Nr. sprawy: 06/PN/ND.ZP/2019

Samodzielny Publiczny Zespół Zakładów Opieki Zdrowotnej w Kozienicach
ul. Al. Władysława Sikorskiego 10
26-900 Kozienice

Załącznik nr 6 do SIWZ

Przedmiot zamówienia:

„Świadczenie specjalistycznych usług towarzyszących wdrożeniu elektronicznej platformy gromadzenia, analizy i udostępniania danych medycznych”

Przedmiotowe zamówienie wchodzi w zakres projektu pt. „Elektroniczna platforma gromadzenia, analizy i udostępniania danych medycznych w SP ZZOZ w Kozienicach”

realizowanego w ramach:
Regionalnego Programu Operacyjnego Województwa Mazowieckiego na lata 2014-2020.
Projekt nr RPMA.02.01.01-14-7923/17

Zaakceptował: …….

Kozienice,kwiecień 2019 r.

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

Do przetargu pod nazwą:

„Świadczenie specjalistycznych usług towarzyszących wdrożeniu elektronicznej platformy gromadzenia, analizy i udostępniania danych medycznych"

a. Zakres zamówienia

Zgodnie z założeniami projektu wynikającymi ze Studium Wykonalności, o nazwie: „Elektroniczna platforma gromadzenia, analizy i udostępniania danych medycznych w SP ZZOZ w Kozienicach" realizowanego w ramach Regionalnego Programu Operacyjnego Województwa Mazowieckiego na lata 2014-2020, Samodzielny Publiczny Zespół Zakładów Opieki Zdrowotnej w Kozienicach zamawia niżej wyszczególnione produkty i usługi, zgodnie z opisem parametrów minimalnych poszczególnych elementów zamówienia zawartym w dalszej części dokumentu.

1. Przedmiot zamówienia obejmuje następujący zakres prac:
   a) Audyt teleinformatyczny obejmujący:
   - Analizę i ocenę wszelkiej dokumentacji powstałej w trakcie realizacji projektu;
   - Weryfikację powstałej w ramach projektu dokumentacji technicznej i użytkowej po kątem jej zgodności z założeniami projektu;
   - Analizę procesów biznesowych po wdrożeniu platformy e-usług;
   - Rekomendacje dla dalszego rozwoju systemu – koncepcja jego rozbudowy;

   b) Audyt bezpieczeństwa;
   c) Budowa systemu bezpieczeństwa informacji;
   d) Przygotowanie dokumentacji kończącej projekt celem jego rozliczenia i zakończenia;

b. Szczegółowy opis wymagań

b.1. Przeprowadzenie audytu IT

Audyt przeprowadzony będzie pod kątem oceny zgodności wdrożonego systemu z założeniami zawartymi w Studium wykonalności projektu i gotowości do świadczenia e-usług zdrowotnych oraz wprowadzenia elektronicznej dokumentacji medycznej. Obejmie następujące zagadnienia:

1. Infrastruktura przetwarzania danych – sprzęt komputerowy,
2. Infrastruktura teleinformatyczna – sieci komputerowe LAN,
3. Oprogramowanie systemowe i użytkowe,
4. Systemy i infrastruktura dziedzinowo powiązane,
5. Analiza procesów biznesowych,
6. Analiza dojrzałości dopasowania obszaru IT do wymogów procesów biznesowych.

Wyniki audytu mają umożliwić szczegółową weryfikację poziomu osiągnięcia założeń projektu oraz identyfikację nowych potrzeb w procesie tworzenia, analizy oraz archiwizacji informacji medycznej składającej się na dokumentację medyczną a przez to objętych procesem komputeryzacji i informatyzacji w ramach projektu.

Audyt ma również wskazać zakres czynności, które muszą być podjęte w celu dostosowania pozyskanej w ramach projektu infrastruktury teleinformatycznej do kolejnych wymagań i potrzeb do stanu na dzień zakończenia wdrożenia systemu.

.Analiza procesów biznesowych pozwali na określenie nowych ról oraz uprawnień dla użytkowników oprogramowania służącego do rejestrowania, analizy oraz archiwizacji informacji medycznej mającej znaczenie w kontekście elektronicznej dokumentacji medycznej.

Analiza dojrzałości dopasowania obszaru IT do wymogów procesów biznesowych posłuży do określenia poziomu spełnienia założonych wymagań dla wdrożenia systemu teleinformatycznego.

Wnioski z przeprowadzonych audytów służyć będą do wskazania rekomendacji w zakresie modernizacji/rozbudowy obszaru IT (Koncepcja dalszej rozbudowy).

W wyniku realizacji tego etapu zamówienia zostaną opracowane:

1. raport z audytu infrastruktury teleinformatycznej wraz z oceną dostarczonego sprzętu komputerowego (oraz jeśli to konieczne infrastruktury powiązanej),
2. nowe zapotrzebowania na sprzęt w zakresie infrastruktury teleinformatycznej (w tym sprzęt komputerowy),
3. wymogi w zakresie środowiska przetwarzania danych dla sprzętu oraz oprogramowania systemowego,
4. wymogi dla bezpieczeństwa danych, w tym systemów archiwizacji, backupu, ciągłości działania systemów,
5. wymogi w zakresie dostosowania infrastruktury teleinformatycznej, w tym m.in: sieciowej, zasilania dedykowanego, przystosowania pomieszczeń oraz pomieszczeń serwerowych do realizacji wdrożenia kolejnych systemów oprogramowania HIS oraz EDM nie objętych projektem.
6. dokumentacja analityczna procesów biznesowych obejmująca modelowanie w postaci graficznej wraz z opisem obiektów umieszczonych na modelach,

7 ocena dopasowania procesów biznesowych do obszaru funkcjonowania IT w jednostkach objętych projektem,

8 model przepływu informacji tworzonych lokalnie w jednostkach w relacji z wymaganiami stawianymi przez tworzone w innych projektach: e-zdrowie dal Mazowsza - regionalny system informacji medycznej w powiązaniu z projektami budowanymi na poziomie centralnym,

9 wymagania funkcjonalne dla oprogramowania użytkowego odpowiadające zdefiniowanym potrzebom w analizie procesów biznesowych.

