lub wskazanemu przez niego podmiotowi, polegającego na:
15. odbyciu maksymalnie dziesięciu spotkań w drodze wideokonferencji lub w siedzibie Zamawiającego (według wyboru Zamawiającego, przy czym w siedzibie Zamawiającego nie więcej niż cztery spotkania), w terminach wskazanych przez Zamawiającego, trwających według potrzeb Zamawiającego (nie dłużej jednak niż 8 godzin w ciągu dnia), z udziałem członków Personelu Podstawowego wskazanych przez Zamawiającego;
16. udzielenia konsultacji i odpowiedzi na pytania lub zagadnienia przedstawione przez Zamawiającego lub przez wskazany przez niego podmiot, w terminie nie później niż dwóch Dni roboczych od dnia zgłoszenia za pośrednictwem wskazanego przez Zamawiającego kanału takiego żądania przez Zamawiającego lub wskazany przez niego podmiot.

Od Wykonawcy wymaga się:

1. sprawnej i terminowej realizacji zadania oraz współpracy z Zamawiającym,
2. wyznaczenia osoby do kontaktów roboczych z Zamawiającym;
3. konsultowania i informowania o stanie prac, pojawiających się problemach i innych zagadnieniach istotnych dla realizacji badania;
4. na spotkaniach z Zamawiającym wymagany jest każdorazowo udział osoby koordynującej pracę Zespołu Wykonawcy;
5. zagwarantowania dyspozycyjności i dostępności w pracach podejmowanych w ramach wykonania zadania wszystkich ekspertów, którzy wejdą w skład zespołu Wykonawcy.

W ofercie Wykonawca ma obowiązek wskazać cenę całkowitą oraz ceny cząstkowe realizacji zamówienia w podziale na zadania.

1. Kary umowne
2. W przypadku odstąpienia od Umowy lub jej wypowiedzenia przez Wykonawcę z przyczyn nieleżących po stronie Zamawiającego, bądź odstąpienia od Umowy lub jej wypowiedzenia przez Zamawiającego z przyczyn leżących po stronie Wykonawcy, Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 10% całkowitego wynagrodzenia brutto.
3. W przypadku naruszenia postanowień Umowy dotyczących poufności Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 5% całkowitego wynagrodzenia brutto za każde stwierdzone naruszenie.
4. W przypadku niedotrzymania przez Wykonawcę terminów usunięcia Awarii lub Błędów (w tym w ramach realizacji obowiązków Wykonawcy wynikających z rękojmi lub gwarancji) Wykonawca zapłaci Zamawiającemu karę umowną:
5. w wysokości 0,2% całkowitego wynagrodzenia brutto za każdą rozpoczętą godzinę zwłoki (maksymalnie łącznie 10% całkowitego wynagrodzenia brutto) w usunięciu Awarii lub Błędu Krytycznego;
6. w wysokości 0,1% całkowitego wynagrodzenia brutto za każdy rozpoczęty dzień zwłoki (maksymalnie łącznie 5% całkowitego wynagrodzenia brutto) w usunięciu Błędu Niekrytycznego.
7. Zamawiający może potrącić karę umowną z wynagrodzenia Wykonawcy lub z zabezpieczenia należytego wykonania Umowy, na co Wykonawca wyraża zgodę i do czego upoważnia Zamawiającego bez potrzeby uzyskania pisemnego potwierdzenia lub wystawić notę obciążeniową.
8. Zamawiającemu przysługuje prawo dochodzenia na zasadach ogólnych odszkodowania przewyższającego wysokość zastrzeżonych kar umownych.
9. Kary umowne mogą być naliczane niezależnie od siebie i podlegają sumowaniu.
10. Odstąpienie od umowy lub jej wypowiedzenie przez którąkolwiek ze Stron nie powoduje utraty prawa przez Zamawiającego do kar umownych należnych na podstawie postanowień umowy.

Załączniki do OPZ:

Załącznik 1.- Testy aplikacji WWW według standardu OWASP ASVS 4.

