Znak sprawy: 8/WOMP-ZCLiP/2022 *Załącznik Nr 2 do SWZ*

OPIS PRZEDMIOTU ZAMÓWIENIA

I. Nazwa:

Informatyzacja WOMP-ZCLiP w Szczecinie w ramach projektu pn. „Zachodniopomorskie e-Zdrowie” współfinansowanego środkami Unii Europejskiej w ramach Regionalnego Programu Operacyjnego Województwa Zachodniopomorskiego na lata 2014-2020 Oś Priorytetowa 9 Infrastruktura publiczna, Działanie 9.10 Wsparcie rozwoju e-usług publicznych (e-Zdrowie).

II. Nazwy i kody Wspólnego Słownika Zamówień (Klasyfikacji CPV):

48180000-3 Pakiety oprogramowania medycznego,
48780000-9 Pakiety oprogramowania do zarządzania systemem, przechowywaniem i zawartością,
48000000-8 - Pakiety oprogramowania i systemy informatyczne,
48700000-5 - Pakiety oprogramowania użytkowego,
48761000-0 - Pakiety oprogramowania antywirusowego,
45300000-0 - Roboty instalacyjne w budynkach,
32420000-3 - Urządzenia sieciowe,
30233000-1 – Urządzenia do przechowywania i odczytu danych,
48600000-4 – Pakiety oprogramowanie dla baz danych i operacyjne,
72000000-5 - Usługi informatyczne: konsultacyjne, opracowywania oprogramowania, internetowe i wsparcia (w tym 72263000-6 - Usługi wdrażania oprogramowania).

Spis treści

Rozdział I. Założenia początkowe oraz wymagania ogólne

I.1 Wprowadzenie

Zamówienie realizowane jest w ramach projektu „Zachodniopomorskie e-Zdrowie" współfinansowanego środkami Unii Europejskiej w ramach Regionalnego Programu Operacyjnego Województwa Zachodniopomorskiego na lata 2014-2020 Oś Priorytetowa 9 Infrastruktura publiczna, Działanie 9.10 Wsparcie rozwoju e-usług publicznych (e-Zdrowie).
Przedmiotowe postępowanie dotyczy informatyzacji WOMP-ZCLiP w Szczecinie będącego jednocześnie Zamawiającym i Partnerem Projektu.

I.2 Integracja z centralnym systemem e-zdrowie

1. Dostarczony przez Wykonawcę Szpitalny System Informatyczny (SSI) w ramach realizacji niniejszego przedmiotu zamówienia musi zapewniać integrację funkcjonalną z systemem teleinformatycznym, o którym mowa w art. 7 ust. 1 ustawy z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia (t.j. Dz.U.2022 poz.1555 z późn. zm.) co najmniej w zakresie opisanym w dokumentach opublikowanych przez Centrum e-Zdrowie (dotychczas CSIOZ), tj.:
   1) „Opis usług biznesowych Systemu P1 wykorzystywanych w systemach usługodawców",
   2) „Opis funkcjonalny Systemu P1 z perspektywy integracji systemów zewnętrznych"

   oraz dokumentacją:
   3) „Minimalne wymagania dla systemów usługodawców" https://www.gov.pl/web/zdrowie/minimalne-wymagania-dla-systemow-uslugodawcow
   4) Dokumentacja integracyjna Systemu P1 w zakresie obsługi ZM,
   5) Dokumentacja integracyjna Systemu P1 w zakresie obsługi EDM,
   6) Dokumentacja integracyjna Systemu P1 w zakresie obsługi zgód pacjenta
   7) Dokumentacja integracyjna Systemu P1 w zakresie Systemu Elektronicznej Rejestracji.
2. W zakresie integracji i komplementarności z centralnymi systemami e-zdrowie, na Wykonawcy będzie spoczywał obowiązek dostosowania zaoferowanego rozwiązania do wymagań ujętych w dokumentach publikowanych poprzez Centrum e-Zdrowia, w tym w szczególności do wszelkiej dokumentacji integracyjnej.
3. Dokumenty, o których mowa powyżej są dostępne na stronie internetowej Centrum e-Zdrowia, pod adresem: http://csioz.gov.pl oraz https://ezdrowie.gov.pl/portal/home/dla-dostawcow/interfejsy. **Zamawiający informuje, iż dokumenty dostępne na w/w stronach internetowych są aktualizowane. Wykonawca zobowiązany jest do weryfikowania czy dokumenty dostępne na w/w stronach uległy zmianie lub aktualizacji i zastosowania przy wykonywaniu Przedmiotu Zamówienia najnowszych dostępnych wersji tych dokumentów.**
4. W zakresie integralności zaoferowanego SSI Wykonawca musi uwzględnić i wdrożyć poniższe wytyczne i założenia:
   1) Dostępność Systemu P1 dla odpowiednio zarejestrowanych w Centrum e-Zdrowia systemów usługodawców i systemów regionalnych wyłącznie poprzez standardowe interfejsy Web Services. Wymagane jest dwustronne uwierzytelnianie systemów nawiązujących komunikację, a także podpisywanie komunikatów certyfikatem dostarczanym bądź wskazanym przez Centrum e-Zdrowia.
   2) Przesyłanie komunikatów do P1 podpisanych elektronicznie przez system komunikujący się z Systemem P1 certyfikatem wydanym przy zakładaniu konta usługodawcy (rejestrowaniu systemu). Wymagania w zakresie rodzaju stosowanego certyfikatu mogą ulec zmianie w wyniku w przypadku zmiany centralnych rozwiązań w zakresie uwierzytelniania użytkowników w obszarze e-zdrowia.

3) Obowiązywanie Modelu Informacji o Zdarzeniu Medycznym i Indeksie Dokumentacji Medycznej (dalej: EDMiZM) w przypadku informacji o zdarzeniu medycznym, publikowanymi przez Centrum e-Zdrowia na stronie internetowej: https://ezdrowie.gov.pl/portal/home/dla-dostawcow/interfejsy.
4) Obowiązywanie EDMiZM publikowanego przez Centrum e-Zdrowia w przypadku rejestru (indeksu) Elektronicznej Dokumentacji Medycznej na stronie internetowej: https://ezdrowie.gov.pl/portal/home/dla-dostawcow/interfejsy. .
5) Zgoda pacjenta na udostępnienie jego dokumentacji medycznej – funkcjonalność ta jest wymagana i powinna być zgodna z modelem dokumentu zgody oraz modelami interfejsów pozwalających na wnioskowanie o zgodę, które zostały opublikowane przez Centrum e-Zdrowia na stronie internetowej: https://ezdrowie.gov.pl/portal/home/dla-dostawcow/interfejsy.
6) Wymiana Elektronicznej Dokumentacji Medycznej (dalej: EDM) – funkcjonalność ta jest wymagana i powinna być zgodna z modelem wniosku i dokumentu udostępnienia oraz modelami interfejsów, które zostały opublikowane przez Centrum e-Zdrowia na stronie internetowej: https://ezdrowie.gov.pl/portal/home/dla-dostawcow/interfejsy.
7) Konieczność rozbudowy funkcjonalnej użytkowanych systemów oprogramowania dla zapewnienia integracji systemu HIS podmiotu leczniczego (zewnętrznego w stosunku do P1) celem osiągnięcia funkcjonalności Systemu Elektronicznej Rejestracji (e-Rejestracji centralnej).

5. Jednocześnie, zaoferowany SSI musi spełniać następujące założenia funkcjonalne:
   1) prowadzenie i wymiana Elektronicznej Dokumentacji Medycznej (EDM), w tym indywidualnej dokumentacji medycznej (wewnętrznej i zewnętrznej) z uwzględnieniem rozwiązania umożliwiającego zbieranie przez podmiot udzielający świadczeń opieki zdrowotnej, jednostkowych danych medycznych w elektronicznym rekordzie pacjenta oraz tworzenie EDM zgodnej co najmniej ze standardem HL7 CDA, opracowanym i opublikowanym przez Centrum e-Zdrowie – Polską Implementacją Krajową HL7 CDA (tzw. IG).
   2) prowadzenie lokalnego repozytorium EDM (z obsługą przechowywania EDM) oraz uwzględniać rozwiązania zapewniające wymianę EDM pomiędzy repozytorium Zamawiającego a Platformą P1. Platforma P1 będzie zawierała indeks EDM (Rejestr EDM), w którym będą się znajdować informacje o EDM tworzonym i przechowywanym u Zamawiającego.
   3) Przeniesienie ok 700 000 dokumentów z obecnie używanego rozwiązania repozytorium chmurowego EDM firmy Kamsoft do Lokalnego Repozytorium EDM budowanego w ramach niniejszego postępowania. Efektem przeniesienia dokumentów do lokalnego repozytorium ma być informacja w P1 o zmianie lokalizacji dokumentów elektronicznych z chmurowego rozwiązania Kamsoft na Lokalne Repozytorium EDM Zamawiającego,
   4) przechowywanie zaindeksowanych dokumentów EDM przeznaczonych do udostępniania na platformie P1 przez Lokalne Repozytorium EDM. Lokalne Repozytorium EDM pełnić będzie funkcję Document Repository.
   5) W przypadku skorzystania z prawa opcji (opcja nr 1) opisanego w rozdziale II.5 przechowywanie zaindeksowanych dokumentów EDM przeznaczonych do udostępniania na platformie P1 przez Regionalne Repozytorium EDM. Regionalne Repozytorium EDM pełnić będzie funkcję Document Repository.
   6) Repozytorium EDM musi realizować co najmniej usługę przyjmowania, archiwizacji i udostępniania EDM zgodnej z PIK HL7 CDA, a w przypadku repozytoriów badań obrazowych, przyjmowanie, archiwizację i udostępnianie obiektów DICOM.

I.3 Akty prawne

Dostarczone rozwiązania teleinformatyczne, ze szczególnym uwzględnieniem dostarczanego i wdrażanego Oprogramowania, muszą być zgodne z powszechnie obowiązującymi przepisami prawa polskiego i europejskiego. Oprogramowanie musi pozwalać na gromadzenie, przetwarzanie i analizowanie danych i informacji w obszarach objętych wdrożeniem, na bazie tych danych musi umożliwiać wytwarzanie prawidłowej, kompletnej, ujętej w obowiązujących przepisach prawa dokumentacji (dokumenty, raporty, wykazy, oświadczenia, zaświadczenia itp.).

I.4 Zakres zamówienia

Zamawiający wymaga rozbudowy dotychczas użytkowanego systemu HIS poprzez realizację zamówienia opisanego w poniższych rozdziałach:

- wariant podstawowy – rozdz. II.1, II.2, II.3, II.4
- wariant opcjonalny – wariant podstawowy + opcja nr 1 i opcja nr 2 wskazane w rozdz. II.5 niniejszego OPZ.

W formularzu ofertowym Wykonawca musi wycenić oba warianty. Wariant opcjonalny jest opcją w rozumieniu art. 441 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych, zwanej dalej ustawą Pzp (t.j. Dz.U. z 2022 poz. 1710 ze zm.).

I.5 Ogólny opis przedmiotu zamówienia

1. Przedmiot zamówienia obejmuje:

a) Modernizacja sieci teleinformatycznej i serwerowni w zakresie:

Poz. OPZ	OPIS	ILOŚĆ
Rozdział II.1	**Modernizacja sieci teleinformatycznej**	
II.1.1	Poprawa stanu technicznego Serwerowni	1 kpl.
II.1.2	Urządzenie zabezpieczające UTM	2 kpl.

b) Infrastruktura serwerowa w zakresie:

Poz. OPZ	Opis	Ilość
Rozdział II.2	**Infrastruktura serwerowa i sieciowa**	
II.2.1	Pamięć masowa NAS	1

c) Oprogramowanie systemowe i narzędziowe w zakresie:

POZ. OPZ	OPIS	ILOŚĆ
ROZDZIAŁ II.3	**OPROGRAMOWANIE SYSTEMOWE I NARZĘDZIOWE**	
II.3.1	Serwerowy system operacyjny	1
II.3.2	Oprogramowanie antywirusowe	1

d) dostawa i wdrożenie e-usług do Systemu WOMP:

POZ. OPZ	OPIS
ROZDZIAŁ II.4	**SZPITALNY SYSTEM INFORMATYCZNY**

II.4	a. EDM a. Zdarzenia medyczne (integracja z P1 – raportowanie ZM, indeksowanie EDM) b. Lokalne Repozytorium EDM e-Usługi – dostawa i wdrożenie a. EDM dla lekarza b. EDM dla pacjenta c. eRejestracja lokalna z powiadomieniami d. Integracja z krajowym Systemem Elektronicznej Rejestracji na platformie

2. Przedmiot zamówienia musi być dostarczany, wdrożony i zainstalowany w całości w siedzibie Zamawiającego (ul. Bol. Śmiałego 33 w Szczecinie) oraz w placówkach, w których Zamawiający świadczy usługi zdrowotne (ul. Kopernika 18 Szczecin, ul. Mickiewicza 18 Stargard, Aleja Żołnierza 5 Stargard).
3. Wykonawca musi skalkulować w cenie wszystkie dostawy i usługi objęte Przedmiotem Zamówienia, w szczególności: dostawy sprzętu i oprogramowania, wynagrodzenie za przeniesienie praw autorskich lub udzielenie licencji, wsparcie techniczne wraz z aktualizacjami (gwarancję), koszt wdrożenia, zamówienie w wariancie opcjonalnym (opcja nr i nr 2).
4. Wszystkie dostarczane Produkty (rozumiane jako elementarny efekt działań/prac/dostaw objętych całym zakresem przedmiotu zamówienia wykonywanych przez Wykonawcę podczas realizacji Umowy w poszczególnych Etapach) oraz Komponenty (rozumiane jako integralna część dostawy i wdrożenia przedmiotu zamówienia, składający się przynajmniej z jednego Produktu lub wielu Produktów powiązanych ze sobą merytorycznie) podlegają dostawom, usługom projektowania, instalacji, konfiguracji i wdrożenia.
5. Usługi projektowania, instalacji, konfiguracji i wdrożenia Wykonawca przeprowadzi zgodnie z zapisami niniejszego OPZ w uzgodnieniu z Zamawiającym, zgodnie z obowiązującymi przepisami, zasadami wykonywania projektów teleinformatycznych, z uwzględnieniem standardu WCAG 2.1 oraz najlepszymi praktykami w ich realizacji.
6. Wykonawca jest zobowiązany do realizacji Przedmiotu Zamówienia zgodnie z zasadami i wytycznymi Zamawiającego, zapisami OPZ, SWZ oraz Umowy.