Audyt infrastruktury będzie zrealizowany na podstawie:

1. uzgodnień z Beneficjentem i Partnerami Projektu;
2. dokumentacji otrzymanej od Beneficjenta i Partnerów Projektu;
3. wizji lokalnej służącej przeglądowi i ocenie wszystkich elementów podlegających audytowi;
4. innych czynności niezbędnych do wykonania przedmiotu zamówienia.

Raport z audytu infrastruktury teleinformatycznej

Raport zawierał będzie następujące dane:

1 opis stanu obecnej infrastruktury, w tym w szczególności:

1) infrastruktura sieciowa pasywna i aktywna,

2) instalacje i systemy budynkowe, w tym: monitoring, kontrola dostępu, zarządzanie mediami, elektryka itp.,

3) pomieszczenia techniczne z wyposażeniem zawierające w/w infrastrukturę sieciową typu serwerownie, punkty dystrybucyjne, kablownie, siłownie, etc.,

4) instalacje dedykowanego zasilania urządzeń komputerowych wraz z podtrzymaniem zasilania na wypadek awarii,

5) użytkowany sprzęt komputerowy,

6) użytkowane środowisko systemowe – systemy operacyjne,

7) systemy bezpieczeństwa, w tym kontrola styku z Internetem,

8) systemy archiwizacji i backupu danych, zapewnienie ciągłości działania,

9) systemy dziedzinowe: przywoławcze, komunikacji wewnętrznej, teleradiologii, blok operacyjny, gospodarka lekami itp.

2 rekomendacje i zalecenia w obszarze infrastruktury teleinformatycznej oraz infrastruktury powiązanej w projekcie:

1) opisanie zakresu planowanych do wykonania prac i dostaw do późniejszego wykorzystania w Projekcie technicznym budowy serwerowni i sieci komputerowej,

2) pozostałe parametry audytowanych elementów infrastruktury (szczegółowy zakres dla każdego elementu infrastruktury podlega uzgodnieniu z Zamawiającym.

Wykonawca wykona opracowania (produkty dokumentacyjne):

1) raport z audytu w formie papierowej oraz na nośniku elektronicznym w programie ogólnodostępnym w formacie „*.pdf” oraz innym edytowalnym np. „*.docx” lub „*.doc” umożliwiającym nanoszenie uzupełnień i komentarzy w trybie śledzenia przez wielu autorów z możliwością ich identyfikacji.

Analiza procesów biznesowych

Analiza procesów biznesowych u Zamawiającego odnosi się do obszarów działalności leczniczej.

Wymagania:

1 Poziom szczegółowości analizy procesów biznesowych powinien umożliwiać przyporządkowanie użytkowników do poszczególnych procesów biznesowych w danej jednostce w zakresie przewidzianym do wdrożenia w projekcie.

2 Procesy biznesowe powinny być również zmapowane na istniejące i zamówione systemy teleinformatyczne w tym przede wszystkim systemy HIS, EDM, ERP, sprawozdawczość zarządcza oraz na istniejący i planowany do dostawy i instalacji sprzęt teleinformatyczny, w zakresie przewidzianym potrzebami projektu.

3 Wynikiem prac Wykonawcy będą modele odzwierciedlające procesy biznesowe, które muszą obejmować systemy i sprzęt zakupywany przez jednostki organizacyjne Zamawiającego, jak również systemy i sprzęt będący już w posiadaniu jednostek.

4 Partnerzy projektu zapewnią Wykonawcy dostęp do poszczególnych placówek oraz dostępność osób, które będą mogły udzielić informacji niezbędnych Wykonawcy do prac analitycznych oraz opracowania modeli.

5 Opracowanie i przedstawienie Zamawiającemu rekomendowanego harmonogramu wdrożenia produktów projektu uwzględniającego stopień informatyzacji poszczególnych jednostek oraz stopień złożoności tego wdrożenia. Harmonogram powinien mieć wskazaną ścieżkę krytyczną i zidentyfikowane ryzyka wdrożeniowe.

6 Metamodel opisujący strukturę modeli wytworzonych w ramach prac analitycznych uwzględniający m.in.:

1) listę typów obiektów,
2) atrybuty obiektów,
3) dozwolone powiązania między obiektami,
4) dozwolone wartości atrybutów,
5) listę typów diagramów,
6) dozwolone obiekty na poszczególnych typach diagramów,
7) poziom szczegółowości poszczególnych modeli.