Załącznik 1 do OPZ

**Testy aplikacji WWW według standardu OWASP ASVS 4.0 Level 1 – Greybox (bez dostępu do systemu operacyjnego i kodu źródłowego )**

1. Verify that user set passwords are at least 12 characters in length. ([C6](<https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab=Formal_Numbering)>)
2. Verify that there are no periodic credential rotation or password history requirements.
3. Verify that "paste" functionality, browser password helpers, and external password managers are permitted.
4. Verify that the user can choose to either temporarily view the entire masked password, or temporarily view the last typed character of the password on platforms that do not have this as native functionality.
5. Verify that passwords 64 characters or longer are permitted. ([C6](<https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab=Formal_Numbering)>)
6. Verify that passwords can contain spaces and truncation is not performed. Consecutive multiple spaces MAY optionally be coalesced. ([C6](<https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab=Formal_Numbering)>)
7. Verify that Unicode characters are permitted in passwords. A single Unicode code point is considered a character, so 12 emoji or 64 kanji characters should be valid and permitted.
8. Verify users can change their password.
9. Verify that password change functionality requires the user's current and new password.
10. Verify that passwords submitted during account registration, login, and password change are checked against a set of breached passwords either locally (such as the top 1,000 or 10,000 most common passwords which match the system's password policy) or using an external API. If using an API a zero knowledge proof or other mechanism should be used to ensure that the plain text password is not sent or used in verifying the breach status of the password. If the password is breached, the application must require the user to set a new non-breached password. ([C6](<https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab=Formal_Numbering)>)
11. Verify that a password strength meter is provided to help users set a stronger password.
12. Verify that there are no password composition rules limiting the type of characters permitted. There should be no requirement for upper or lower case or numbers or special characters. ([C6](<https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab=Formal_Numbering)>)
13. Verify that anti-automation controls are effective at mitigating breached credential testing, brute force, and account lockout attacks. Such controls include blocking the most common breached passwords, soft lockouts, rate limiting, CAPTCHA, ever increasing delays between attempts, IP address restrictions, or risk-based restrictions such as location, first login on a device, recent attempts to unlock the account, or similar. Verify that no more than 100 failed attempts per hour is possible on a single account.
14. Verify that the use of weak authenticators (such as SMS and email) is limited to secondary verification and transaction approval and not as a replacement for more secure authentication methods. Verify that stronger methods are offered before weak methods, users are aware of the risks, or that proper measures are in place to limit the risks of account compromise.
15. Verify that secure notifications are sent to users after updates to authentication details, such as credential resets, email or address changes, logging in from unknown or risky locations. The use of push notifications - rather than SMS or email - is preferred, but in the absence of push notifications, SMS or email is acceptable as long as no sensitive information is disclosed in the notification.
16. Verify system generated initial passwords or activation codes SHOULD be securely randomly generated, SHOULD be at least 6 characters long, and MAY contain letters and numbers, and expire after a short period of time. These initial secrets must not be permitted to become the long term password.
17. Verify that a system generated initial activation or recovery secret is not sent in clear text to the user. ([C6](<https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab=Formal_Numbering)>)
18. Verify password hints or knowledge-based authentication (so-called "secret questions") are not present.
19. Verify password credential recovery does not reveal the current password in any way. ([C6](<https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab=Formal_Numbering)>)
20. Verify shared or default accounts are not present (e.g. "root", "admin", or "sa").
21. Verify that if an authentication factor is changed or replaced, that the user is notified of this event.
22. Verify forgotten password, and other recovery paths use a secure recovery mechanism, such as TOTP or other soft token, mobile push, or another offline recovery mechanism. ([C6](<https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab=Formal_Numbering)>)
23. Verify that clear text out of band (NIST "restricted") authenticators, such as SMS or PSTN, are not offered by default, and stronger alternatives such as push notifications are offered first.