   Ilekroć w niniejszym OPZ Zamawiający użył w opisie oznaczeń norm, aprobat, specyfikacji technicznych i systemów odniesienia, o których mowa w art. 101 ust. 1-3 albo art. 99 ust. 5 ustawy Pzp należy je rozumieć jako przykładowe. Zamawiający zgodnie z art. 101 ust. 4 ustawy Pzp dopuszcza rozwiązanie równoważne opisywanym w treści SWZ. Jeżeli zapisy zawarte w OPZ wskazywałyby w odniesieniu do rozwiązań, materiałów lub urządzeń znaki towarowe lub pochodzenie Zamawiający, zgodnie z art. 101 ust 4 ustawy Pzp, dopuszcza składanie ofert na rozwiązanie równoważne. Wszelkie „produkty" pochodzące od konkretnych producentów określają minimalne parametry jakościowe i cechy użytkowe, jakim musi odpowiadać produkt, aby spełnić wymagania stawiane przez Zamawiającego i stanowią wyłącznie wzorzec jakościowy przedmiotu zamówienia. Poprzez zapis dot. minimalnych wymagań parametrów jakościowych Zamawiający rozumie wymagania materiałów, sprzętu i urządzeń zawarte w ogólnie dostępnych źródłach, katalogach, stronach internetowych producentów. Operowanie przykładowymi nazwami producenta ma jedynie na celu doprecyzowanie poziomu oczekiwań Zamawiającego w stosunku do określonego rozwiązania. Tak więc posługiwanie się nazwami producentów /produktów/ ma wyłącznie charakter przykładowy. Zamawiający, przy opisie przedmiotu

zamówienia, wskazując oznaczenie konkretnego producenta (dostawcy) lub konkretny produkt, dopuszcza jednocześnie produkty równoważne o parametrach jakościowych i cechach użytkowych, co najmniej na poziomie parametrów wskazanego produktu, uznając tym samym każdy produkt o wskazanych parametrach lub lepszych. W takiej sytuacji Zamawiający wymaga złożenia stosownych dokumentów, wykazujących spełnienie przez produkty równoważne ww. parametrów i cech. Wykonawca musi dostarczyć wszelkie urządzenia i elementy, które są niezbędne do prawidłowego funkcjonowania całości. W przypadku, gdy w trakcie realizacji Przedmiotu Zamówienia okaże się, że brakuje jakiegokolwiek urządzenia lub elementu, którego brak spowoduje nieprawidłowe funkcjonowanie całości Przedmiotu Zamówienia, Wykonawca dostarczy je na własny koszt i ryzyko.

7. Zamawiający wymaga, aby zaoferowane rozwiązanie (system) było rozwiązaniem istniejącym, działającym, gotowym do wdrożenia i zapewniającym realizację wszystkich wymaganych w SWZ (w szczególności OPZ) funkcjonalności na dzień składania ofert i nie może być w fazie opracowywania, budowy, testów, projektowania itp.
8. Wszelkie dostarczane urządzenia:
   1) muszą być fabrycznie nowe, pochodzić z autoryzowanego kanału sprzedaży producenta i reprezentować model bieżącej linii produkcyjnej. Nie dopuszcza się urządzeń: odnawianych, demonstracyjnych lub powystawowych. Urządzenia muszą posiadać gwarancję na okres co najmniej 5 lat,
   2) nie dopuszcza się urządzeń posiadających wadę prawną w zakresie pochodzenia sprzętu, wsparcia technicznego i gwarancji producenta,
   3) elementy, z których zbudowane są urządzenia muszą być produktami producenta urządzeń lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta,
   4) urządzenia i ich komponenty muszą być oznakowane w taki sposób, aby możliwa była identyfikacja zarówno produktu jak i producenta,
   5) urządzenia muszą być dostarczone Zamawiającemu w oryginalnych opakowaniach producenta,
   6) do każdego urządzenia musi być dostarczony komplet standardowej dokumentacji dla użytkownika w języku polskim lub angielskim w formie papierowej lub elektronicznej,
   7) specyfikacja urządzeń nie może podlegać modyfikacjom.

I.6 Termin realizacji Przedmiotu Zamówienia

Wykonawca zrealizuje przedmiot Umowy w terminie **do dnia 31.10.2023 r**.

I.7 Powiązania między OPZ a Modelem Realizacyjnym

1. Zakres, kształt oraz funkcjonalności poszczególnych usług elektronicznych dla wszystkich podmiotów leczniczych uczestniczącym w projekcie „Zachodniopomorskie e-Zdrowie” określone zostały w Modelu realizacyjnym – **załącznik nr 4** do SWZ.
2. W przypadku różnic w zakresie e-usług oraz funkcjonalności Projektu ZeZ między niniejszym Opisem Przedmiotu Zamówienia Partnera a Modelem realizacyjnym nadrzędne są wymagania zawarte w niniejszym Opisie Przedmiotu Zamówienia oraz Umowie.

I.8 Organizacja wdrożenia

I.8.1.1 Założenia podstawowe

1. Przedmiot Zamówienia będzie realizowany w oparciu o zdefiniowany uprzednio przez Wykonawcę i zaakceptowany Harmonogram wdrożenia, który musi być pisemnie uzgodniony i zaakceptowany przez Zamawiającego oraz odpowiednio aktualizowany w toku realizacji Przedmiotu Zamówienia. Zmiany Harmonogramu wymagają uzgodnienia i pisemnej akceptacji Zamawiającego.
2. Wykonawca w Harmonogramie wdrożenia musi uwzględnić w szczególności podział na zadania takie jak projektowanie, dostawy, usługi instalacji/konfiguracji, testowanie, wdrożenie i odbiory.
3. Wykonawca umożliwi Zamawiającemu udział we wszystkich pracach realizowanych przez Wykonawcę w ramach realizacji Przedmiotu Zamówienia (m.in. w czasie projektowania, dostaw, instalacji/budowy, konfiguracji, wdrożeniu, testowaniu i odbiorach).
4. Wykonawca zobowiązany jest do udziału w cyklicznych naradach przeglądu prac w siedzibie Zamawiającego. Zamawiający przewiduje częstotliwość narad 1 raz w tygodniu lub rzadziej za zgodą obu stron.
5. Wykonawca zobowiązany jest przeprowadzić dostawy Przedmiotu Zamówienia w dokładnych terminach i godzinach uzgodnionych z Zamawiającym.
6. W przypadku dostarczania Infrastruktury Serwerowej oraz Sieciowej musi być ona oznakowana w taki sposób, aby możliwa była identyfikacja systemowa zarówno produktu jak i producenta, pochodzić z oficjalnych kanałów dystrybucji producentów i dostarczona w oryginalnych opakowaniach fabrycznych.
7. Wdrożenie należy rozumieć jako szereg uporządkowanych i zorganizowanych działań mających na celu wykonanie Przedmiotu Zamówienia.
8. Wdrożenie będzie realizowane w ramach powołanych do tego celu struktur organizacyjnych po stronie Wykonawcy.
9. W ramach wdrożenia Wykonawca przygotuje informacje na temat struktury organizacyjnej Zespołu Wykonawcy zajmującej się realizacją Przedmiotu Zamówienia, w ramach której muszą zostać powołane minimum następujące role:
    1) Kierownik Projektu ze strony Wykonawcy,
    2) Zespół Wdrożeniowy ze strony Wykonawcy.
10. Wdrożenie, z zastrzeżeniami wskazanymi poniżej, w punktach muszą realizować osoby wymienione w ofercie Wykonawcy, przy czym:
    1) Osoby Zespołu Wykonawcy muszą być dyspozycyjne w trakcie wykonywania prac,
    2) Wykonawca przekaże Zamawiającemu wykaz numerów telefonów kontaktowych oraz adresów mailowych do kluczowych osób biorących udział w realizacji Przedmiotu Zamówienia po stronie Wykonawcy.
11. Wykonawca zorganizuje prace tak, aby w maksymalnym stopniu nie zakłócać ciągłości funkcjonowania prac u Zamawiającego. Wykonawca ponosi pełną odpowiedzialność, w tym finansową jeżeli na skutek swojej działalności doprowadzi do przestoju przychodni bądź utraty danych Zamawiającego w którymkolwiek z już istniejących systemów.

12. Obiekty podlegające inwestycji (obiekty służby zdrowia, w których świadczone są usługi medyczne) są użytkowane w trybie ciągłym w czasie godzin pracy przez cały okres wykonywania Przedmiotu Zamówienia, co może powodować utrudnienia w miejscu prowadzenia prac. Nie ma możliwości całkowitego wyłączenia i zamknięcia w/w obiektów lub ich części na czas realizacji Przedmiotu Zamówienia. Poszczególne prace będą realizowane etapowo, tak aby zachować ciągłość świadczenia usług medycznych.
13. Wykonawca musi uwzględnić, że wszystkie prace wykonywane będą w użytkowanych obiektach przy dużym ruchu pracowników i chorych, tzn. organizacja prac musi przede wszystkim zapewniać bezpieczeństwo pracowników i pacjentów w godzinach pracy Zamawiającego.

I.8.1.2 Przygotowanie Dokumentacji

1. W ramach realizowanych prac Wykonawca musi opracować dla Zamawiającego Dokumentację Przedmiotu Zamówienia (zwaną dalej Dokumentacją), która składa się z nw. zakresów:
   1) Harmonogram Wdrożenia,
   2) Dokumentacja Analizy Przedwdrożeniowej (DAP),
   3) Dokumentacja Powykonawcza.
2. Dokumentacja powyższa musi zawierać bazowe zapisy opisujące budowane rozwiązania, procesy oraz sposób organizacji prac i wdrożenia. Na podstawie zapisów w Dokumentacji będą prowadzone i odbierane poszczególne etapy realizowane w ramach Przedmiotu Zamówienia. Dokumenty te wraz ze SWZ z załącznikami będą stanowiły podstawę do weryfikacji wdrożenia w trakcie odbiorów.
3. Dokumentacja podlega uzgadnianiu i akceptacji Zamawiającego. Akceptacja Harmonogramu wdrożenia i DAP warunkuje rozpoczęcie prac Wykonawcy.
4. Dokumentacja Analizy Przedwdrożeniowej DAP wraz z Harmonogramem wdrożenia muszą być opracowane w oparciu o wymagania określone w niniejszym OPZ.

I.8.1.3 Harmonogram wdrożenia

Wykonawca zobowiązany jest opracować na podstawie SWZ oraz OPZ szczegółowy Harmonogram wdrożenia. Harmonogram należy przedstawić Zamawiającemu **w terminie do 14 (czternastu) dni od daty zawarcia Umowy.**

I.8.1.4 Analiza Przedwdrożeniowa

1. Jako Analizę Przedwdrożeniową należy rozumieć zakres czynności do wykonania przez Wykonawcę mający na celu analizę środowiska biznesowego i informatycznego Zamawiającego. W wyniku przeprowadzenia Analizy przedwdrożeniowej Wykonawca przedstawi Zamawiającemu Dokumentację Analizy Przedwdrożeniowej (zwaną dalej DAP), na podstawie której będzie realizowany organizacyjnie i technicznie Przedmiot Zamówienia. Dokumentacja Analizy Przedwdrożeniowej będzie podlegała uzgodnieniu i akceptacji Zamawiającego.
2. Dokumentacja Analizy Przedwdrożeniowej musi zawierać w szczególności:

ZAWARTOŚĆ DOKUMENTACJI ANALIZY PRZEDWDROŻENIOWEJ DAP
1. Wymagane dane w zakresie SSI:
1) wykaz oraz szczegółowy opis i harmonogram budowy SSI i e-usług,
2) architektura SSI i e-usług,

3)	analiza migracji danych oraz opis sposobu migracji – jeżeli dotyczy,
4)	przygotowanie planu modernizacji sieci teleinformatycznej,
5)	przygotowanie planu instalacji i konfiguracji sprzętu sieciowego,
6)	przygotowanie planu instalacji Infrastruktury serwerowej z uwzględnieniem rozmieszczenia sprzętu w lokalizacjach Zamawiającego,
7)	przygotowanie planu instalacji i konfiguracji infrastruktury komputerowej,
8)	jednoznacznie określone założenia integracji z innymi systemami informatycznymi, które posiada Zamawiający,
9)	plan pracy na dalsze etapy Wdrożenia,
10)	plan migracji danych z SSI, który posiada Zamawiający – jeżeli dotyczy,
11)	szczegółowa specyfikacja oprogramowania objętego zakresem umowy,
12)	wykaz oraz szczegółowy opis i harmonogram niezbędnych prac konfiguracyjnych,
13)	ustawienia konfiguracyjne urządzeń i oprogramowania wchodzących w skład SSI,
14)	propozycje scenariuszy testowych uwzględniających zakres czynności operacyjnych, które należy wykonać w celu potwierdzenia, że wskazane wymagane funkcjonalności zostały prawidłowo skonfigurowane i działają zgodnie z opisami procesów,
15)	harmonogram instruktażu personelu oraz administratorów SSI.
2.	**Wymagane dane ZARZĄDCZE:**
	plan i sposób komunikacji Stron.
3.	**Wymagane dane dotyczące INFRASTRUKTURY SERWEROWEJ, SIECIOWEJ I KOMPUTEROWEJ:**
1)	podział Przedmiotu Zamówienia na Produkty, a następnie ich pogrupowanie w Komponenty,
2)	analiza wymagań Przedmiotu Zamówienia zawierająca opis sposobu realizacji wymagań, sposób testowania i odbioru,
3)	karty katalogowe urządzeń potwierdzające spełnienie wymagań,
4)	plan dostaw,
5)	opis prac modernizacji Sieci teleinformatycznej,
6)	opis instalacji i wdrożenia Oprogramowania wdrażanego wraz z Infrastrukturą serwerową,
7)	opis modernizacji i budowy Infrastruktury serwerowej, sieciowej oraz komputerowej,
8)	lista Komponentów, które będą podlegały osobnym odbiorom – jeżeli dotyczy,
9)	szczegółowy zakres i zawartość pozostałej Dokumentacji.