7 Wynikiem przeprowadzonych w/w prac będzie dokumentacja analityczna obejmująca modele w postaci graficznej wraz z opisem obiektów umieszczonych na modelach:

1) model celów z określonymi miarami celów. Identyfikacja i opis celów prowadzonych prac analitycznych z definicją miar ich osiągnięcia,
2) model struktury organizacyjnej. Opis struktury organizacyjnej jednostek zamawiającego uczestniczących w projekcie z uwzględnieniem zależności organizacyjnej poszczególnych jednostek oraz rodzajami stanowisk pracy,

3) model lokalizacji. Identyfikacja i opis lokalizacji poszczególnych jednostek organizacyjnych oraz elementów infrastruktury teleinformatycznej wykorzystywanej i nabywanej w projekcie,
4) modele ról i aktorów. Identyfikacja i opis aktorów uczestniczących w analizowanych procesach biznesowych oraz opisanie ich ról i uprawnień w kontekście planowanego do wdrożenia systemu,
5) model infrastruktury teleinformatycznej. Identyfikacja i opis elementów infrastruktury teleinformatycznej zarówno tej posiadanej przez zamawiającego jak i dostarczonej na potrzeby systemu,
6) model środowiska pracy łączący wybrane informacje z modeli. Opis środowiska wdrożeniowego systemu,
7) mapa procesów biznesowych w standardzie BPMN lub równoważnym. Identyfikacja i opis głównych procesów biznesowych w podziale na rodzaje jednostek Zamawiającego,
8) modele procesów biznesowych. Definicja i opis poszczególnych procesów biznesowych w kontekście wdrażanego systemu, umożliwiająca konfigurację i dostosowanie systemu do poszczególnych ról użytkowników.

Wszystkie modele będą:

1 prezentować stan docelowy po wdrożeniu systemu (pokrycie poszczególnych procesów przez systemy istniejące i wdrażane w projekcie i wskazanie przypisanej infrastruktury),
2 powinny być przygotowane i prezentowane dla każdej jednostki oddzielnie.

Na potrzeby weryfikacji kompletności i spójności poszczególnych modeli należy przygotować macierze prezentujące wybrane przekroje informacyjne wskazanych modeli.

1. Analizowane procesy biznesowe muszą zostać poddane analizie dojrzałości dopasowania procesów biznesowych do procesów obszaru IT w oparciu o wybraną przez Wykonawcę metodykę.
2. Wykonawca wykona opracowania (produkty dokumentacyjne):
   1) opracowane procesy biznesowe wraz z modelami w postaci papierowej oraz elektronicznej w formacie umożliwiającym nanoszenie uzupełnień i komentarzy w trybie śledzenia przez wielu autorów z możliwością ich identyfikacji.
   2) Wykonawca na czas realizacji projektu zapewni Zamawiającemu narzędzia informatyczne umożliwiające uczestnikom projektu nanoszenie uzupełnień i komentarzy w trybie śledzenia przez wielu autorów z możliwością ich identyfikacji za pośrednictwem strony internetowej.

Analiza poziomu dojrzałości dopasowania biznes – IT

Analiza poziomu dojrzałości dopasowania procesów biznesowych w obszarze zarządczym (biznes) do obszaru IT odnosi się do obszarów działalności leczniczej. Zamawiający nie preferuje określonego mo-

delu analitycznego.

Analiza powinna obejmować następujące obszary strategiczne w działalności podmiotu leczniczego służące ocenie dopasowania strategicznego IT:

– **Nadzór (Governance)** – rozumiany jako zapewnienie by przedstawiciele biznesu i IT przeprowadzali formalne dyskusje i analizy w zakresie priorytetowania inwestycji i alokacji zasobów IT, w szczególności obejmuje integrowanie strategii IT i biznesu, zapewnienie odpowiedniej struktury organizacyjnej, kontrolę nad kosztami IT oraz priorytetowanie i ocenę efektywności inwestycji IT

– **Pomiar wartości (Value measurments)** - umiejętność zmierzenia oraz zademonstrowania biznesowi wartości IT za pomocą takich miar jakie biznes zrozumie; wiąże sie to z wprowadzeniem formalnych gwarancji jakości świadczonych usług przez IT, ocen efektywności inwestycji w IT oraz praktyk ciągłego doskonalenia, a także z integracją miar technicznych i biznesowych w docelowym kierunku czterech perspektyw strategicznej karty wyników

– **Partnerstwo (Partnership)** - docelowo IT powinno mieć możliwość wpływania na kształt strategii przedsiębiorstwa i sposób jej realizacji, dzielić z biznesem ryzyka i nagrody oraz podlegać bezpośrednio Prezesowi, występującemu w roli sponsora biznesowego; wówczas IT stanie się partnerem biznesu w tworzeniu wartości przedsiębiorstwa

– **Komunikacja (Communications)** - obejmuje efektywną wymianę poglądów jak też zrozumienie, co jest wymagane by przygotować odpowiednią strategię a następnie z sukcesem ją wdrożyć; w praktyce po stronie IT brakuje często świadomości celów biznesowych a po stronie biznesu – zrozumienia specyfiki IT i jego znaczenia dla biznesu

– **Umiejętności (Skills)** – szeroki zakres działań związanych z zarządzaniem zasobami ludzkimi w przedsiębiorstwie; wychodzą poza standardowe procesy związane z rekrutacją, szkoleniami i utrzymaniem pracowników w kierunku zapewnienia innowacyjnego i przedsiębiorczego środowiska przygotowanego na funkcjonowanie w ciągle zmieniającym się otoczeniu

– **Zakres i architektura (Scope and Architecture)** - obejmuje ocenę dojrzałości infrastruktury IT przedsiębiorstwa; przechodząc od wsparcia prostych czynności biurowych do zintegrowanych i wystandaryzowanych w skali całego przedsiębiorstwa zaawansowanych systemów wpierających kluczowe procesy biznesowe, a także kreujących nowe procesy, infrastruktura IT umożliwia nie tylko efektywną realizację obecnej strategii przedsiębiorstwa, lecz także pozwala na szybkie i elastyczne reagowanie na zmiany zachodzące na rynku oraz kreowanie nowych przewag konkurencyjnych.