24. Verify that the out of band verifier expires out of band authentication requests, codes, or tokens after 10 minutes.
25. Verify that the out of band verifier authentication requests, codes, or tokens are only usable once, and only for the original authentication request.
26. Verify that the out of band authenticator and verifier communicates over a secure independent channel.
27. Verify that time-based OTPs have a defined lifetime before expiring.
28. Verify the application never reveals session tokens in URL parameters or error messages.
29. Verify the application generates a new session token on user authentication. ([C6](<https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab=Formal_Numbering)>)
30. Verify that session tokens possess at least 64 bits of entropy. ([C6](<https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab=Formal_Numbering)>)
31. Verify the application only stores session tokens in the browser using secure methods such as appropriately secured cookies (see section 3.4) or HTML 5 session storage.
32. Verify that logout and expiration invalidate the session token, such that the back button or a downstream relying party does not resume an authenticated session, including across relying parties. ([C6](<https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab=Formal_Numbering)>)
33. Verify that cookie-based session tokens have the 'Secure' attribute set. ([C6](<https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab=Formal_Numbering)>)
34. Verify that cookie-based session tokens have the 'HttpOnly' attribute set. ([C6](<https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab=Formal_Numbering)>)
35. Verify that cookie-based session tokens utilize the 'SameSite' attribute to limit exposure to cross-site request forgery attacks. ([C6](<https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab=Formal_Numbering)>)
36. Verify that cookie-based session tokens use "\_\_Host-" prefix (see references) to provide session cookie confidentiality.
37. Verify that if the application is published under a domain name with other applications that set or use session cookies that might override or disclose the session cookies, set the path attribute in cookie-based session tokens using the most precise path possible. ([C6](<https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab=Formal_Numbering)>)
38. Verify the application ensures a valid login session or requires re-authentication or secondary verification before allowing any sensitive transactions or account modifications.
39. Verify that the application enforces access control rules on a trusted service layer, especially if client-side access control is present and could be bypassed.
40. Verify that all user and data attributes and policy information used by access controls cannot be manipulated by end users unless specifically authorized.
41. Verify that the principle of least privilege exists - users should only be able to access functions, data files, URLs, controllers, services, and other resources, for which they possess specific authorization. This implies protection against spoofing and elevation of privilege. ([C7](<https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab=Formal_Numbering)>)
42. Verify that the principle of deny by default exists whereby new users/roles start with minimal or no permissions and users/roles do not receive access to new features until access is explicitly assigned.  ([C7](<https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab=Formal_Numbering)>)
43. Verify that access controls fail securely including when an exception occurs. ([C10](<https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab=Formal_Numbering)>)
44. Verify that sensitive data and APIs are protected against direct object attacks targeting creation, reading, updating and deletion of records, such as creating or updating someone else's record, viewing everyone's records, or deleting all records.
45. Verify that the application or framework enforces a strong anti-CSRF mechanism to protect authenticated functionality, and effective anti-automation or anti-CSRF protects unauthenticated functionality.
46. Verify administrative interfaces use appropriate multi-factor authentication to prevent unauthorized use.
47. Verify that directory browsing is disabled unless deliberately desired. Additionally, applications should not allow discovery or disclosure of file or directory metadata, such as Thumbs.db, .DS\_Store, .git or .svn folders.
48. Verify that the application has defenses against HTTP parameter pollution attacks, particularly if the application framework makes no distinction about the source of request parameters (GET, POST, cookies, headers, or environment variables).
49. Verify that frameworks protect against mass parameter assignment attacks, or that the application has countermeasures to protect against unsafe parameter assignment, such as marking fields private or similar. ([C5](<https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab=Formal_Numbering)>)
50. Verify that all input (HTML form fields, REST requests, URL parameters, HTTP headers, cookies, batch files, RSS feeds, etc) is validated using positive validation (whitelisting). ([C5](<https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab=Formal_Numbering)>)
51. Verify that structured data is strongly typed and validated against a defined schema including allowed characters, length and pattern (e.g. credit card numbers or telephone, or validating that two related fields are reasonable, such as checking that suburb and zip/postcode match). ([C5](<https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab=Formal_Numbering)>)
52. Verify that URL redirects and forwards only allow whitelisted destinations, or show a warning when redirecting to potentially untrusted content.