I.8.1.5 Dokumentacja Powykonawcza

1. Warunkiem dokonania Odbioru Końcowego jest dostarczenie przez Wykonawcę Dokumentacji Powykonawczej obejmującej dokumentację użytkową, techniczną i eksploatacyjną. Dokumentacja Powykonawcza musi być dostarczona w języku polskim, w wersji elektronicznej w formacie edytowalnym oraz w co najmniej jednym egzemplarzu papierowym.
2. W dokumentacji muszą być zawarte opisy wszelkich cech, właściwości i funkcjonalności pozwalających na poprawną z punktu widzenia technicznego eksploatację rozwiązań.
3. W szczególności dokumentacja ta musi zawierać:

1) Wymogi ogólne:

a) pełen sposób licencjonowania wszystkich elementów aplikacji i środowiska,

b) opis architektury technicznej:
   - wyszczególnienie oraz opis powiązań wszystkich komponentów sprzętowych, systemowych i aplikacyjnych występujących lub wymaganych do poprawnej pracy aplikacji zgodnie z wymaganiami wydajności, funkcjonalności i bezpieczeństwa (minimalny, maksymalny, rekomendowany),
   - dokładne określenie wykorzystywanych i dopuszczalnych wersji dla komponentów innych dostawców,
c) konfiguracja musi obejmować wszystkie wdrożone urządzenia, zainstalowane w ramach budowy systemu IT,
d) przykładowy zestaw wymaganych danych konfiguracyjnych obejmuje:
   - serwery – parametry sprzętowe (procesor, pamięć, dyski, karty sieciowe, zasilanie, itp.),
   - sieć (adresacja IP, itp.),
   - podsystem dyskowy (punkty montowania/litery dysków, wolumeny logiczne, grupy wolumenowe, zasoby dyskowe, RAID, itp.),
   - system operacyjny (parametry jądra, moduły, usługi, stos TCP/IP, itp.),
   - klaster (węzły fizyczne, paczki klastrowe, kolejność przełączania, itp.),
   - listę zainstalowanego oprogramowania, itp.,
   - pamięć masowa NAS – parametry sprzętowe (dyski, karty itp.), grupy dyskowe, zasoby dyskowe, itp.,
   - sprzęt sieciowy – parametry sprzętowe, podział na VLAN-y itp.,
e) opis architektury logicznej:
   - schemat i opis powiązań logicznych poszczególnych komponentów i ich role w architekturze,
f) mapę i opis interface'ów:
   - interfejsy muszą zawierać szczegółowy opis techniczny, w szczególności zawierać informację o: typie interfejsu, wykorzystywanych protokołach, portach sieciowych, strukturze interfejsu, itp. oraz o zakresie wymiany danych i sposobu kontroli prawidłowości działania,
g) opis wymagań sprzętowych, systemowych, sieciowych itp.:
   - wymagania dla poszczególnych komponentów architektury, odniesienia do oczekiwanych wymagań wydajnościowych, funkcjonalnych i bezpieczeństwa (minimalny, maksymalny, rekomendowany),
h) procedury lub instrukcje instalacji, reinstalacji, deinstalacji oraz aktualizacji:
   - szczegółowy opis postępowania w przypadku tworzenia lub zmian w środowisku; jeśli wykorzystywane są procedury innych dostawców dla standardowych komponentów (np. baz danych) wystarczy wskazać w dokumentacji szczegółowe odniesienie do procedur standardowych właściwych dla tych komponentów,
i) dokumentację administracyjną związaną z poprawną eksploatacją:
   - opis (w postaci procedur lub instrukcji) wszystkich rutynowych czynności administracyjnych dla aplikacji i systemu informatycznego (dziennych, tygodniowych, miesięcznych itp.) oraz działań pozwalających na utrzymanie wymaganej dostępności, wydajności i bezpieczeństwa,
j) dokumenty z testów:
   - plan testów, scenariusze testowe i protokoły z testów akceptacyjnych, wydajnościowych, testów operacji administratora technicznego oraz testów bezpieczeństwa w tym ciągłości działania (przełączanie, odtwarzanie, weryfikacja poprawności),
k) dokumentację wdrożeniową:

- dokumentacja powdrożeniowa: zawiera szczegółowy opis wykonanych czynności instalacyjnych oraz konfiguracyjnych wszystkich komponentów systemu,
- dokumentacja parametryzacji: wyszczególnienie wartości wszystkich ustawionych parametrów użytkowych zarówno samej aplikacji jak i pozostałych komponentów systemu, parametry systemu operacyjnego oraz parametry sprzętu, w tym konfiguracji środowiska produkcyjnego (serwery baz danych, serwery aplikacji, inne zastosowane),
- dokumentacja uruchomieniowa: opisuje wszystkie istotne kroki (czynności) wykonane w celu pierwszego uruchomienia aplikacji/systemu, w tym opis migracji/konwersji danych, testy uruchomieniowe,
- dokumentacja pilotażowa: jeśli był stosowany w trakcie wdrożenia pilotaż jako element stabilizacji i testów,

l) wersjonowanie:
- opis zasad wersjonowania i sposobu patchowania aplikacji,

m) zalecenia:
- opis zasad i zaleceń strojenia aplikacji,

n) instrukcje obsługi i instrukcje użytkowania dla wersji dostarczonego oprogramowania z podziałem na poszczególne moduły,

o) w zakresie obszarów administratora dokumentacja musi zawierać dodatkowo co najmniej:
- opis podstawowych ról użytkowników i zasad ich kreowania,
- opis zarządzania uprawnieniami użytkownika i tworzenia profili,
- lista dostępnych uprawnień użytkownika wraz z opisem efektu w zakresie dostępu do danych w SSI lub/i e-usług,
- opis zarządzania autoryzacją i autentykacją użytkowników,

p) wkład do Polityki bezpieczeństwa w zakresie wdrożonego Systemu oraz Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych opracowany zgodnie z wymaganiami określonymi w Rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych). Wkład do Polityki Bezpieczeństwa musi zawierać w szczególności:
- wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych,
- opis struktury zbiorów danych wskazującej zawartość poszczególnych pól informacyjnych i powiązań między nimi,
- informacje o sposobie przepływu danych pomiędzy poszczególnymi systemami,
- opis środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

2) Wymogi szczegółowe:

a) opis aplikacji i konfiguracji aplikacji/systemu:

- opis musi obejmować ogół oprogramowania wdrożonego, zainstalowanego w ramach budowy systemu IT,

- opis musi zawierać opis systemu lub systemów informatycznych, zawierający wykaz programów, procedur lub funkcji, w zależności od struktury oprogramowania, wraz z opisem algorytmów i parametrów oraz programowych zasad ochrony danych, w tym w szczególności metod zabezpieczania dostępu do danych i systemu ich

przetwarzania, sposobu komunikacji pomiędzy systemami, zakresu wymienianych danych i sposobu ich szyfrowania,

- przykładowy zestaw wymaganych danych konfiguracyjnych obejmuje: wersję oprogramowania, narzędzia, użytkowników i grupy systemowe, katalog instalacyjny, położenie plików konfiguracyjnych, pierwotne parametry konfiguracyjne i zmodyfikowane w procesie instalacji, położenie plików logów, położenie i opis innych kluczowych plików i katalogów, parametry instancji, itp.,
- konfiguracja musi obejmować wersję aplikacji, pełen zestaw parametrów konfiguracyjnych aplikacji wraz z opisem użycia, katalogi instalacyjne, położenie plików konfiguracyjnych, położenie plików logów, położenie i opis innych kluczowych plików i katalogów, itp.

b) Procedury eksploatacji:
   - w szczególności dokumentacja musi zawierać procedury tworzenia/odtwarzania kopii bezpieczeństwa operacyjnego i kopii zapasowych oraz odtwarzania/kreowania z kopii wszystkich komponentów,
   - odtworzenia systemów i środowiska informatycznego Zamawiającego po katastrofie (Disaster Recovery),

c) Procedury backupowe:
   - zalecany tryb backupu elementów infrastruktury software'owej oraz zakres danych podlegających backupowi. Procedury odtworzeniowe muszą w szczególności opisywać sposób odtworzenia funkcjonalności aplikacji i elementów infrastruktury software'owej w przypadku Błędu lub Awarii.

I.8.1.6 Odbiór Etapu/Dokumentacji/Końcowy

1. Odbiory Etapów/Dokumentacji będą się odbywać po zakończeniu określonych prac danego Etapu/Dokumentacji.
2. Odbiór końcowy Przedmiotu Zamówienia ma na celu potwierdzenie wykonania wszystkich zadań wynikających z Umowy, w tym odebrania wszystkich Komponentów i Etapów oraz dostarczenia wymaganej zamówieniem Dokumentacji i przeszkolenia personelu.
3. Odbiory będą odbywać się zgodnie z zapisami w Umowie stanowiącej **załącznik nr 10** do SWZ.

I.8.1.7 Dostawa i instalacja oprogramowania standardowego

1. Oprogramowanie standardowe rozumiane jako oprogramowanie dostarczone i zainstalowane na Infrastrukturze serwerowej oraz Infrastrukturze sieciowej posiadanej przez Zamawiającego lub dostarczane zgodnie z Umową stanowiącą **załącznik nr 10** do SWZ oraz w istniejących systemach informatycznych zgodnie z wymaganiami niniejszego Opisu Przedmiotu Zamówienia musi zapewniać prawidłowe funkcjonowanie Oprogramowania aplikacyjnego, sprzętu oraz istniejących systemów informatycznych na wszystkich stanowiskach pracy (stanowiskach komputerowych) Zamawiającego.
2. Dostawa i instalacja zostaną wykonane w lokalizacjach zgodnych z instalacją urządzeń u Zamawiającego i zgodnie z Harmonogramem wdrożenia.

3. Oprogramowanie standardowe musi zostać skonfigurowane tak, aby działało poprawnie zgodnie z jego przeznaczeniem i architekturą Systemu oraz zapewniało prawidłową pracę Oprogramowania aplikacyjnego.

I.8.1.8 Dostawa, instalacja, konfiguracja i wdrożenie modułu Oprogramowania aplikacyjnego

1. Zadanie dostawy, instalacji, konfiguracji i wdrożenia Oprogramowania aplikacyjnego obejmuje:

POZ. OPZ	OPIS
ROZDZIAŁ II.5	**SZPITALNY SYSTEM INFORMATYCZNY**
II.5	a.
	EDM: a. Zdarzenia medyczne (integracja z P1 – raportowanie ZM, indeksowanie EDM) b. Lokalne Repozytorium EDM
	e-Usługi – dostawa i wdrożenie a. EDM dla lekarza b. EDM dla pacjenta c. eRejestracja lokalna z powiadomieniami d. Integracja z krajowym Systemem Elektronicznej Rejestracji na platformie P1

2. Dostawa i instalacja muszą być wykonane w wyznaczonych lokalizacjach Zamawiającego.
3. Po zakończeniu prac instalacyjnych Oprogramowanie musi zostać skonfigurowane i wdrożone w sposób kompleksowy tak, aby oferowało wszystkie funkcjonalności opisane w SWZ oraz zgodnie z Dokumentacją i wskazanymi przez Zamawiającego wytycznymi na etapie Analizy Przedwdrożeniowej oraz oczekiwaniami konfiguracyjnymi samego procesu wdrażania (w zakresie opisanych w OPZ wymagań funkcjonalnych) oraz musi być w pełni zintegrowane, w tym w zakresie wymiany danych z obecnie posiadanym przez Zamawiającego systemem, którego elementy zostały wymienione w punkcie II.5.3 niniejszego OPZ.
4. Oprogramowanie aplikacyjne musi zostać zainstalowane przez Wykonawcę z wykorzystaniem w szczególności Sprzętu dostarczanego przez Wykonawcę i w środowiskach informatycznych Zamawiającego. Oprogramowanie aplikacyjne musi zostać zainstalowane i skonfigurowane w sposób kompleksowy na wszystkich stanowiskach komputerowych Zamawiającego.
5. Zamawiający przewiduje konieczność przeprowadzenia przez Wykonawcę migracji dotychczasowego środowiska SSI na platformę sprzętową dostarczaną w ramach Przedmiotu Zamówienia. Wykonawca ponosi pełną odpowiedzialność za migrowane środowiska oraz zgromadzone dane.
6. Zamawiający na potrzeby realizacji Przedmiotu Zamówienia przewidział Infrastrukturę serwerową i Oprogramowanie o parametrach wskazanych w rozdziale II niniejszego OPZ.

I.8.1.9 Testy

1. W ramach Przedmiotu Zamówienia muszą zostać przeprowadzone wszystkie testy opisane w Dokumentacji. Celem testów jest weryfikacja przez Zamawiającego czy wszystkie prace wykonane w trakcie realizacji Przedmiotu Zamówienia zostały wykonane prawidłowo i zgodnie z założeniami funkcjonalnymi i jakościowymi. Testy będą przeprowadzane przez Wykonawcę przy

współudziale Zamawiającego jak i wskazanych przez Zamawiającego osób i podmiotów zewnętrznych.

2. Pozytywne zakończenie testów wraz z usunięciem wskazanych Wad i Usterek jest niezbędne, aby dla poszczególnych Komponentów oraz całego Przedmiotu Zamówienia dokonać odbiorów w ramach poszczególnych Etapów i Odbioru Końcowego.
3. Zamawiający ma prawo do weryfikacji należytego wykonania Umowy dowolną metodą, w tym także z wykorzystaniem opinii zewnętrznego audytora. W szczególności uzgodnienie określonych scenariuszy testowych nie wyklucza prawa do weryfikacji prac innymi testami i scenariuszami.
4. W przypadku zidentyfikowania Wad Wykonawca jest zobowiązany do ich poprawy przed Odbiorem Końcowym Przedmiotu Zamówienia.

I.8.1.10 Dodatkowe zobowiązania Wykonawcy

1. Wykonanie Przedmiotu Zamówienia z efektywnością oraz zgodnie z praktyką i wiedzą zawodową.
2. Dokonanie z Zamawiającym wszelkich koniecznych ustaleń mogących wpływać na zakres i sposób realizacji Przedmiotu Zamówienia oraz ciągła współpraca z Zamawiającymi na każdym etapie realizacji.
3. Stosowanie się do wytycznych i polityk bezpieczeństwa informacji obowiązujących u Zamawiającego.
4. Udzielanie na każde żądanie Zamawiającego pełnej informacji na temat stanu realizacji Przedmiotu Zamówienia.
5. Współdziałanie z osobami wskazanymi przez Zamawiającego.