Uzyskane wyniki w zastosowanym modelu analitycznym powinny opisywać poziom dopasowania biznes – IT lub lukę w dopasowaniu w obszarach newralgicznych z punktu widzenia relacji biznes - IT.

Zalecany sposób prowadzenia analiz w oparciu o następujące kryteria:

Lp.	Obszar	Kryteria
1.	**Nadzór**	• Formalne strategiczne planowanie biznesowe • Formalne strategiczne planowanie IT • Struktura organizacyjna • Zależności organizacyjne • Kontrola budżetowania IT • Cel inwestowania w IT • Komitet sterujący • Proces priorytetowania
2.	**Komunikacja**	• Zrozumienie biznesu przez IT • Zrozumienie IT przez biznes

		• Uczenie się organizacji • Sztywność komunikacji • Dzielenie się wiedzą • Efektywność współpracy między pracownikami IT i biznesowymi
3.	**Partnerstwo**	• Postrzeganie wartości IT przez biznes • Rola IT w strategicznym planowaniu biznesowym • Wspólne cele, ryzyka i nagrody/kary • Zarządzanie związkami IT-biznes • Charakter związków IT-biznes • Sponsor biznesowy
4.	**Pomiar wartości**	• Metryki IT • Metryki biznesowe • Połączenie miedzy metrykami IT i biznesowymi • Gwarancja jakości świadczonych usług • Benchmarking • Formalne oceny inwestycji IT • Ciągłe doskonalenie
5.	**Umiejętności**	• Innowacyjność, przedsiębiorczość • Styl zarządzania • Gotowość na zmiany • Możliwość kariery wewnątrz przedsiębiorstwa • Szkolenia miedzywydziałowe • Środowisko • Rekrutacja i utrzymanie
6.	**Zakres i architektura**	• Rodzaj głównych systemów • Standardy • Integracja architektury • Postrzegana rola infrastruktury

b.2. Audyt bezpieczeństwa Platformy e-usług (systemu informatycznego)

Celem głównym Audytu jest określenie poziomu bezpieczeństwa wdrażanej Platformy e-usług, wskazanie punktów obniżających ten poziom oraz zaproponowanie rozwiązań, które doprowadzą środowisko do akceptowalnego przez Zamawiającego poziomu bezpieczeństwa.

Audyt bezpieczeństwa Platformy - będzie obejmował:

a.i.1. Kontrolę spójności oraz zgodności z przepisami obowiązującego prawa.

Audyt będzie obejmował kontrolę spójności oraz zgodności z przepisami prawa, a także weryfikację poziomu przestrzegania tych regulacji. Zakres kontroli obejmie samą Platformę i dokumentacje bezpieczeństwa Platformy pod kątem aktualności, kompletności, poprawności, a także zgodności z obowiązującym prawem i standardami (w szczególności kontrola zgodności z wymaganiami określonymi w Rozporządzeniu Rady Ministrów z 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).

a.i.2. Weryfikację bezpieczeństwa przetwarzania danych osobowych pod względem zgodności z obowiązującym prawem.

Audyt będzie obejmował sprawdzenie aktualnego stanu przetwarzania danych osobowych zarówno pod kątem zagadnień technicznych, organizacyjnych oraz prawnych ze szczególnym uwzględnieniem wymagań zgodnych z normą ISO 27001 i opisanych w ustawie o ochronie danych osobowych zgodnie z Dyrektywą RODO, jak również w Rozporządzeniu MSWiA z dnia 29 kwietnia 2004 r. „w sprawie dokumentacji przetwarzania danych osobo-

wych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych" (Dz. U. 2004 nr 100 poz. 1024).

a.i.3. Weryfikacje bezpieczeństwa Platformy, jako systemu teleinformatycznego.

Celem audytu jest wykrycie faktycznych oraz potencjalnych luk i błędów w oprogramowaniu, które mogą być wykorzystane do naruszenia bezpieczeństwa przetwarzanych informacji, a także bezpieczeństwa Zamawiającego lub Użytkowników systemów. Przeprowadzenie audytu na etapie wytwarzania i przekazywania do użytkowania Platformy pozwolić ma na dostarczenie odbiorcom projektu rozwiązań gwarantujących osiągnięcie wymaganego poziomu bezpieczeństwa w fazie użytkowania. Zakres obszarów podlegających audytowi:

1.1. Konfiguracja systemów operacyjnych, w szczególności:

a) weryfikację udostępnionych usług sieciowych wraz ze wskazaniem ich podatności,
b) weryfikację zbędnych usług,
c) weryfikację dodatkowych metod zabezpieczeń (np. systemy antywirusowe, anty-malware, HIPS, IPS/IDS itp),
d) weryfikację zaimplementowanych systemów aktualizacji i mechanizmów ich wdrażania,
e) weryfikację zaimplementowanych systemów kopii zapasowych,
f) weryfikację zaimplementowanych systemów logowania zdarzeń,
g) weryfikację mechanizmów administracji zdalnej,
h) weryfikację uprawnień Użytkowników oraz przypisania do właściwych grup, w szczególności weryfikację uprawnień do najważniejszych zasobów.