53. Verify that all untrusted HTML input from WYSIWYG editors or similar is properly sanitized with an HTML sanitizer library or framework feature. ([C5](<https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab=Formal_Numbering)>)
54. Verify that unstructured data is sanitized to enforce safety measures such as allowed characters and length.
55. Verify that the application sanitizes user input before passing to mail systems to protect against SMTP or IMAP injection.
56. Verify that the application avoids the use of eval() or other dynamic code execution features. Where there is no alternative, any user input being included must be sanitized or sandboxed before being executed.
57. Verify that the application protects against template injection attacks by ensuring that any user input being included is sanitized or sandboxed.
58. Verify that the application protects against SSRF attacks, by validating or sanitizing untrusted data or HTTP file metadata, such as filenames and URL input fields, use whitelisting of protocols, domains, paths and ports.
59. Verify that the application sanitizes, disables, or sandboxes user-supplied SVG scriptable content, especially as they relate to XSS resulting from inline scripts, and foreignObject.
60. Verify that the application sanitizes, disables, or sandboxes user-supplied scriptable or expression template language content, such as Markdown, CSS or XSL stylesheets, BBCode, or similar.
61. Verify that output encoding is relevant for the interpreter and context required. For example, use encoders specifically for HTML values, HTML attributes, JavaScript, URL Parameters, HTTP headers, SMTP, and others as the context requires, especially from untrusted inputs (e.g. names with Unicode or apostrophes, such as ねこ or O'Hara). ([C4](<https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab=Formal_Numbering)>)
62. Verify that the application protects against XPath injection or XML injection attacks. ([C4](<https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab=Formal_Numbering)>)
63. Verify that output encoding preserves the user's chosen character set and locale, such that any Unicode character point is valid and safely handled. ([C4](<https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab=Formal_Numbering)>)
64. Verify that context-aware, preferably automated - or at worst, manual - output escaping protects against reflected, stored, and DOM based XSS. ([C4](<https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab=Formal_Numbering)>)
65. Verify that data selection or database queries (e.g. SQL, HQL, ORM, NoSQL) use parameterized queries, ORMs, entity frameworks, or are otherwise protected from database injection attacks. ([C3](<https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab=Formal_Numbering)>)
66. Verify that where parameterized or safer mechanisms are not present, context-specific output encoding is used to protect against injection attacks, such as the use of SQL escaping to protect against SQL injection. ([C3, C4](<https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab=Formal_Numbering)>)
67. Verify that the application projects against JavaScript or JSON injection attacks, including for eval attacks, remote JavaScript includes, CSP bypasses, DOM XSS, and JavaScript expression evaluation. ([C4](<https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab=Formal_Numbering)>)
68. Verify that the application protects against LDAP Injection vulnerabilities, or that specific security controls to prevent LDAP Injection have been implemented. ([C4](<https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab=Formal_Numbering)>)
69. Verify that the application protects against OS command injection and that operating system calls use parameterized OS queries or use contextual command line output encoding. ([C4](<https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab=Formal_Numbering)>)
70. Verify that the application protects against Local File Inclusion (LFI) or Remote File Inclusion (RFI) attacks.
71. Verify that serialized objects use integrity checks or are encrypted to prevent hostile object creation or data tampering. ([C5](<https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab=Formal_Numbering)>)
72. Verify that the application correctly restricts XML parsers to only use the most restrictive configuration possible and to ensure that unsafe features such as resolving external entities are disabled to prevent XXE.
73. Verify that deserialization of untrusted data is avoided or is protected in both custom code and third-party libraries (such as JSON, XML and YAML parsers).
74. Verify that when parsing JSON in browsers or JavaScript-based backends, JSON.parse is used to parse the JSON document. Do not use eval() to parse JSON.