Rozdział II. Szczegółowy opis przedmiotu zamówienia

II.1 Modernizacja sieci teleinformatycznej i serwerowni

1. Przedmiot Zamówienia obejmuje zakup infrastruktury niezbędnej do modernizacji Sieci teleinformatycznej i Serwerowni oraz serwis gwarancyjny dostarczanych urządzeń przez okres zadeklarowany w ofercie.
2. Wykonawca zobowiązany jest dostarczyć i uruchomić kompleksową platformę dotyczącą modernizacji Sieci teleinformatycznej i Serwerowni dla prawidłowego funkcjonowania Szpitalnego Systemu Informatycznego
3. Dostawa i instalacja zostaną wykonane w lokalizacjach Zamawiającego zgodnie z Harmonogramem wdrożenia.
4. Modernizacja Sieci teleinformatycznej i Serwerowni musi zostać skonfigurowana tak, aby działała poprawnie zgodnie z jej przeznaczeniem i architekturą SSI oraz zapewniała prawidłową pracę Oprogramowania aplikacyjnego.
5. Infrastruktura musi być dostarczona do Zamawiającego, w terminie ustalonym z upoważnionym przedstawicielem Zamawiającego.
6. Wykonawca dostarczy i zainstaluje infrastrukturę niezbędną do modernizacji Serwerowni zgodnie ze specyfikacją wymagań technicznych (zawartą w tabelach i opisach zamieszczonych poniżej w OPZ) o parametrach minimalnych wymienionych poniżej.
7. Wszystkie urządzenia muszą być fabrycznie nowe - na dzień dostawy sprzęt nie może być starszy niż 9 (dziewięć) miesięcy.

8. Zamawiający wymaga zainstalowania w/w systemów w miejscach wskazanych przez Zamawiającego.
9. Z uwagi na fakt, że realizacja zamówienia dotyczy obiektu użytkowanego, przed przystąpieniem do wykonywania jakichkolwiek prac, związanych z realizacją zamówienia, Wykonawca uzgodni z Zamawiającym terminy wykonywania prac. Ponadto, Wykonawca będzie zobowiązany do ścisłego współdziałania z upoważnionym przedstawicielem Zamawiającego podczas wykonywania prac w czynnym obiekcie lub w jego części, w celu zminimalizowania ograniczeń i uciążliwości związanych z wykonywanymi pracami, a w szczególności uzgadniania i ścisłego przestrzegania terminów oraz zakresów prowadzenia prac.
10. Zamawiający zaleca Wykonawcom dokonanie wizji lokalnej obiektów celem samodzielnej weryfikacji zakresu prac koniecznych do wykonania, tj. przeloty, odwierty, układanie tras kablowych, prace remontowe, itp. – dla prawidłowego oszacowania czasu realizacji wykonania Przedmiotu Zamówienia oraz jego wyceny. Wykonawca określi na potrzeby wykonania wyceny i projektu oszacowania poziomu trudności prac i ilości koniecznych do zastosowania materiałów. W wyjątkowych przypadkach Wykonawca może nie odbyć wizji lokalnej, z zastrzeżeniem, iż wówczas wymagane jest złożenie przez niego wraz z Ofertą oświadczenia o zapoznaniu się z zakresem i terenem prowadzenia prac i nie zgłaszaniu żadnych uwag.
11. Wszystkie miejsca, w których będą prowadzone prace budowlane (rozkucia, przekucia, przewierty itp.) muszą zostać doprowadzone do stanu wizualnie zbieżnego z wyglądem miejsca otaczającego i nie mogą być w stanie pogorszonym (należy dokonać uzupełnień brakującego tynku i pomalować te miejsca w kolorze zbliżonym do otaczającego go miejsca). Po wykonaniu prac budowlano-instalatorskich pomieszczenia zostaną doprowadzone do stanu nie gorszego niż przed rozpoczęciem robot, co zostanie potwierdzone przez przedstawiciela Zamawiającego i jest warunkiem koniecznym do podpisania Protokołu Odbioru Końcowego. Listwy kablowe muszą być położone estetycznie, równo, muszą być zakryte na całej długości. Otwory w ścianach oraz ubytki tynku zagipsowane oraz pomalowane kolorem, jaki został użyty do pomalowania pomieszczenia.
12. Wszelkie uszkodzenia infrastruktury ogólnej przez Wykonawcę w którymkolwiek obiekcie Zamawiającego podczas prowadzenia prac instalacyjnych obciążają Wykonawcę i muszą być usunięte w ramach nieodpłatnego usunięcia szkód w terminie natychmiastowym po ich stwierdzeniu.
13. W okresie prowadzenia prac instalacyjnych i ich wykończenia Wykonawca zobligowany jest stosować się do przepisów i zasad zapewniających odpowiednie warunki wykonywania pracy i pobytu osób na terenie realizacji Przedmiotu Zamówienia, w tym także zapewniać poprawne oddziaływanie prowadzonych prac na środowisko, ze szczególnym uwzględnieniem przepisów BHP, ustawy o ochronie środowiska i ustawy o odpadach i stosownych przepisów wykonawczych. Zamawiający wymaga, aby Wykonawca we własnym zakresie i na własny koszt zapewnił składowanie i sprzątanie odpadów.
14. W zakresie części modernizacji pomieszczenia Serwerowni wymagane jest wykonanie następujących usług:
    1) **Sprzężenie z agregatem prądotwórczym -** instalacja fizyczna dostarczonych Produktów:
        a) przygotowanie planu instalacji:
        b) zestawienie dostarczanych Produktów,
        c) propozycję rozmieszczenia Produktów w pomieszczeniu serwerowni,
        d) propozycję testów odbiorczych,
        e) w ramach zadania wymagana jest kompleksowa instalacja przyłączy elektrycznych dla potrzeb agregatu oraz instalacja i podłączenie agregatu, zgodnie z przedmiarami i dokumentacją stanowiącą **załączniki nr 5-7** do SWZ.

f) sieć będzie miała prawidłowo zabezpieczoną wartość poziomu uziomu, zgodnie z przepisami szczegółowymi dla tego typu działania oraz przepisami wykonawczymi SEP i norm Prawa Budowlanego,
g) przekroje przewodów należy dobrać na podstawie stosownych obliczeń uwzględniając wymogi obowiązujących norm i przepisów,
h) Wykonawca wykona system odprowadzania spalin oraz system wentylacji,
i) Zasady uruchomienia agregatu i prace z tym związane Wykonawca zobowiązany jest uzgodnić z Działem Technicznym Zamawiającego,
j) wszystkie połączenia i przyłączenia przewodów należy wykonać w sposób pewny, trwały w czasie, chroniący przed korozją,

2) Urządzenie zabezpieczające UTM

a) Instalacja, montaż, uruchomienie oraz konfiguracja UTM-a:
- montaż urządzenia w szafie rackowej,
- podłączenie UTM-a do zasilania,
- inicjalne uruchomienie UTM-a,
- aktywacja licencji UTM-a,
- testy działania UTM-a oraz weryfikacja parametrów,
- podłączenie przełącznika do sieci LAN do przełączników LAN,
- konfiguracja interfejsów sieciowych oraz interfejsu do zarządzania.

3) Wymagania ogólne

a) Wykonawca zainstaluje, podłączy, uruchomi i skonfiguruje w/w systemy,
b) Wykonawca po zrealizowaniu prac przeprowadzi minimum 2 godzinny instruktaż z zasad użytkowania i działania zamontowanych Produktów.

Wymagane jest dostarczenie poniżej opisanych urządzeń o minimalnych parametrach funkcjonalnych:

II.1.1.1 Poprawa stanu technicznego Serwerowni

Wymagane jest wykonanie instalacji elektrycznych oraz instalacji odprowadzania spalin i wentylacji zgodnie z posiadanymi przez Zamawiającego przedmiarami dotyczącymi podłączenia agregatu prądotwórczego.

Cecha	Opis wymagań
Sprzężenie z agregatem prądotwórczym	Projekt instalacji przyłączeniowej agregatu prądotwórczego jest w posiadaniu Zamawiającego i będzie udostępniony na etapie postępowania przetargowego, po zgłoszeniu chęci do jego wglądu. Dostępne także są: • przedmiar robót branży elektrycznej, • przedmiar robót branży sanitarnej – instalacja odprowadzenia spalin i wentylacji. W ramach zadania wymagana jest kompleksowa instalacja przyłączy elektrycznych dla potrzeb agregatu oraz instalacja i podłączenie agregatu. Wykonawca wykona także system odprowadzania spalin oraz system wentylacji.

II.1.1.2 UTM

Wymagane jest dostarczenie:

1) odnowienia licencji dla posiadanych przez Zamawiającego 2 sztuk UTM-ów PaloAlto PA-220 – licencje TP + URL + DNS + Wildfire + Wsparcie z terminem ważności - 5 (pięć) lat od końca obowiązywania aktualnych na dzień podpisania umowy licencji posiadanych przez Zamawiającego

2) 2 sztuk nowych UTM-ów o następujących minimalnych parametrach funkcjonalnych:

Komponent	Opis wymagań
Wymagania ogólne	Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić: 1) niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. 2) System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trybów: Routera z funkcją NAT, transparentnym. 3) W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a. 4) System musi wspierać IPv4 oraz IPv6 w zakresie: a) Firewall, b) ochrony w warstwie aplikacji, c) protokołów routingu dynamicznego.
Redundancja, monitoring i wykrywanie awarii	1) W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall. 2) Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. 3) System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.
Interfejsy, Dysk, Zasilanie	1) System realizujący funkcję Firewall musi dysponować minimum 8 portami Gigabit Ethernet RJ-45, 2) system Firewall musi posiadać wbudowany port konsoli (RS-232/USB/RJ-45) oraz dodatkowy dedykowany port Gigabit Ethernet RJ-45 do zarządzania, 3) w ramach systemu Firewall musi być możliwość zdefiniowania co najmniej 64 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q, 5) system musi mieć możliwość instalacji w szafie serwerowej 19".
Parametry	1) W zakresie Firewall'a obsługa nie mniej niż 100 tys. jednoczesnych

wydajnościowe	połączeń oraz 2 tys. nowych połączeń na sekundę, 2) przepustowość Statefull Firewall: nie mniej niż 0.5 Gbps.
Funkcje Systemu Bezpieczeństwa	W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych: 1) kontrola dostępu - zapora ogniowa klasy Stateful Inspection, 2) kontrola Aplikacji, 3) ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS, 4) ochrona przed atakami - Intrusion Prevention System, 5) kontrola stron WWW, 6) mechanizmy ochrony przed wyciekiem poufnej informacji (DLP), 7) analiza ruchu szyfrowanego protokołem SSL.
Polityki, Firewall	1) Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 2) System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT
Routing i obsługa łączy WAN	W zakresie routingu rozwiązanie powinno zapewniać obsługę: a) routingu statycznego, b) protokołów dynamicznego routingu w oparciu o protokół OSPF
Zarządzanie pasmem	1) System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma 2) Musi istnieć możliwość określania pasma dla poszczególnych aplikacji. 3) System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.
Ochrona przed malware	1) Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji. 2) System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach Przedmiotu Zamówienia musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.
Ochrona przed atakami	1) Ochrona IPS musi opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. 2) System musi chronić przed atakami na aplikacje pracujące na niestandardowych portach. 3) Baza sygnatur ataków musi być aktualizowana automatycznie lub zgodnie z harmonogramem definiowanym przez administratora. 4) Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur. 5) System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. 6) Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: SQL Injecton, 7) Wykrywanie i blokowanie komunikacji C&C do sieci botnet.

Kontrola aplikacji	1) Baza Kontroli Aplikacji musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 2) Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) muszą być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. 3) Baza musi zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. 4) Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.
Kontrola WWW	1) Moduł kontroli WWW musi korzystać z bazy adresów URL pogrupowanych w kategorie tematyczne. 2) W ramach filtra www muszą być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam. 3) Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL 4) Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania. 5) W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych ulr - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.
Uwierzytelnianie użytkowników w ramach sesji	1) System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą: a) haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu, b) haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP, c) haseł dynamicznych (RADIUS) w oparciu o zewnętrzne bazy danych. 2) Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego. 3) Rozwiązanie musi umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.
Zarządzanie	1) Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania. 2) Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów. 3) Musi istnieć możliwość włączenia mechanizmów uwierzytelniania dwuskładnikowego dla dostępu administracyjnego. 4) System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow. 5) System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API.

	6) Element systemu pełniący funkcję Firewall musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. 7) Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone. 8) Element systemu realizujący funkcję firewall musi umożliwiać administratorom wgląd w historyczne zmiany konfiguracji firewalla w CLI lub GUI.
Logowanie	1) W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. 2) Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu. 3) Musi istnieć możliwość logowania do serwera SYSLOG.
Certyfikaty	Poszczególne elementy oferowanego systemu bezpieczeństwa muszą posiadać następujące certyfikacje: ICSA lub EAL4 lub równoważne dla funkcji Firewall.
Serwisy i licencje	Zamawiający wymaga dostarczenia licencji upoważniających do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów obejmujących na okres co najmniej 60 miesięcy: 1. Kontrolę Aplikacji, 2. IPS, 3. Antywirus, 4. Analizę typu Sandbox, 5. Antyspam, 6. Web Filtering, 7. bazy reputacyjne adresów IP/domen.
Gwarancja oraz wsparcie	System musi być objęty serwisem gwarancyjnym producenta przez okres co najmniej 60 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji Oprogramowania oraz wsparcie techniczne w trybie 24x7.
Opisy do wymagań ogólnych	1) W przypadku istnienia takiego wymogu w stosunku do technologii objętej Przedmiotem Zamówienia (tzw. produkty podwójnego zastosowania), Wykonawca powinien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (t.j. Dz.U. z 2022 r. poz. 1666 ze zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego

	zastosowania. 2) Wykonawca powinien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań. 3) Deklaracja zgodności EU - CE.