1.2. Konfiguracja baz danych, w szczególności:

a) weryfikację sposobu udostępniania baz na poziomie sieciowym,
b) weryfikację zaimplementowanych systemów kopii zapasowych,
c) analizę implementacji zasad „utwardzania" bazy danych (np. logowanie zdarzeń, składowanie logów, partycjonowanie bazy, monitorowanie dostępu do obiektów, monitorowanie instrukcji języka SQL.),
d) analizę architektury bazy danych (np. wykorzystanie mechanizmów autoryzacji oraz uwierzytelniania, segmentacja uprawnień, przechowywanie oraz dostęp do danych wrażliwych, szyfrowanie danych),
e) analizę komunikacji z klientami bazodanowymi (mechanizmy kryptograficzne, transfery danych).

1.3. Bezpieczeństwo aplikacji, w szczególności:

f) identyfikację wrażliwych punktów w systemie,
g) inspekcję mechanizmów uwierzytelniania/autoryzacji,
h) weryfikację implementacji mechanizmów ochronnych dla wszystkich serwerów aplikacyjnych i modułów dostępowych,
i) weryfikację elementów charakterystycznych dla serwera www,
j) weryfikację obsługi błędów,
k) analizę poziomu bezpieczeństwa oferowanego przez aplikację,
l) analizę architektury sieciowej.

1.4. Bezpieczeństwo sieci, w szczególności:

Analizę sieci LAN:

a) weryfikacja segmentacji sieci LAN na strefy sieciowe (z uwzględnieniem wykorzystania urządzeń typu firewall, access list oraz VLAN),

b) określenie usług działających w podsieciach,

c) poszukiwanie podatności w podsieciach,

d) weryfikacja mechanizmów ochronnych w warstwie 2 i 3 modelu OSI/ISO,

e) weryfikacja dostępu do Internetu z LAN,

f) szczegółowa analiza wybranej komunikacji sieciowej,

g) weryfikacja zasad utrzymania sieci.

Analizę sieci WAN oraz styku z siecią Internet:

a) weryfikacja topologii/architektury sieci,

b) testy szczelności systemów klasy firewall, UTM,

c) ogólna analiza komunikacji sieciowej z poziomu sieci WAN oraz Internet,

d) skanowanie portów różnymi technikami,

e) wykrywanie usług sieciowych udostępnionych w sieci WAN oraz Internet,

f) próba detekcji wersji oraz typu oprogramowania systemowego zainstalowanego na urządzeniach dostępnych w szczególności z sieci Internet,

g) testowanie odporności usług wystawionych do sieci Internet na ataki,

h) testy penetracyjne sieci i VPN.

a.i.4. Weryfikacje spełnienia wymagań określonych dla Platformy e-usług w zakresie bezpieczeństwa.

Audyt będzie obejmował analizę realizacji przez wykonawcę Platformy e-sług (systemu informatycznego) wymagań w zakresie funkcjonalności dotyczących bezpieczeństwa, określonych w opisie przedmiotu zamówienia zaprojektowania, wykonania i wdrożenia Platformy. Zakres usług realizowanych w ramach tego zadania obejmuje przeprowadzenie audytu ze szczególnym uwzględnieniem poniższych aspektów:

a) Audyt architektury aplikacji.

b) Audyt zastosowanej technologii.

c) Analiza wydajności kodu.

d) Podstawowa analiza baz danych (normalizacja).

e) Audyt kosztów modyfikowania podczas utrzymania i rozwoju.

f) Analiza użytych funkcji lub komponentów pod kątem elementów przestarzałych („deprecated") lub elementów posiadających znane luki bezpieczeństwa lub podatności.

W ramach audytu Platformy wymagane jest sprawdzenie dostępności strony internetowej, przeprowadzając pełną weryfikacje zgodności serwisu z międzynarodowymi standardami WCAG:

a) Sprawdzenie zgodności z W3C,

b) Sprawdzenie zgodności z W3C CSS,

c) Sprawdzenie zgodności z WAI (WCAG 2.0).

a.i.5. Testy penetracyjne oraz analizę sposobu implementacji mechanizmów bezpieczeństwa.

Zamawiający wymaga w ramach realizacji zadania, wykonywania testów penetracyjnych z wykorzystaniem standardów testowania bezpieczeństwa:

- OWASP (Open Web Application Security Project) ASVS 2014.
- Open Source Security Testing Methodology Manual (OSSTMM).
- Penetration Testing Execution Standard (PTES).

lub równoważnych (za równoważne Zamawiający uzna, standardy opisujące przebieg procesu testowania bezpieczeństwa systemów IT oraz obszary systemowe podlegające weryfikacji).

1.5. Wykorzystanie zbiorów danych o znanych podatnościach i słabościach bezpieczeństwa

Zamawiający wymaga wykorzystania znanych zbiorów danych o podatnościach i słabościach bezpieczeństwa systemów teleinformatycznych, w trakcie prac prowadzonych przez Wykonawcę w ramach przedmiotu zamówienia, np.

a.a) SANS Top 20 Critical Security Controls.

a.b) Common Vulnerabilities and Exposures.

a.c) WASC (Web Application Security Consortium) Threat Classification.

lub równoważnych (za równoważne Zamawiający uzna takie bazy danych, które stanowią aktualne źródło informacji o lukach bezpieczeństwa, są publikowane lub utrzymywane przez uznane powszechnie organizacje, działające na rzecz zapewnienia bezpieczeństwa systemów teleinformatycznych).