75. Verify that all cryptographic modules fail securely, and errors are handled in a way that does not enable Padding Oracle attacks.
76. Verify that the application does not log credentials or payment details. Session tokens should only be stored in logs in an irreversible, hashed form. ([C9, C10](<https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab=Formal_Numbering)>)
77. Verify that the application does not log other sensitive data as defined under local privacy laws or relevant security policy. ([C9](<https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab=Formal_Numbering)>)
78. Verify that a generic message is shown when an unexpected or security sensitive error occurs, potentially with a unique ID which support personnel can use to investigate.  ([C10](<https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab=Formal_Numbering)>)
79. Verify the application sets sufficient anti-caching headers so that sensitive data is not cached in modern browsers.
80. Verify that data stored in client side storage (such as HTML5 local storage, session storage, IndexedDB, regular cookies or Flash cookies) does not contain sensitive data or PII.
81. Verify that authenticated data is cleared from client storage, such as the browser DOM, after the client or session is terminated.
82. Verify that sensitive data is sent to the server in the HTTP message body or headers, and that query string parameters from any HTTP verb do not contain sensitive data.
83. Verify that users have a method to remove or export their data on demand.
84. Verify that users are provided clear language regarding collection and use of supplied personal information and that users have provided opt-in consent for the use of that data before it is used in any way.
85. Verify that all sensitive data created and processed by the application has been identified, and ensure that a policy is in place on how to deal with sensitive data. ([C8](<https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab=Formal_Numbering)>)
86. Verify that secured TLS is used for all client connectivity, and does not fall back to insecure or unencrypted protocols. ([C8](<https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab=Formal_Numbering)>)
87. Verify using online or up to date TLS testing tools that only strong algorithms, ciphers, and protocols are enabled, with the strongest algorithms and ciphers set as preferred.
88. Verify that old versions of SSL and TLS protocols, algorithms, ciphers, and configuration are disabled, such as SSLv2, SSLv3, or TLS 1.0 and TLS 1.1. The latest version of TLS should be the preferred cipher suite.
89. Verify that if the application has a client or server auto-update feature, updates should be obtained over secure channels and digitally signed. The update code must validate the digital signature of the update before installing or executing the update.
90. Verify that the application employs integrity protections, such as code signing or sub-resource integrity. The application must not load or execute code from untrusted sources, such as loading includes, modules, plugins, code, or libraries from untrusted sources or the Internet.
91. Verify that the application has protection from sub-domain takeovers if the application relies upon DNS entries or DNS sub-domains, such as expired domain names, out of date DNS pointers or CNAMEs, expired projects at public source code repos, or transient cloud APIs, serverless functions, or storage buckets (autogen-bucket-id.cloud.example.com) or similar. Protections can include ensuring that DNS names used by applications are regularly checked for expiry or change.
92. Verify the application will only process business logic flows for the same user in sequential step order and without skipping steps.
93. Verify the application will only process business logic flows with all steps being processed in realistic human time, i.e. transactions are not submitted too quickly.
94. Verify the application has appropriate limits for specific business actions or transactions which are correctly enforced on a per user basis.
95. Verify the application has sufficient anti-automation controls to detect and protect against data exfiltration, excessive business logic requests, excessive file uploads or denial of service attacks.
96. Verify the application has business logic limits or validation to protect against likely business risks or threats, identified using threat modelling or similar methodologies.
97. Verify that the application will not accept large files that could fill up storage or cause a denial of service attack.
98. Verify that user-submitted filename metadata is not used directly with system or framework file and URL API to protect against path traversal.
99. Verify that user-submitted filename metadata is validated or ignored to prevent the disclosure, creation, updating or removal of local files (LFI).
100. Verify that user-submitted filename metadata is validated or ignored to prevent the disclosure or execution of remote files (RFI), which may also lead to SSRF.