II.2 Dostawa i wdrożenie infrastruktury serwerowej

1. Wykonawca zobowiązany jest dostarczyć i uruchomić kompleksową platformę Infrastruktury serwerowej (pamięć masową NAS wraz z niezbędnym Oprogramowaniem Narzędziowym – systemowym i pozostałym Oprogramowaniem) dla prawidłowego funkcjonowania Szpitalnego Systemu Informatycznego i e-usług.
2. Dostawa i instalacja zostaną wykonane w lokalizacjach Zamawiającego zgodnie z Harmonogramem wdrożenia.
3. Infrastruktura serwerowa musi zostać skonfigurowana tak, aby działała poprawnie zgodnie z jej przeznaczeniem i architekturą HIS oraz zapewniała prawidłową pracę Oprogramowania aplikacyjnego.
4. Infrastruktura musi być dostarczona do Zamawiającego, w terminie ustalonym z upoważnionym przedstawicielem Zamawiającego.
5. Jeżeli zajdzie potrzeba, wraz z dostarczoną Infrastrukturą serwerową, Wykonawca zobowiązany jest dostarczyć niezbędne elementy np. urządzenia i wyposażenie – kable połączeniowe, elementy mocujące, uznane przez Wykonawcę za niezbędne i umożliwiające prawidłowe działanie całego Systemu. Dostarczona Infrastruktura Serwerowa musi zapewniać bezproblemową pracę po podłączeniu jej do sieci informatycznej Zamawiającego.
6. Wykonawca jest zobowiązany dokonać montażu dostarczonej Infrastruktury Serwerowej oraz oprogramowania w miejscach wskazanych przez Zamawiającego.
7. Wszystkie elementy Infrastruktury serwerowej muszą zostać zamontowane w szafie serwerowej rack, w sposób umożliwiający ich prawidłową wentylację.
8. Szczegóły dotyczące instalacji i uruchomienia Infrastruktury serwerowej zostaną ustalone w trakcie Analizy Przedwdrożeniowej.
9. Zamawiający zaleca i umożliwia odbycie wizji lokalnej Wykonawcy. Wizja lokalna może odbyć się w pracujące dni powszednie (poniedziałek – piątek) w zakresie godzin od 08.00 do 15.00 po uzgodnieniu konkretnego terminu z Zamawiającym.
10. Wykonawcy, którzy są zainteresowani przeprowadzeniem ww. wizji lokalnej w celu zapoznania się z obiektem, zobowiązani są zgłosić chęć uczestniczenia w wizji lokalnej za pośrednictwem mail na adres: sekretariat@womp.szczecin.pl oraz informatyk@womp.szczecin.pl. O terminie przeprowadzenia wizji lokalnej Wykonawca zostanie poinformowany e-mailem. **Wykonawca przed odbyciem wizji lokalnej zobowiązany będzie do podpisania umowy o zachowaniu poufności informacji uzyskanych w trakcie wizji lokalnej, według wzoru stanowiącego załącznik 11 do SWZ.**
11. W zakresie części serwerowej w ramach Przedmiotu Zamówienia wymagane jest wykonanie następujących usług:
    1) Instalacja fizyczna dostarczonej Infrastruktury:
        a) Przygotowanie planu instalacji:

- zestawienie dostarczanych urządzeń,
- propozycję rozmieszczenia elementów w istniejących szafach rackowych,
- propozycję testów odbiorczych,

b) Instalacja, montaż i uruchomienie systemu dyskowego NAS:
- montaż NAS-a w istniejącej szafie rackowej,
- podłączenie urządzenia do sieci LAN do nowych/istniejących przełączników LAN,
- podłączenie systemu do zasilania,
- inicjalne uruchomienie systemu dyskowego,
- testy działania oraz weryfikacja parametrów,

2) Instalacja oprogramowania systemowego:

a) Inwentaryzacja stanu obecnego:
- zestawienie nazewnictwa poszczególnych elementów istniejącego systemu,
- zestawienie zainstalowanych łat systemu operacyjnego,
- zestawienie zainstalowanych wersji oprogramowania,

b) Przygotowanie projektu technicznego:
- zestawienie stosowanej nomenklatury,
- rysunki logicznej struktury systemu,
- propozycję nazewnictwa poszczególnych elementów systemu wirtualizacji,
- zestawienie wymaganych wersji oprogramowania,
- propozycje konfiguracji systemów operacyjnych,

c) Implementacja zgodna z projektem:
- instalacja oprogramowania systemowego,
- konfiguracja oprogramowania systemowego,
- aktywacja dostarczonego oprogramowania,

d) Przygotowanie dokumentacji powykonawczej zawierającej:
- zestawienie stosowanej nomenklatury,
- zestawienie wersji zainstalowanego oprogramowania systemowego.

12. Po zakończonym montażu Wykonawca przekaże Zamawiającemu wszystkie hasła dostępowe do kont „super użytkowników” oraz dokumentację do wszystkich oferowanych urządzeń, Oprogramowania narzędziowego (systemowego, bazodanowego, itd.) wraz z dokumentami potwierdzającymi nabycie dla Zamawiającego licencji oraz co najmniej 1 (jednym) nośnikiem danych zawierającymi zainstalowane Oprogramowanie. Wykonawca wykona również instruktaże użytkowe dla wskazanych przez Zamawiającego administratorów, z zakresu konfiguracji, obsługi i prawidłowej eksploatacji zainstalowanego Sprzętu ze szczególnym uwzględnieniem obsługi i zaawansowanego zarządzania macierzą danych, w środowisku Zamawiającego.
13. Wykonawca zobowiązany jest zapewnić co najmniej 60 -miesięczny okres gwarancji obejmujący wsparcie i możliwość prowadzenia konsultacji w zakresie administracji zaoferowanym i dostarczonym Oprogramowaniem narzędziowym (systemowym, i bazodanowym) z osobami wskazanymi przez Wykonawcę, posiadającymi odpowiednie certyfikaty producentów urządzeń i Oprogramowania na warunkach gwarancji producenta lub dostawcy sprzętu. Pozostałe wymagania dotyczące gwarancji zostały opisane w OPZ w rozdziale III. Gwarancja.

II.2.1.1 Pamięć masowa NAS

Wymagane jest dostarczenie 1 szt. Pamięci masowej NAS o następujących minimalnych parametrach funkcjonalnych:

L.p.	Opis wymagań
1.	Urządzenie typu NAS z możliwością zarządzania poprzez panel web na urządzeniu.
2.	Obudowa – max. 3U z szynami do montażu w szafie RACK 19’.
3.	Procesor – minimum Czterordzeniowy procesor z min. 2,2, GHz
4.	Architektura procesora – 64-bitowy z obsługą x86
5.	Mechanizm szyfrowania.
6.	Pamięć systemowa – 16 GB UDIMM DDR4 (1 x 16 GB).
7.	Gniazdo pamięci -2 x Long-DIMM DDR4.
8.	Pamięć flash – 5 GB (
9.	1) Wnęka dysków – 16 dysków 3,5” SATA 6 Gb/s, 3 Gb/s, 2) zainstalowane min 16 dysków 3,5” 10TB SATA 6Gb/s 7200 obr., z deklaracją producenta do zastosowań NAS lub serwerowych. 3) dyski wymienne podczas pracy urządzenia. 4) Zainstalowana karta rozszerzeń 2x M.2 PCIe NVMe 5) Zainstalowane 2 dyski M.2 PCIe NVMe 3.0 x4 – 1TB (1000GB) o prędkości odczytu i zapisu min 3300 MB/s oraz odczycie losowym 600 000 IOPS i zapisie losowym 550 000 IOPS oraz niezawodności MTBF min. 1 500 000 godz.
10.	Kompatybilność dysków – 3,5-calowe wnęki: a) 3,5-calowe dyski twarde SATA, b) 2,5-calowe dyski twarde SATA, c) 2,5-calowe dyski SSD SATA.
11.	Gniazdo dysku M.2 SSD – Opcjonalne poprzez kartę PCIe.
12.	Obsługa przyspieszenia pamięci podręcznej SSD.
13.	2 porty 2,5 Gigabit Ethernet (2,5G/1G/100M).
14.	Zainstalowana karta rozszerzeń 2 x 10GbE SFP+ wraz z wkładkami 10Gb MM SR 850nm.
15.	Wake on LAN (WOL) minimum dla portów 2,5GbE.
16.	Ramka Jumbo.
17.	Jedno Gniazdo PCIe Gen 2 x2.
18.	3 porty USB
19.	Zasilacz - 2 x minimum 550 W PSU, 100–240 V.
20.	1) Wspierane systemy operacyjne:Apple Mac OS 10.10 or later, 1) Ubuntu, CentOS, RHEL, SUSE, 2) Microsoft Windows 10, 3) Microsoft Windows Server 2016, 2019.
21.	Wspierane przeglądarki – minimalne wersje: 1) Google Chrome, 2) Microsoft Internet Explorer 10, 3) Mozilla Firefox.
22.	Wspierane systemy plików: 1) dla dysków wewnętrznych (EXT4), 2) dla dysków zewnętrznych (EXT3, EXT4, NTFS, FAT32, HFS+, and exFAT).
23.	1) Funkcje sieciowe:TCP/IP: Dual stack (IPv4 and IPv6), 1) Jumbo frame, 2) Port trunking (Link aggregation): a) failover, b) Load balancing, 3) DHCP server and client, 4) Virtual switch:

	a) Network Address Translation (NAT), b) Spanning Tree Protocol (STP), 5) Static Route, 6) DDNS, 7) Web server, 8) File server: a) File sharing across Windows, Mac, and Linux/UNIX, b) Microsoft networking (CIFS/SMB), c) Apple networking (AFP), d) NFS version 3/4 services, e) Windows ACL (CIFS/SMB), f) Advanced folder permissions (AFP, CIFS/SMB, and FTP), g) Shared folder aggregation (CIFS/SMB), 9) FTP server: a) FTP, SFTP and TFTP protocols, b) FTP over SSL/TLS (explicit FTPS), c) FXP suport.
24.	Funkcje storage: 1) RAID: RAID 0, 1, 5, 6, 10, , JBOD, Single, 2) RAID Hot Spare and Global Hot Spare, 3) RAID Rebuild Speed Customization, 4) Online RAID capacity expansion, 5) Online RAID level migration, 6) Disk auto S.M.A.R.T. data migration, 7) Disk bad block scan and S.M.A.R.T test, 8) Disk bad block recovery, 9) Disk secure data erase, 10) Storage pools, 11) SCSI targets with multiple LUNs per target, 12) LUN masking, 13) Online LUN capacity expansion, 14) SPC-3 persistent reservation, 15) MPIO & MC/S, 16) iSCSI LUN backup, one-time snapshot, and restoration, 17) Virtual disks using iSCSI initiator.
25.	1) Bezpieczeństwo:Network access protection with auto-blocking (SSH, Telnet, HTTP(S), FTP, CIFS/SMB, and AFP), 2) Host access control for shared folders (CIFS/SMB), 3) AES 256-bit folder-based and volume-based encryptions which are validated by FIPS 140-2 CAVP (Cryptographic Algorithm Validation Program), 4) 256-bit external drive encryption (AES), 5) Instant alerts through email, SMS, push service, and audio.
26.	6) Deklaracja zgodności EU - CE
27.	Gwarancja co najmniej 5 lat

II.3 Oprogramowanie systemowe i narzędziowe

II.3.1.1 Serwerowy system operacyjny

1. Wymagane jest dostarczenie licencji serwerowego systemu operacyjnego na 1 szt. serwera posiadającego 24 cory CPU.
2. Zamawiający wymaga, aby wszystkie elementy systemu oraz jego licencja pochodziły od tego samego producenta. Licencja ma umożliwiać downgrade do poprzednich wersji systemu operacyjnego oraz uprawniać do uruchamiania SSO w środowisku fizycznym i nieograniczoną ilość środowisk systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji.
3. Wymaga się dostarczenia licencji na 1 serwer posiadający 24 rdzenie.
4. Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy:

L.p.	Opis wymagań
1	System musi posiadać możliwość wykorzystania 320 logicznych procesorów oraz 4 TB pamięci RAM w środowisku fizycznym.
2	System musi posiadać możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności 64TB przez każdy wirtualny serwerowy system operacyjny.
3	System musi posiadać możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania do 7000 maszyn wirtualnych.
4	System musi posiadać możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.
5	System musi posiadać wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.
6	System musi posiadać wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.
7	System musi posiadać automatyczną weryfikację cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
8	System musi posiadać możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy.
9	System musi posiadać wbudowane wsparcie instalacji i pracy na wolumenach, które: 1) pozwalają na zmianę rozmiaru w czasie pracy systemu, 2) umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów, 3) umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów, 4) umożliwiają zdefiniowanie list kontroli dostępu (ACL).
10	System musi posiadać wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
11	System musi posiadać wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
12	System musi posiadać możliwość uruchamianie aplikacji internetowych wykorzystujących

	technologię ASP.NET.
13	System musi posiadać możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
14	System musi posiadać wbudowaną zaporę internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
15	Graficzny interfejs użytkownika.
16	Zlokalizowane w języku polskim, następujące elementy: 1) menu, 2) przeglądarka internetowa, 3) pomoc, 4) komunikaty systemowe.
17	System musi posiadać wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
18	System musi posiadać możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
19	Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
20	Pochodzący od producenta systemu serwis zarządzania polityką konsumpcji informacji w dokumentach (Digital Rights Management).
21	System musi posiadać możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji: 1) podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC, 2) usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji: a) Podłączenie SSO do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną, b) Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania, c) Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza. 3) zdalna dystrybucja oprogramowania na stacje robocze, 4) praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej, 5) Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające: a) dystrybucję certyfikatów poprzez http, b) konsolidację CA dla wielu lasów domeny, c) automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen, d) szyfrowanie plików i folderów, e) szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec). 6) posiada możliwość tworzenia systemów wysokiej dostępności (klastry typu failover) oraz rozłożenia obciążenia serwerów, 7) serwis udostępniania stron WWW, 8) wsparcie dla protokołu IP w wersji 6 (IPv6), 9) wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby

	równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows, 10) wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji zapewniają wsparcie dla: a) dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych, b) obsługi ramek typu jumbo frames dla maszyn wirtualnych, c) obsługi 4-KB sektorów dysków, d) nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra. 11) posiada możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk model), 12) posiada możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta SSO umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.
22	Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath).
23	System musi posiadać możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
24	System musi posiadać mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
25	System musi posiadać możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.
26	Dostawca systemu musi zagwarantować wsparcie dla użytkowników przez okres 5 lat.