1.6. Wykorzystanie list kontrolnych

Zamawiający wymaga, aby w ramach realizacji audytu bezpieczeństwa do oceny wykorzystywane były listy kontrolne udostępniane przez uznane organizacje pracujące na rzecz bezpieczeństwa systemów IT, tj.:

a) National Security Agency (NSA).

b) Center for Internet Security (CIS).

lub równoważnych (w szczególności takich, które stanowią aktualne źródło informacji o bezpiecznej konfiguracji, są publikowane lub utrzymywane przez uznane powszechnie organizacje, działające na rzecz zapewnienia bezpieczeństwa systemów teleinformatycznych).

1.7. Typowe zadania dla testowania penetracyjnego

Zamawiający wymaga, aby w ramach realizacji testów penetracyjnych obejmowały one typowe, wymienione niżej zadania (będące elementem każdej metodyki testów penetracyjnych):

a) Target Scoping (Zakres Docelowy – ustalenie charakteru i zasięgu testów)

b) Information Gathering (Gromadzenie Informacji – pasywne zbieranie informacji na temat obiektu testów)

c) Target Discovery (Odkrywanie Celu – pół-pasywne zbieranie informacji, poznanie celów, identyfikacja podsieci, rodzaju architektury, systemów operacyjnych)

d) Enumerating Target (Wyliczanie Elementów – aktywne zbieranie informacji, enumeracja usług, portów, wykrywanie systemów bezpieczeństwa IDS/UPS, FV)

e) Vulnerability Mapping (Mapowanie Podatności – poszukiwanie podatności w elementach znalezionych w poprzednich fazach)

e) Target Exploitation (Docelowa Eksploatacja – 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)

f) Privilage Escalation (Eskalacja Uprawnień – zwiększenie uprawnień w przełamanym systemie i przeniesienie kontroli na kolejne usługi lub systemy)

g) Maintaining Access (Utrzymanie Dostępu – utrzymanie dostępu do skompromitowanego systemu, instalacja tylnych furtek, rootkit-ów.

h) Documentation & Reporting (Dokumentacja i Raportowanie – raport powinien zawierać informacje o znalezionych podatnościach oraz zauważonych problemach)

1.8. Testy penetracyjne i symulowane ataki

Zamawiający wymaga, aby w ramach realizacji zadania zostały przeprowadzone testy penetracyjne i symulowane ataki obejmujące:

1.8.1. Testy bezpieczeństwa Platformy pod kątem ataków typu:

1. Ataki semantyczne na adres URL,
2. Ataki związane z ładowaniem plików,
3. Ataki typu Cross-Site Scripting,
4. Ataki typu Cross-Site Request Forgery,
5. Ataki typu MITM (Man in the Middle),
6. Broken Authentication and Session Management (badanie losowości ID sesji, próba detekcji składni nazywania cookie sesyjnego, sprawdzenie bezpieczeństwa budowy formularza logowania),
7. Authorization Bypass (próby dostępu do zasobów bez uwierzytelnienia Użytkownika),
8. Code Execution (próby wykonania wrogiego kodu na serwerze),
9. Information Leakage (próby detekcji wycieku istotnych informacji – technicznych i biznesowych),
10. Insecure Communications (dostęp do istotnych danych w wyniku braku lub nieodpowiedniego poziomu szyfrowania),
11. Source Disclosure (próby prowadzące do ujawnienia kodów źródłowych wykorzystanego oprogramowania),
12. File Inclusion (załączanie plików lub do ich zawartości złośliwej zawartości),
13. Open Redirection (próby nieautoryzowanego przekierowania),
14. Fałszowanie żądania http,
15. Response Splitting (brak prawidłowej walidacji nagłówków http)
16. Ujawnienie danych przechowywanych w bazie,
17. Trawersowanie katalogów,
18. Ujawnianie kodu źródłowego,
19. Przepełnienie bufora lub stosu,
20. Wstrzykiwanie kodu wykonywalnego innych języków programowania.

1.8.2. Zbadanie, co najmniej:

1. Enumeracji i wykorzystania znanych podatności w celu uzyskania nieautoryzowanego dostępu.

2. Możliwości podszywania się pod Użytkowników i uzyskania nieautoryzowanego dostępu do systemu.
3. Możliwości podszywania się pod Użytkowników uprzywilejowanych i uzyska-nie dostępu do systemu.
4. Możliwości blokowania/umożliwienia dostępu do systemu wszystkim lub wybranym jej Użytkownikom.
5. Metody uwierzytelnienia dwuskładnikowego - próby podatności, weryfikacja działania, próby ominięcia mechanizmu.

1.8.3. Weryfikacja podatności systemu informatycznego na ingerencje ze strony osób trzecich

Weryfikacja powinna zostać przeprowadzona, co najmniej poprzez:

a.i.1. Przeprowadzenie testów penetracyjnych wykonanych ze stacji roboczej podłączonej do systemu informatycznego (Platformy) z sieci Internet.

a.i.2. Przeprowadzenie testów penetracyjnych wykonanych ze stacji roboczej podłączonej do wewnętrznego systemu informatycznego (Platformy) w celu zidentyfikowania możliwości przeprowadzenia włamania z wewnątrz sieci Zamawiającego.

1.9. Obszary bezpieczeństwa

Zamawiający wymaga, aby zakres weryfikacji bezpieczeństwa adresował ryzyka występujące w poniższej przedstawionych obszarach:

a) Uwierzytelnianie
b) Zarządzanie sesją
c) Kontrola dostępu
d) Walidacja wejścia
e) Kryptografia
f) Obsługa błędów i logowanie 7
g) . Ochrona danych
h) Bezpieczeństwo komunikacji
i) Wyszukiwanie złośliwego kodu
j) Logika biznesowa
k) Weryfikacja zasobów i plików

a.i.6. Raport audytorski

W wyniku przeprowadzonego Audytu Wykonawca sporządzi i dostarczy Raport audytorski składający się z:

a) szczegółowego raportu z testów penetracyjnych,
b) szczegółowego raportu z audytu kodów źródłowych,
c) szczegółowego raportu konfiguracji,
d) raportu podsumowującego wyniki raportów szczegółowych wraz z rekomendacjami dla kadry kierowniczej.