101. Verify that the application protects against reflective file download (RFD) by validating or ignoring user-submitted filenames in a JSON, JSONP, or URL parameter, the response Content-Type header should be set to text/plain, and the Content-Disposition header should have a fixed filename.
102. Verify that untrusted file metadata is not used directly with system API or libraries, to protect against OS command injection.
103. Verify that files obtained from untrusted sources are stored outside the web root, with limited permissions, preferably with strong validation.
104. Verify that files obtained from untrusted sources are scanned by antivirus scanners to prevent upload of known malicious content.
105. Verify that the web tier is configured to serve only files with specific file extensions to prevent unintentional information and source code leakage. For example, backup files (e.g. .bak), temporary working files (e.g. .swp), compressed files (.zip, .tar.gz, etc) and other extensions commonly used by editors should be blocked unless required.
106. Verify that direct requests to uploaded files will never be executed as HTML/JavaScript content.
107. Verify that the web or application server is configured with a whitelist of resources or systems to which the server can send requests or load data/files from.
108. Verify that all application components use the same encodings and parsers to avoid parsing attacks that exploit different URI or file parsing behavior that could be used in SSRF and RFI attacks.
109. Verify that access to administration and management functions is limited to authorized administrators.
110. Verify API URLs do not expose sensitive information, such as the API key, session tokens etc.
111. Verify that enabled RESTful HTTP methods are a valid choice for the user or action, such as preventing normal users using DELETE or PUT on protected API or resources.
112. Verify that JSON schema validation is in place and verified before accepting input.
113. Verify that RESTful web services that utilize cookies are protected from Cross-Site Request Forgery via the use of at least one or more of the following: triple or double submit cookie pattern (see [references](<https://www.owasp.org/index.php/Cross-Site_Request_Forgery_(CSRF)_Prevention_Cheat_Sheet))>, CSRF nonces, or ORIGIN request header checks.
114. Verify that XSD schema validation takes place to ensure a properly formed XML document, followed by validation of each input field before any processing of that data takes place.
115. Verify that all components are up to date, preferably using a dependency checker during build or compile time. ([C2](<https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab=Formal_Numbering)>)
116. Verify that all unneeded features, documentation, samples, configurations are removed, such as sample applications, platform documentation, and default or example users.
117. Verify that if application assets, such as JavaScript libraries, CSS stylesheets or web fonts, are hosted externally on a content delivery network (CDN) or external provider, Subresource Integrity (SRI) is used to validate the integrity of the asset.
118. Verify that web or application server and framework error messages are configured to deliver user actionable, customized responses to eliminate any unintended security disclosures.
119. Verify that web or application server and application framework debug modes are disabled in production to eliminate debug features, developer consoles, and unintended security disclosures.
120. Verify that the HTTP headers or any part of the HTTP response do not expose detailed version information of system components.
121. Verify that every HTTP response contains a content type header specifying a safe character set (e.g., UTF-8, ISO 8859-1).
122. Verify that all API responses contain Content-Disposition: attachment; filename="api.json" (or other appropriate filename for the content type).
123. Verify that a content security policy (CSPv2) is in place that helps mitigate impact for XSS attacks like HTML, DOM, JSON, and JavaScript injection vulnerabilities.
124. Verify that all responses contain X-Content-Type-Options: nosniff.
125. Verify that HTTP Strict Transport Security headers are included on all responses and for all subdomains, such as Strict-Transport-Security: max-age=15724800; includeSubdomains.
126. Verify that a suitable "Referrer-Policy" header is included, such as "no-referrer" or "same-origin".
127. Verify that a suitable X-Frame-Options or Content-Security-Policy: frame-ancestors header is in use for sites where content should not be embedded in a third-party site.
128. Verify that the application server only accepts the HTTP methods in use by the application or API, including pre-flight OPTIONS.
129. Verify that the supplied Origin header is not used for authentication or access control decisions, as the Origin header can easily be changed by an attacker.
130. Verify that the cross-domain resource sharing (CORS) Access-Control-Allow-Origin header uses a strict white-list of trusted domains to match against and does not support the "null" origin.