II.3.1.2 Oprogramowanie Antywirusowe

3) Zamawiający wymaga rozszerzenia aktualnie posiadanych licencji w ilości 270 sztuk oraz przedłużenia posiadanego oprogramowania Antywirusowego Eset Endpoint Protection Standard, - na 5 (pięć) lat od końca obowiązywania aktualnych na dzień podpisania umowy licencji posiadanych przez Zamawiającego.

Zamawiający dopuszcza dostawę nowych 300 sztuk z licencją na okres 60 miesięcy o następujących funkcjonalnościach:

Cecha	Opis wymagań
Ochrona stacji roboczych - Windows	Pełne wsparcie dla systemu Windows 7/Windows 8/Windows 8.1/Windows 10.
	Wsparcie dla 32- i 64-bitowej wersji systemu Windows.
	Wersja programu dostępna co najmniej w języku polskim oraz angielskim.
	Instalator musi umożliwiać wybór wersji językowej programu, przed rozpoczęciem procesu instalacji.
	Pomoc w programie (help) i dokumentacja do programu dostępna w języku

	polskim oraz angielskim.
	Skuteczność programu potwierdzona nagrodami VB100 i AV-comparatives.
Ochrona antywirusowa i antyspyware	Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
	Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
	Wbudowana technologia do ochrony przed rootkitami.
	Wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
	Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
	Możliwość skanowania całego dysku, wybranych katalogów, pojedynczych plików „na żądanie” lub według harmonogramu.
	System musi posiadać możliwość definiowania zadań w harmonogramie, w taki sposób, aby zadanie przed wykonaniem sprawdzało czy komputer pracuje na zasilaniu bateryjnym, jeśli tak – nie wykonywało danego zadania.
	Możliwość utworzenia wielu różnych zadań skanowania według harmonogramu (w tym: co godzinę, po zalogowaniu i po uruchomieniu komputera). Każde zadanie ma mieć możliwość uruchomienia z innymi ustawieniami (czyli metody skanowania, obiekty skanowania, czynności, rozszerzenia przeznaczone do skanowania, priorytet skanowania).
	Skanowanie „na żądanie” pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
	Możliwość określania priorytetu wykorzystania procesora (CPU) podczas skanowania „na żądanie” i według harmonogramu.
	Możliwość skanowania dysków sieciowych i dysków przenośnych.
	Skanowanie plików spakowanych i skompresowanych.
	Możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.
	Administrator musi mieć możliwość dodania wykluczenia dla zagrożenia po nazwie, sumie kontrolnej (SHA1) oraz lokalizacji pliku.
	Możliwość automatycznego wyłączenia komputera po zakończonym skanowaniu.
	Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji programu.
	Użytkownik musi posiadać możliwość tymczasowego wyłączenia ochrony na czas co najmniej 10 minut lub do ponownego uruchomienia komputera.
	W momencie tymczasowego wyłączenia ochrony antywirusowej użytkownik musi być poinformowany o takim fakcie odpowiednim powiadomieniem i informacją w interfejsie aplikacji.
	Ponowne włączenie ochrony antywirusowej nie może wymagać od użytkownika ponownego uruchomienia komputera.
	Możliwość przeniesienia zainfekowanych plików i załączników poczty w bezpieczny obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej.
	Wbudowany konektor dla programów MS Outlook, Outlook Express, Windows Mail I Windows Live Mail.

	Skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu MS Outlook, Outlook Express, Windows Mail i Windows Live Mail.
	Skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie" (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).
	Automatyczna integracja skanera POP3 i IMAP z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.
	Możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail.
	Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch musi być automatycznie blokowany, a użytkownikowi wyświetlane jest stosowne powiadomienie.
	Blokowanie możliwości przeglądania wybranych stron internetowych. Program musi umożliwić blokowanie danej strony internetowej po podaniu przynajmniej całego adresu URL strony lub części adresu URL.
	Możliwość zdefiniowania blokady wszystkich stron internetowych z wyjątkiem listy stron, ustalonej przez administratora.
	Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji.
	Program musi umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
	Program musi zapewniać skanowanie ruchu szyfrowanego transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji, takich jak: przeglądarki internetowe oraz programy pocztowe.
	Możliwość zgłoszenia witryny z podejrzeniem phishingu z poziomu graficznego interfejsu użytkownika, w celu analizy przez laboratorium producenta.
	Administrator musi mieć możliwość zdefiniowania portów TCP, na których aplikacja będzie realizowała proces skanowania ruchu szyfrowanego.
	Program musi posiadać funkcjonalność, która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika.
	Procesy zweryfikowane jako bezpieczne mają być pomijane podczas procesu skanowania oraz przez moduły ochrony w czasie rzeczywistym.
	Użytkownik musi posiadać możliwość przesłania pliku celem zweryfikowania jego reputacji bezpośrednio z poziomu menu kontekstowego.
	W przypadku, gdy stacja robocza nie będzie posiadała dostępu do sieci Internet, ma odbywać się skanowanie wszystkich procesów, również tych, które wcześniej zostały uznane za bezpieczne.
	Wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru z jaką heurystyką ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.

	Możliwość automatycznego wysyłania nowych plików/zgłoszeń/próbek do laboratoriów producenta bezpośrednio z programu (nie wymaga ingerencji użytkownika). Użytkownik musi mieć możliwość określenia rozszerzeń dla plików, które nie będą wysyłane automatycznie.
	Do wysłania próbki zagrożenia do laboratorium producenta, aplikacja nie może wykorzystywać klienta pocztowego zainstalowanego na komputerze użytkownika.
	Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń muszą być w pełni anonimowe.
	Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.
	Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby każdy użytkownik przy próbie dostępu do konfiguracji, był proszony o jego podanie.
	Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet, gdy posiada ona prawa lokalnego lub domenowego administratora. Przy próbie deinstalacji program musi pytać o hasło.
	Hasło do zabezpieczenia konfiguracji programu oraz deinstalacji musi być takie samo.
	Program musi mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku aktualizacji – poinformować o tym użytkownika i wyświetlenia listy niezainstalowanych aktualizacji.
	Program musi mieć możliwość definiowania typu aktualizacji systemowych o braku, których będzie informował użytkownika w tym przynajmniej: aktualizacje krytyczne, aktualizacje ważne, aktualizacje zalecane oraz aktualizacje o niskim priorytecie. Musi być możliwość dezaktywacji tego mechanizmu.
	Po instalacji programu, użytkownik musi mieć możliwość przygotowania płyty CD, DVD lub pamięci USB, z której będzie w stanie uruchomić komputer w przypadku infekcji i przeskanować dysk w poszukiwaniu zagrożeń.
	System antywirusowy, uruchomiony z płyty bootowalnej lub pamięci USB, musi umożliwiać pełną aktualizację silnika detekcji z Internetu lub z bazy zapisanej na dysku.
	System antywirusowy, uruchomiony z płyty bootowalnej lub pamięci USB, musi pracować w trybie graficznym.
	Program musi umożliwiać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.
	Funkcja blokowania nośników wymiennych, bądź grup urządzeń, musi umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń, minimum w oparciu o typ, numer seryjny, dostawcę oraz model urządzenia.
	Program musi mieć możliwość utworzenia reguły na podstawie podłączonego urządzenia. Dana funkcjonalność musi pozwalać na automatyczne wypełnienie typu, numeru seryjnego, dostawcy oraz modelu

	urządzenia.
	Program musi umożliwiać użytkownikowi nadanie uprawnień dla podłączanych urządzeń, w tym co najmniej: dostęp w trybie do odczytu, pełen dostęp, ostrzeżenie, brak dostępu do podłączanego urządzenia.
	Program musi posiadać funkcjonalność, umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika.
	W momencie podłączenia zewnętrznego nośnika, aplikacja musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika.
	Administrator musi posiadać możliwość takiej konfiguracji programu, aby skanowanie całego nośnika odbywało się automatycznie lub za potwierdzeniem przez użytkownika.
	Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS).
	Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów: 1) tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika, 2) tryb interaktywny, w którym to program pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie, 3) tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika, 4) tryb uczenia się, w którym program uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach, 5) tryb inteligentny, w którym program będzie powiadamiał wyłącznie o szczególnie podejrzanych zdarzeniach.
	Tworzenie reguł dla modułu HIPS musi odbywać się co najmniej w oparciu o: aplikacje źródłowe, pliki docelowe, aplikacje docelowe, elementy docelowe rejestru systemowego.
	Użytkownik na etapie tworzenia reguł dla modułu HIPS musi posiadać możliwość wybrania jednej z trzech akcji: pytaj, blokuj, zezwól.
	Oprogramowanie musi posiadać zaawansowany skaner pamięci.
	Program musi być wyposażony w mechanizm ochrony przed exploitami w popularnych aplikacjach, przynajmniej czytnikach PDF, aplikacjach JAVA, przeglądarkach internetowych.
	Program musi być wyposażony we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której został zainstalowany, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników.
	Funkcja, generująca taki log, musi posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla programu i mogą stanowić zagrożenie bezpieczeństwa.
	Program musi posiadać funkcję, która aktywnie monitoruje wszystkie pliki programu, jego procesy, usługi i wpisy w rejestrze i skutecznie blokuje ich

	modyfikacje przez aplikacje trzecie.
	Automatyczna, inkrementacyjna aktualizacja silnika detekcji.
	Możliwość utworzenia kilku zadań aktualizacji. Każde zadanie musi być uruchamiane przynajmniej z jedną z opcji: co godzinę, po zalogowaniu, po uruchomieniu komputera.
	Możliwość określenia maksymalnego wieku dla silnika detekcji, po upływie którego program zgłosi posiadanie nieaktualnego silnika detekcji.
	Program musi posiadać funkcjonalność tworzenia lokalnego repozytorium aktualizacji modułów.
	Program musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji modułów za pomocą wbudowanego w program serwera HTTP.
	Program musi być wyposażony w funkcjonalność, umożliwiającą tworzenie kopii wcześniejszych aktualizacji modułów w celu ich późniejszego przywrócenia (rollback).
	Program wyposażony tylko w jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
	Aplikacja musi posiadać funkcjonalność, która automatycznie wykrywa aplikacje pracujące w trybie pełnoekranowym.
	W momencie wykrycia trybu pełnoekranowego, aplikacja musi wstrzymać wyświetlanie wszystkich powiadomień związanych ze swoją pracą oraz wstrzymać zadania znajdujące się w harmonogramie zadań aplikacji.
	Użytkownik musi mieć możliwość skonfigurowania po jakim czasie włączone mają zostać powiadomienia oraz zadania, pomimo pracy w trybie pełnoekranowym.
	Program musi być wyposażony w dziennik zdarzeń, rejestrujący informacje na temat znalezionych zagrożeń, kontroli dostępu do urządzeń, skanowania oraz zdarzeń.
	Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora, autoryzowanego przez producenta programu.
	Program musi posiadać możliwość utworzenia dziennika diagnostycznego z poziomu interfejsu aplikacji.
	Program musi posiadać możliwość aktywacji przy użyciu co najmniej jednej z trzech metod: poprzez podanie poświadczeń administratora licencji, klucza licencyjnego lub aktywacji programu w trybie offline.
	Możliwość podejrzenia informacji o licencji, która znajduje się w programie.
	W programie musi istnieć możliwość tymczasowego wstrzymania działania polityk, wysłanych z poziomu serwera zdalnej administracji.
	Wstrzymanie polityk musi umożliwić lokalną zmianę ustawień programu na stacji końcowej.
	Funkcja wstrzymania polityki musi być realizowana tylko przez określony czas, po którym automatycznie zostaną przywrócone dotychczasowe ustawienia.
	Administrator musi mieć możliwość wstrzymania polityk na 10 minut, 30 minut, 1 godzinę lub 4 godziny.
	Aktywacja funkcji wstrzymania polityki musi obsługiwać uwierzytelnienie za pomocą hasła lub konta użytkownika.

	Program musi posiadać opcję automatycznego skanowania komputera po wyłączeniu wstrzymania polityki.
	Możliwość zmiany konfiguracji programu z poziomu dedykowanego modułu wiersza poleceń. Zmiana konfiguracji jest w takim przypadku autoryzowana bez hasła lub za pomocą hasła do ustawień zaawansowanych.
	Program musi posiadać możliwość definiowana stanów aplikacji, jakie będą wyświetlane użytkownikowi, co najmniej: ostrzeżeń o wyłączonych mechanizmach ochrony czy stanie licencji.
	Administrator musi mieć możliwość dodania własnego komunikatu do stopki powiadomień, jakie będą wyświetlane użytkownikowi na pulpicie.
	Program musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
	Wbudowany skaner UEFI nie może posiadać dodatkowego interfejsu graficznego i musi być transparentny dla użytkownika, aż do momentu wykrycia zagrożenia.
	Aplikacja musi posiadać dedykowany moduł, zapewniający ochronę przed oprogramowaniem wymuszającym okup.
	Administrator musi mieć możliwość dodania wykluczenia dla procesu, wskazując plik wykonywalny.
	Program musi posiadać możliwość przeskanowania pojedynczego pliku, poprzez opcję „przeciągnij i upuść”.
	Administrator musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.
	Administrator musi posiadać możliwość wyłączenia z przesyłania do analizy producenta określonych plików i folderów.
	Program musi posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zdefiniowanego przedziału czasowego.
	Wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.
	Program musi umożliwiać ochronę przed dołączeniem komputera do sieci botnet. Program ma posiadać pełne wsparcie zarówno dla protokołu IPv4 jak i dla standardu IPv6.
	W przypadku konieczności wprowadzenia zmian w Infrastrukturze sieciowej lub/i zmiany oprogramowania na serwerach oraz stanowiskach klienckich Zamawiającego, wynikającej z zakupu nowej licencji, Wykonawca jest zobowiązany do dostarczenia, instalacji i pełnej konfiguracji wszystkich uznanych za niezbędne elementów wymaganych do korzystania z licencji.

II.4 Dostawa i wdrożenie SSI wraz z e-usługami

II.4.1.1 Ogólna architektura funkcjonalna projektu ZeZ

W odniesieniu do poszczególnych e-usług, w zależności od uwarunkowań implementacji wymagany jest następujący poniżej omówiony zakres prac w warstwie lokalnej.