Raport audytorski powinien zawierać:

e) Szczegółowy opis i ocenę stanu wszystkich obszarów podlegających Audytowi
f) Wyniki testów i ich interpretację, w szczególności:

- Informacje dotyczące ogólnej oceny poziomu bezpieczeństwa oraz odporności na ataki Platformy, zawierające podsumowanie ilości stwierdzonych nieprawidłowości z oceną krytyczności.

- Opis lokalizacji wykrytych podatności - sposobu, w jaki można zlokalizować i powtórzyć testowy atak na podatność (Proof of Concept).
- Informacje na temat poziomu ochrony realizowanego przez Platformę zabezpieczeń.

g) Wnioski z Audytu (określenie ilościowego i jakościowego poziomu niebezpieczeństwa podatności).

h) Wykaz wszystkich problemów oraz wynikających z tego ryzyk wraz z oceną ryzyka wystąpienia wykrytych zagrożeń.

i) Rekomendacje i zalecenia dotyczące sposobów, metod i środków usunięcia stwierdzonych problemów, nieprawidłowości, podatności i ryzyk (lista poprawek oraz szczegółowy opis zalecanych zmian).

a.i.7. Gwarancja bezstronności

Wykonawca zobowiązuje się, że osoby zdolne do wykonania zamówienia złożą oświadczenie o bezstronności wykazując, że:

a) Nie brały i nie biorą udziału w pracach nad zaprojektowaniem, wykonaniem i wdrożeniem Platformy po stronie wykonawcy Platformy i podwykonawców.

b) Nie pozostają w żadnym stosunku faktycznym ani prawnym, który może budzić uzasadnione wątpliwości, co do bezstronności, z wykonawcą Platformy i podwykonawcami.

b.3. Budowa systemu bezpieczeństwa informacji

Zgodnie z wymaganiami prawnymi oraz dobrymi praktykami w zakresie ochrony informacji, ochrona danych osobowych wymaga budowy systemu bezpieczeństwa informacji.

Celem działania jest zapewnienie zgodności z obecnymi wymaganiami prawnymi w zakresie ochrony danych osobowych wynikających z wejścia w życie od 25 maja 2018 Rozporządzenia Parlamentu Europejskiego 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych. Dotychczas obowiązujące akty prawne w zakresie ochrony danych osobowych, między innymi ustawa z dnia 29 sierpnia 1997 roku o ochronie danych osobowych oraz rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych. Powyższe regulacje prawne w obecnym kształcie utraciły moc w dniu 25 maja 2018 roku.

Zakładany zakres prac:

1. Przegląd zbiorów danych osobowych oraz systemów służących do ich przetwarzania

   Przegląd zbiorów polega na zidentyfikowaniu wszystkich zbiorów danych osobowych występujących w urzędzie oraz analizie podstaw prawnych przetwarzania. Audytorzy oceniają spełnienie przez Klienta obowiązków (m.in.: informacyjnego, rejestracyjnego) nałożonych na niego przez prawo. Aplikacje i systemy informatyczne służące do przetwarzania danych osobowych podlegają ocenie pod kątem zgodności z wymaganiami prawnymi.

2. Szacowanie ryzyka dla danych osobowych

   Metodyka analizy ryzyka powinna opierać się na normie PN-ISO/IEC 27005. Wybór tej normy wynika z wymagań Rozporządzenia o Krajowych Ramach Interoperacyjności (Rozdział IV, § 20. 1 ust. 3). Zadanie obejmuje:

a.a) Określenie rejestru aktywów (listy składników aktywów informacyjnych – np. procesy, infrastruktura, systemy, zbiory danych, budynki, usługi zewnętrzne),

a.b) Określenie katalogu zagrożeń, które mogą wystąpić dla poszczególnych składników aktywów,

a.c) Przybliżona ocena wpływu danego zagrożenia na dany składnik aktywów,

a.d) Przybliżona ocena prawdopodobieństwa wystąpienia danego zagrożenia,

a.e) Ustalenie indeksu ryzyka, jako wypadkowej wpływu i prawdopodobieństwa (punkty 3 i 4),

a.f) Rekomendacje, co do zastosowania zabezpieczeń zmniejszających poziom ryzyka'

a.g) Przedstawienie ryzyk szczątkowych do akceptacji przez Kierownictwo.

3. Wsparcie przy opracowaniu lub aktualizacji dokumentacji

Zadanie obejmuje:

a) Opracowanie Polityki Bezpieczeństwa Danych Osobowych,

b) Opracowanie Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych,

c) Opracowanie instrukcji postępowania w przypadku naruszenia ochrony danych osobowych, Oferta usług w zakresie ochrony danych osobowych strona 4 z 6

d) Opracowanie (w oparciu o informacje przekazane przez Klienta) wymaganych przepisami prawa:

- wykazu zbiorów danych osobowych oraz systemów służących do ich przetwarzania,
- opisu struktury zbiorów danych osobowych,
- wykazu pomieszczeń przetwarzania danych osobowych,
- opisu przepływu danych między systemami,

e) Opracowanie ewidencji osób upoważnionych do przetwarzania danych osobowych oraz przygotowaniu upoważnień do przetwarzania danych osobowych dla pracowników.

b.4. Szkolenia użytkowników

1. Szkolenia w zakresie przyjmowanej Polityki bezpieczeństwa danych osobowych.

Tematyka szkolenia obejmuje podstawową wiedzę w zakresie:

- danych osobowych,
- omówienie uwarunkowań prawnych,
- wskazanie obowiązków pracowników wynikających z przyjmowanej Polityki bezpieczeństwa danych osobowych.