Dla e-usług założono i przyjęto udział obecnych i planowanych rozwiązań zarówno na poziomie centralnym, na poziomie warstwy regionalnej - Województwa Zachodniopomorskiego oraz na poziomie warstwy lokalnej - Zamawiającego:

1) Poziom centralny, w tym w szczególności P1 w zakresie:
   a) Internetowe Konto Pacjenta (IKP),
   b) rejestr Elektroniczna Dokumentacja Medyczna (EDM) w obecnym i dalszych rozszerzeniach zakresu stosowania dla kolejnych dokumentów medycznych (od 25 kwietnia 2020 r. EDM stanowią również opisy badań diagnostycznych innych niż laboratoryjne, a od 25 kwietnia 2021 r. są to także wyniki badań laboratoryjnych wraz z opisem),
   c) Zdarzenia Medyczne,
   d) zgody pacjenta,
   e) kolejne e-usługi planowane do uruchomienia w przyszłości, m.in. e-Rejestracja, e-Wizyty, zamawianie e-Recept,
   f) uwierzytelnianie z wykorzystaniem Węzła Krajowego Identyfikacji Elektronicznej poprzez: Profil zaufany (PZ), e-dowód oraz mojeID - przy pomocy banku lub innego dostawcy tożsamości.

2) Warstwa regionalna w zakresie:

Platforma regionalna (www) o następującym zakresie funkcjonalnym:
   a) Portal Projektu ZeZ,
   b) Systemy analityczne:
      1. System Analiz Zarządczych
      2. System Analiz Sprawozdawczych
      3. Platforma zakupowa SPZOZ/Grupowe zamówienia.

3) Warstwa lokalna na poziomie Zamawiającego:
   a) integracja z krajowym Systemem Elektronicznej Rejestracji (SER) na Platformie P1,
   b) e-Rejestracja lokalna przez stronę www w powiązaniu z e-Rejestracją centralną (SER) w P1),
   c) lokalne repozytorium EDM,
   d) EDM i zdarzenia medyczne dla pacjenta (poprzez IKP),
   e) EDM i zdarzenia medyczne dla lekarza,
   f) przesyłanie indeksów EDM oraz danych o zdarzeniach medycznych (ZM) do P1,
   g) odczyt i zapis zgód pacjenta na potrzeby integracji z P1.

Warstwa centralna i lokalna uczestniczy w świadczeniu usług oraz zapewnia udostępnianie EDM pacjentowi oraz innym podmiotom leczniczym bez udziału regionalnego Repozytorium EDM.

Rejestr oraz repozytorium EDM wskazane na poziomie centralnym oraz lokalnym, rozumiane są następująco:

- źródłem danych dla dokumentacji EDM (Document Source) jest system części białej (HIS, LIS, RIS) w podmiocie leczniczym,
- dokumenty EDM są składowane i archiwizowane w repozytorium lokalnym podmiotu leczniczego;

- informacje opisujące dokumentację medyczną (metadane, indeksy) oraz wskazujące, gdzie przechowywana jest właściwa dokumentacja zawarte są w Rejestrze EDM w P1 w ramach Krajowej Domeny (IHE XDS.b),
- informacje do Rejestru EDM są przekazywane bezpośrednio przez podmiot leczniczy,
- lokalne Repozytorium pełni rolę Document Repository EDM danego podmiotu leczniczego (Partnera Projektu);
- realizacja zapytań o dokumenty EDM składanych przez innych świadczeniodawców, odbywa się z poziomu lokalnego Repozytorium EDM z wykorzystaniem Rejestru EDM w P1, po zweryfikowaniu zgody pacjenta;
- udostępnianie EDM dla zewnętrznych użytkowników (pacjentów) odbywa się z lokalnego Repozytorium EDM poprzez Internetowe Konto Pacjenta w systemie P1 (dla pacjentów) lub poprzez systemy dziedzinowe, w tym HIS (dla pracowników medycznych).

Uwagi:

- raportowanie/przekazywanie informacji o Zdarzeniach Medycznych będzie realizowane przez podmiot leczniczy lokalnie ze wskazaniem lokalnego Repozytorium jako Document Repository EDM;
- podmiot leczniczy wdraża e-Rejestrację lokalną, do której dostęp zapewniony będzie poprzez stronę (witrynę) www podmiotu leczniczego;
- systemy oprogramowania danego podmiotu zostaną zintegrowane z Systemem Elektronicznej Rejestracji na Platformie P1.

II.4.1.2 Wymogi dotyczące interoperacyjności dla oferowanych modułów i usług

1. Wykonawca zobowiązuje się dostarczyć Zamawiającemu wymagane funkcjonalności modułu HIS poprzez rozbudowanie istniejącego systemu o nowe funkcjonalności w taki sposób, aby w jak najszerszym zakresie zostały zaspokojone potrzeby Zamawiającego. **Zamawiający nie przewiduje wymiany posiadanego systemu na nowy.**
2. Obecnie Zamawiający używa w części medycznej dziedzinowy system KS-SOMED firmy Kamsoft Sp. z o.o., który zintegrowany jest z następującymi systemami: ERP Kamsoft S.A. oraz LIS firmy Kamsoft S.A.
3. System Informatyczny, stanowiący źródło Elektronicznej Dokumentacji Medycznej EDM musi mieć zaimplementowane i uruchomione mechanizmy integracji oraz zapewnić prawidłową integrację z systemem EDM.
4. System informatyczny w obszarze e-Usług musi spełniać wymagania Web Content Accessibility Guidelines (WCAG 2.1), z uwzględnieniem poziomu AA, określonych w załączniku pn. „Wytyczne dla dostępności treści internetowych 2.1 stosowane dla stron internetowych i aplikacji mobilnych w zakresie dostępności dla osób niepełnosprawnych” do ustawy z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych (Dz.U. z 2019 r. poz. 848 ze zm.).
5. Szpitalny System Informatyczny, jako produkt z zakresu tzw. e-Zdrowia, musi spełniać wymogi i zalecenia im stawiane (według stanu aktualnego na dzień Odbioru Końcowego), co najmniej takie jak:
   1) zapewnienie pełnej zgodności z opracowaniami publikowanymi przez Centrum Systemów Informacyjnych Ochrony Zdrowia,

2) zgodność z Rozporządzeniem Ministra Zdrowia z dnia 6 kwietnia 2020 r. w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania (t.j. Dz.U. z 2022 r. poz. 1304 ze zm.),

3) zgodność z Ustawą z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia (t.j. Dz.U z 2022 r. poz.1555 ze zm.),

4) zgodność z Ustawą z dnia 1 marca 2018 r. o zmianie niektórych ustaw w związku z wprowadzeniem e-recepty (Dz.U. z 2018 r. poz. 697 ze zm.),

5) zgodność z Ustawą z dnia 19 lipca 2019 r. o zmianie niektórych ustaw w związku z wdrażaniem rozwiązań w obszarze e-zdrowia (Dz.U z 2019 r. poz. 1590 ze zm.),

6) zapewnienie komunikacji umożliwiającej pozyskiwanie aktualnych danych z rejestrów zintegrowanych z Platformą Rejestrów Medycznych (P2), odpowiadających analogicznym rejestrom zaimplementowanym w modułach SSI,

7) zapewnienie wsparcia obsługi dla Karty Specjalisty Medycznego (KSM)

oraz zgodność z wszelkimi innymi aktami prawnymi zmieniającymi, wprowadzającymi nowe lub uchylającymi powyższe akty prawne oraz przepisami wykonawczymi do nich, jak również wytycznymi Centrum Systemów Informacyjnych Ochrony Zdrowia lub innych właściwych podmiotów.

II.4.1.3 Dostępność dostarczanego rozwiązania

Szpitalny System Informatyczny działa w trybie 24 godzinnym przez wszystkie dni w roku z dostępnością, co najmniej na poziomie 99% w skali miesiąca dla części białej HIS oraz e-usług. System nie jest dostępny, gdy występuje sytuacja uniemożliwiająca wykorzystanie którejś z jego funkcji z przyczyn leżących wewnątrz Systemu (np. Awarii, spadku przepustowości Systemu i wynikającego stąd przeciążenia Systemu, Awarii Infrastruktury). Planowane prace serwisowe (tzw. down time) odbywają się wyłącznie w soboty i niedziele w godzinach od 20:00 do 22:00. W ciągu jednego miesiąca mogą odbyć się maksymalnie cztery takie przerwy.

Czas planowych prac serwisowych (down time) nie jest liczony jako niedostępność i musi być uzgodniony z Zamawiającym i przez niego zaakceptowany w formie pisemnej (mailowej lub w formie pisma).

II.4.1.4 Stan obecny oprogramowania dziedzinowego HIS i ERP

Zamawiający eksploatuje obecnie oprogramowanie dziedzinowe w zakresie oraz ilościach przedstawionych w poniższej tabeli. Oprogramowanie jest w pełni zintegrowane. Oprogramowanie dziedzinowe pozostaje w opiece serwisowej i konserwacji producenta Kamsoft S.A.

Nazwa Modułu	Przedmiot i rodzaj Licencji	Ilość Licencji
HIS		
Moduł Rejestracja Poradnia	stanowisko	35
Moduł lekarski Gabinet ogólny	stanowisko	100
Moduł lekarski Okulista	stanowisko	6
Rehabilitacja planowanie zabiegów	stanowisko	17
Rejestracja internetowa	system	1
Umowy Enterprise	system	1

Scheduler	system	1
Moduł fiskalny - kasa	stanowisko	5
Wyróżnienie rezerwacji – pacjenci z deklaracjami	system	1
Terminarz z uwzględnieniem poradni	system	1
Cyfrowe podpisywanie EDM	stanowisko	100
Archiwizacja cyfrowo podpisanej EDM	system	1
Zmienny kwant czasu w terminarzu	system	1
Wspomaganie rozliczeń JGP w AOS	stanowisko	71
BLOZ Odpłatności	stanowisko	158
Słowniki ICD	system	1
Integracja z systemem Kadrowo - Płacowym	serwer	1
Integracja z systemem Finansowo - Księgowym	serwer	1
Integracja z systemem laboratoryjnym	serwer	1
Laboratoryjny system informatyczny LIS		
SYSTEM ALAB	Integracja przez portal ALAB	Opis integracji II.4.2
Wspomaganie prowadzenia kontroli jakości (KJ)	system	1
Podłączenie drukarki fiskalnej - Kasa	stanowisko	1
Integracja z systemem Finansowo - Księgowym	serwer	1
Integracja z systemem Kadrowo - Płacowym	serwer	1
System Magazynowy		
Stanowisko podstawowe magazyn	stanowisko	3
System Finansowo - Księgowy		
Stanowisko podstawowe	stanowisko	8
Koszty	system	1
Rozliczenia międzyokresowe	system	1
Rezerwy na należnościach	system	1
Fakturowanie	system	1
Grupowa weryfikacja czynnego podatnika VAT	system	1
Weryfikacja rachunków bankowych – Biała Lista	system	1
Moduł e-deklaracje	System	1
System Kadrowo Płacowy	System	1

Moduł kreatora podwyżek	System	1
Ewidencja Środków Materiałowych		
Stanowisko Podstawowe	stanowisko	2
Moduł obsługi źródeł finansowania	system	1
Moduł gospodarki remontowej	system	1

II.4.1.5 Zakres wdrożenia w zakresie SSI i e-usług

1. Zamawiający oczekuje rozbudowy obecnie eksploatowanego Oprogramowania Dziedzinowego o moduły wskazane w tabeli poniżej.

Nazwa Modułu	Przedmiot i rodzaj Licencji	Ilość Licencji
eRejestracja	serwer	1

Aktualizacja i wdrożenie do najnowszej wersji posiadanego przez Zamawiającego systemu informatycznego HIS i ERP, w zakresie posiadanych już licencji, wraz z kompleksowym przeszkoleniem wszystkich pracowników i osób działających w systemie w zakresie, którego dotyczy wdrożenie.

II.4.1.6 SSI – wymagania szczegółowe

Dostawa i wdrożenie SSI obejmuje rozszerzenie przedmiotu/ilości licencji. Wszystkie wymienione w niniejszym rozdziale aplikacje oraz te, które zostaną zaktualizowane do najnowszej wersji oprogramowania, muszą zostać objęte usługami wdrożeniowymi oraz serwisem gwarancyjnym.

II.4.1.7 Oprogramowanie aplikacyjne – wymagania ogólne

1. Wykonawca zobowiązuje się dostarczyć Zamawiającemu określone funkcjonalności SSI, poprzez rozszerzenie dotychczas eksploatowanego rozwiązania w taki sposób, aby w jak najszerszym zakresie zostały zaspokojone potrzeby Zamawiającego.
2. Zamawiający wymaga w zakresie dostarczonego rozwiązania informatycznego, aby w pełni współpracowało z posiadanym i eksploatowanym przez Zamawiającego HIS Dziedzinowym i ERP bez konieczności dokonywania w nim zmian.
3. System musi być przystosowany do wymiany danych z platformami ogólnokrajowymi P1/P2. Dane integrowane pomiędzy modułami HIS, e-usługami oraz aktualnie użytkowanym oprogramowaniem HIS muszą być spójne, edytowalne, podlegające analizie i spełniające warunki walidacji dla określonych typów pól.
4. Zakres danych przetwarzanych przez moduły HIS i e-usługi obejmujących dokumentowanie z procesu udzielania świadczeń składających się na dokumentacje zbiorczą i indywidualną zarówno zewnętrzną jak i wewnętrzną musi być zgodny z zakresem określonym przepisami prawa, płatnika publicznego świadczeń, akredytacji i przekazanych przez szpital wzorów dokumentów.
5. Moduły HIS i e-usługi muszą być dostosowane do struktury organizacyjnej Zamawiającego.