2. Szkolenia w zakresie cyberbezpieczeństwa.

Tematyka szkolenia obejmuje podstawową wiedzę w zakresie:

- Ochrona przed atakami socjotechnicznymi,
- Metody ochrony przed atakami,
- Ataki przez pocztę e-mail
- Ataki przez strony WWW
- Polityka haseł
- Bezpieczna praca z pakietem biurowym
- Bezpieczna praca z programem pocztowym
- Bezpieczna praca z przeglądarką internetową
- Bezpieczne przechowywanie i usuwanie danych

3. Szkolenia muszą być prowadzone przez wykwalifikowanych specjalistów Wykonawcy, posiadających niezbędną wiedzę fachową w zakresie tematyki szkoleń.
4. Szczegółowy harmonogram realizacji szkoleń zostanie uzgodniony z Zamawiającym.

b.5.Przygotowanie dokumentacji kończącej projekt celem jego rozliczenia i zakończenia

a) W zakresie rozliczeń Umów zawartych z wykonawcami robót budowlanych, usług, dostaw, nadzorów i innych wchodzących w zakres inwestycji:

- Kontrola kosztów we wszystkich fazach realizacji inwestycji;
- Analiza harmonogramów płatności dla Wykonawców względem zakończonych robót, dostaw i przedstawienie jej Zamawiającemu;
- Weryfikacja zatwierdzonych do zapłaty faktur wystawionych przez Wykonawców w związku z realizacją inwestycji. Sprawdzenie dokumentów rozliczeniowych pod względem merytorycznym i rachunkowym;
- Kontrolowanie i rozliczenie inwestycji w zgodności z podpisanymi umowami na wykonanie robót budowlano-instalacyjnych/dostaw wyposażenia;
- Weryfikacja prowadzonej ewidencji księgowej w zakresie realizowanej inwestycji;
- Weryfikacja dokumentów inwestycji, w tym protokołów odbiorów częściowych i odbioru końcowego z udziałem przedstawicieli uczestników procesu inwestycyjnego;
- Weryfikacja konieczności naliczania kar umownych należnych Zamawiającemu i przekazanie danych Zamawiającemu w celu ich zatwierdzenia;
- Dokonanie rozliczenia kosztu inwestycji w terminie 30 dni od daty odbioru końcowego inwestycji oraz po dokonaniu zapłaty wszystkich faktur przez Zamawiającego, a następnie przekazanie Zamawiającemu ostatecznej informacji o poniesionych dodatkowych kosztach;
- Przygotowanie dokumentów oraz dowodów księgowych (zgodnie z obowiązującymi przepisami), będących podstawą wprowadzenia do ewidencji księgowej efektów zrealizowanej inwestycji w postaci środków trwałych;
- Wykonanie czynności wynikających z praw i obowiązków Zamawiającego w zakresie gwarancji i rękojmi za wady fizyczne obiektu.
- Pisemne powiadamianie Wykonawcy robót budowlano-instalacyjnych/dostaw wyposażenia o zgłaszanych przez Zamawiającego usterkach i wadach, a także egzekwowanie od Wykonawcy ich usunięcia.
- Udział w przeglądzie gwarancyjnym obiektów budowlanych i nadzór nad usuwaniem wad i usterek przez Wykonawców w okresie gwarancyjnym i rękojmi.
- Organizowanie przeglądów budowlanych w okresie udzielonych gwarancji oraz w okresie rękojmi a w szczególności przed zwolnieniem zabezpieczenia należytego wykonania umowy.
- Sporządzanie protokołów z przeglądów gwarancyjnych.
- Występowanie w imieniu Zamawiającego oraz naliczanie i egzekwowanie kar umownych od

Wykonawców za niezgodne z Umową wykonanie robót budowlano-instalacyjnych/dostaw wyposażenia bądź nieterminowe usunięcie wad.

- Dokonanie ostatecznego odbioru po upływie terminu gwarancji i rękojmi ustalonego w Umowach z Wykonawcami.
- Zarekomendowanie Zamawiającemu zwrotu zabezpieczeń i ewentualnej kwoty zatrzymanej po terminie zgłaszania wad.

b) W zakresie rozliczenia Umowy o dofinansowanie projektu zawartą z Mazowiecką Jednostką Wdrażania Projektów Unijnych:

- Analiza oszczędności w projekcie w stosunku do założeń harmonogramu rzeczowo-finansowego projektu;
- W miarę zaistniałych okoliczności wnioskowanie do Instytucji zarządzającej (MJWPU) o zgodę na zagospodarowanie oszczędności w projekcie;
- Aktualizacja harmonogramów realizacji projektu;
- Aktualizacja kolcowania wniosku o dofinansowanie projektu;
- Przygotowanie dokumentacji do końcowego rozliczenia – aneks końcowy do umowy;
- Weryfikacja wskaźników realizacji projektu: wskaźniki produktu oraz wskaźniki rezultatu;
- Nadzór nad utrzymaniem wskaźników projektu w okresie jego trwałości zgodnie z warunkami umowy o dofinansowanie projektu.