6. Moduły HIS i e-usługi muszą tworzyć i utrzymywać log systemowy (datę i godzinę z dokładnością do sekundy; adres IP stacji lub jej nazwa, unikalny identyfikator użytkownika, a jeżeli dane w Systemie uległy zmianie to również informacje o tym, z jakiej wartości i na jaką wartość została dokonana zmiana), rejestrujący w szczególności zapisy o zalogowaniu do Systemu i wylogowaniu z Systemu każdego z użytkowników.
7. Moduły HIS i e-usługi muszą mieć możliwość definiowania listy personelu białego (w szczególności lekarzy, pielęgniarek, położnych, techników) i ich specjalności zgodnie ze słownikiem i wymaganiami NFZ.
8. Moduły HIS i e-usługi muszą być zintegrowane, przez co rozumie się zintegrowaną pracę wszystkich systemów/modułów w oparciu o swobodną, automatyczną wymienialność danych pomiędzy elementami (modułami) systemu. Aplikacje działają na jednej wspólnej strukturze danych i nie wymagają odrębnego uwierzytelniania (po jednokrotnym zalogowaniu w dowolnym module użytkownik jest zalogowany do wszystkich, do których posiada uprawnienia).
9. Moduły HIS i e-usługi muszą pozwalać na obsługę zdarzeń niepożądanych oraz zapewnić funkcjonalność podglądu księgi zdarzeń niepożądanych. Nadawanie dostępu do funkcjonalności zgodnie z nadanymi uprawnieniami. System musi posiadać możliwość zarejestrowania oraz analizy zdarzeń niepożądanych zgodnie ze standardami akredytacyjnymi publikowanymi przez Centrum Monitorowania Jakości w Ochronie Zdrowia.
10. Moduły HIS i e-usługi muszą posiadać możliwość zarejestrowania oraz analizy zdarzeń zgodnie ze standardami akredytacyjnymi publikowanymi przez Centrum Monitorowania Jakości w Ochronie Zdrowia.
11. Wdrażanie dostarczanego Modułu HIS i e-usługi musi uwzględniać ciągłość funkcjonowania Zamawiającego i eksploatacji posiadanego przez niego HIS Dziedzinowego i ERP. Przez sformułowanie ciągłość pracy Zamawiający rozumie takie przeprowadzenie wdrożenia i migracji danych (na nowe środowisko), które nie będzie powodowało przerw w pracy poszczególnych jednostek organizacyjnych Zamawiającego. W szczególności zapewniona będzie ciągłość: rejestrowania i korzystania z danych przez personel Zamawiającego, dokonywania rozliczeń z NFZ i kontrahentami, sporządzania wymaganej prawem sprawozdawczości. Wszelkie przerwy w tym zakresie wynikające z prowadzonych przez Wykonawcę prac wdrożeniowych muszą zostać uzgodnione z producentem HIS Dziedzinowego i zatwierdzone przez Zamawiającego.
12. Moduły HIS i e-usługi pracują na systemach operacyjnych MS Windows wersjach wspieranych przez firmę Microsoft .
13. Moduły HIS i e-usługi muszą posiadać mechanizmy umożliwiające zapis i przeglądanie danych o logowaniu się użytkowników pozwalające na uzyskanie informacji o czasie i miejscach ich pracy. Log systemu rejestruje wszystkich użytkowników i wykonane przez nich czynności z możliwością analizy historii zmienianych wartości danych. Administrator musi mieć możliwość wyboru danych, które mają być monitorowane w logach systemu z dokładnością do poszczególnych kolumn w tabelach danych.
14. Moduły HIS i e-usługi automatycznie kodują dane zapisywane w logach systemowych na serwerze WWW.
15. W ramach Modułu HIS i e-usługi musi być zapewnione oprogramowanie narzędziowe pozwalające na definiowanie i generowanie dowolnych zestawień i raportów w oparciu o zawartość informacyjną bazy danych, która musi być wspólna dla wszystkich aplikacji SSI.
16. HIS umożliwia przesyłanie i odbieranie wiadomości tekstowych oraz nagrywanie i udostępnianie wiadomości głosowych w dokumentacji medycznej w kontekście konkretnego pacjenta.

17. W HIS wykorzystywane są następujące wspólne dla całego systemu standardowe zbiory słownikowe:
    1) Rozpoznań zgodnie z aktualną klasyfikacją ICD-10.
    2) Procedur medycznych zgodnie z nową edycją klasyfikacji procedur ICD-9 CM.
    3) Kodów terytorialnych.
    4) Płatników (w tym oddziałów NFZ) i umów z nimi zawartych.
    5) Użytkowników.
    6) Jednostek i lekarzy kierujących.
    7) Terminarzy pracy lekarzy
    8) Katalogów badań.
    9) Kontrahentów.
    10) Katalogu leków (w tym receptariusza szpitalnego).
    11) Miejscowości i kodów terytorialnych.
    12) Kodów kreskowych (użytkownik, pacjent, dokument).
    13) Innych, które zostaną ustalone z Zamawiającym w ramach Analizy przedwdrożeniowej.
18. Moduły HIS i e-usługi zintegrowane z HIS mają możliwość budowania wewnętrznego szpitalnego katalogu procedur medycznych, którym jest nadrzędnym katalogiem w stosunku do ICD-9 i wykorzystywanym przez użytkowników systemu. Katalog procedur wewnętrznych jest powiązany z ICD-9 w relacji n do m. (tzn. wiele procedur wewnętrznych może być skorelowane z wieloma procedurami z katalogu ICD-9). Celem katalogu procedur wewnętrznych jest jak najlepsze semantyczne odwzorowanie przypadków klinicznych, natomiast cała sprawozdawczość do NFZ jest realizowana w oparciu o katalog ICD-9. Definiowanie z jednego miejsca hierarchicznej struktury organizacyjnej Zamawiającego.
19. Jeżeli SSI posiada architekturę, w której formularze otwierane są kaskadowo, udostępnia także narzędzie prezentujące ścieżkę zagłębienia użytkownika w danym momencie w aplikacji (np. breadcrumb). Funkcja umożliwia śledzenie jego aktualnej lokalizacji w aplikacji oraz przyspieszoną nawigację dzięki umożliwieniu powrotu do dowolnego miejsca ścieżki.
20. Wszystkie przyciski wykorzystujące skróty klawiszowe jako klawisze funkcyjne (F1…F12) mają je jawnie oznaczone na przycisku tzn. tan sam klawisz funkcyjny wywołuje analogiczny skutek np. F1 = wywołania help.
21. W Zintegrowanym Systemie Informatycznym listy wyboru muszą być dynamicznie ograniczane zgodnie z wyszukiwaną frazą podawaną przez użytkownika. Funkcja ta musi uwzględniać polskie znaki diakrytyczne.
22. W polach, do których podpięte są listy wyboru od razu wpisywana jest wartość domyślna, do której zatwierdzenia wystarcza jeden klawisz/kliknięcie myszką - wymaganie będzie realizowane dla tych pól, które mają zdefiniowane wartości domyślne.
23. W Zintegrowanym Systemie Informatycznym jest dostępna pomoc kontekstowa – Help dla wszystkich modułów w języku polskim minimalnie z dokładnością do ekranu, z którego została uruchomiona pomoc.

24. Językiem obowiązującym w systemie, w chwili instalacji, musi być język polski. Dotyczy to wszystkich menu, ekranów, raportów, wszelkich komunikatów, wprowadzania, wyświetlania, sortowania i drukowania. Polskie znaki diakrytyczne będą, w chwili instalacji, dostępne w każdym miejscu i dla każdej funkcji w Zintegrowanym Systemie Informatycznym łącznie z wyszukiwaniem, sortowaniem (zgodnie z kolejnością liter w polskim alfabecie), drukowaniem i wyświetlaniem na ekranie.
25. System zapewnia mechanizmy walidacji haseł użytkowników zgodnie z wymaganiami ustawowymi przewidzianymi dla rodzaju danych przetwarzanych przez Zintegrowany System Informatyczny.
26. Zintegrowany System Informatyczny umożliwia w tożsamy sposób i z jednego miejsca zarządzanie uprawnieniami użytkowników całego rozwiązania informatycznego z wykorzystaniem usługi Active Directory oraz zachowaniem zasady jednokrotnego logowania z wykorzystaniem infrastruktury PKI.
27. Zintegrowany System Informatyczny zapewnia dwa mechanizmy spójności danych tego samego rekordu edytowanych w równoległych sesjach:
    1) edycja wyłącznie w jednej sesji: rozpoczęcie edycji w jednej sesji blokuje edycję w pozostałych sesjach, które mogą jednak uzyskać dostęp do danych w trybie odczytu. Przed rozpoczęciem edycji w kolejnej sesji pierwsza sesja musi zatwierdzić zmiany, a druga odświeżyć dane przed rozpoczęciem ich edycji;
    2) edycja równoległa ten sam rekord może być edytowany równolegle w wielu sesjach. Zmiany niekonfliktowe (różnych atrybutów) wykonane w innej sesji są automatycznie odświeżane w momencie zapisania zmian w bieżącej sesji. Zmiany konfliktowe (dwie sesje równolegle zmodyfikowały ten sam atrybut) są obsługiwane wg dwóch alternatywnych trybach albo automatyczne nadpisanie (np. data ostatniej edycji rekordu) albo zapytanie do użytkownika.
28. Zintegrowany System Informatyczny zapewnia możliwość przenoszenia sesji użytkownika z jednego stanowiska komputerowego na drugie. Przy uruchomienia na jednej stacji wielu sesji przez użytkownika, system zapewnia możliwość przeniesienia tylko jednej, wskazanej sesji.
29. Uaktualnienia aplikacji w Zintegrowanym Systemie Informatycznym muszą być w sposób automatyczny rozpowszechniane na wszystkie stacje robocze/terminale. Zintegrowany System Informatyczny dysponuje narzędziem konfekcjonującym i instalującym uaktualnienia opublikowane przez Wykonawcę.
30. W Zintegrowanym Systemie Informatycznym jest zaimplementowana obsługa skrótów klawiaturowych (kombinacje klawiszy hot-keys) dedykowanych Administratorowi oraz zaawansowanym użytkownikom (definiowane na poziomie uprawnień) umożliwiająca realizację następujących funkcji:
    a) uzyskanie z poziomu aplikacji informacji o elemencie bazodanowym reprezentowanym przez dany obiekt interfejsu użytkownika (przyciski, pola edycyjne) wraz z prezentacją wszystkich schematów uprawnień, w których wybrany obiekt można użyć do przydzielenia/modyfikacji uprawnień,
    b) uzyskania z poziomu aplikacji informacji o lokalizacji rekordu danych w bazie danych powiązanego z polem, w którym znajduje się kursor,
    c) stworzenia z poziomu aplikacji zapytania za pomocą sql do bazy danych w celu uzyskania żądanego wykazu danych,

d) uzyskania z poziomu aplikacji informacji o nazwie i wersji formularza, na którym obecnie użytkownik pracuje,

e) uzyskania z poziomu aplikacji informacji o identyfikatorach zewnętrznych nadanych przez płatnika NFZ w komunikacji za pomocą formatu otwartego.

31. Pola formularzy w Zintegrowanym Systemie Informatycznym: obligatoryjne, opcjonalne i wypełniane automatycznie muszą być jednoznacznie rozróżnialne przez Użytkownika (np. inny kształt, kolor, itp.). System dynamicznie, w zależności od kontekstu i aktualnie wprowadzonych danych, steruje opcjonalnością i obligatoryjnością innych elementów GIU.
32. Zintegrowany System Informatyczny umożliwia Administratorowi z poziomu aplikacji definiowanie i zmianę praw dostępu dla poszczególnych Użytkowników i grup Użytkowników z dokładnością do poszczególnych:
    1) modułów,
    2) jednostek organizacyjnych,
    3) opcji menu,
    4) formularzy, w tym również przycisków w obrębie formularzy,
    5) raportów.
33. System umożliwia tworzenie dowolnej dokumentacji medycznej w postaci elektronicznej HL7 CDA level 3 odwzorowującej zakres działalności komórek organizacyjnych Zamawiającego ewidencjonowany w modułach tradycyjnej (formularzowej) dokumentacji medycznej.
34. Zintegrowany System Informatyczny zapewnia funkcjonalności umożliwiające prowadzenie repozytorium EDM (z obsługą przechowywania EDM) oraz wymianę EDM pomiędzy repozytorium Zamawiającego a Platformą P1.
35. Repozytorium EDM zapewnia funkcjonalność przyjmowania, archiwizacji i udostępniania EDM zgodnej z HL7 CDA.
36. Dostarczone moduły zintegrowane z Systemem Informatycznym muszą zapewnić integrację funkcjonalną z systemem teleinformatycznym, o którym mowa w art. 7 ust. 1 ustawy z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia (t.j. Dz.U.2022 poz.1555 z późn. zm.), co najmniej w zakresie opisanym w dokumentach: „Opis usług biznesowych Systemu P1 wykorzystywanych w systemach usługodawców", „Opis funkcjonalny Systemu P1 z perspektywy integracji systemów zewnętrznych" opublikowanych przez Centrum e-Zdrowie (dotychczas CSIOZ) https://www.cez.gov.pl/fileadmin/user_upload/opis_funkcjonalny_systemu_p1_z_perspektywy_integracji_systemow_zew_5811ab8ee8e37.pdf oraz „Minimalne wymagania techniczne i funkcjonalne dla systemów usługodawców" 2021-06-18 V2.0 (https://www.gov.pl/web/zdrowie/minimalne-wymagania-dla-systemow-uslugodawcow) oraz dokumentacja integracyjna dla obszaru Zdarzeń Medycznych i Indeksów EDM na postawie Rozporządzenia Ministra Zdrowia z dnia 26 czerwca 2020 r. w sprawie szczegółowego zakresu danych zdarzenia medycznego przetwarzanego w systemie informacji oraz sposobu i terminów przekazywania tych danych do Systemu Informacji Medycznej (Dz.U. z 2020 r. poz. 1253 ze zm.).
37. Zamawiający wymaga, by Zintegrowany System Informatyczny generował dokumenty w postaci elektronicznej i umożliwiał ich podpisywanie kwalifikowanym podpisem

elektronicznym, podpisem zaufanym oraz z wykorzystaniem sposobu potwierdzania pochodzenia oraz integralności danych dostępnego w systemie teleinformatycznym udostępnionym bezpłatnie przez Zakład Ubezpieczeń Społecznych oraz podpisem osobistym.

38. Zgodność z aktualnym stanem prawnym - oferowane Oprogramowanie jest zgodne z aktualnymi aktami prawnymi regulującymi organizację i działalność podmiotów leczniczych, systemu ubezpieczeń społecznych i opieki zdrowotnej w kraju. W ramach gwarancji realizowana jest usługa co najmniej pięcioletniego okresu nadzoru autorskiego i Wykonawca zapewnia aktualizację do zmieniających się przepisów prawa. Brak dostosowania funkcjonalności w ramach ww. nadzoru autorskiego podlega takim samym restrykcjom jak brak usunięcia w terminie Błędu krytycznego.

II.4.1.8 EDM i dokumentacja medyczna

II.4.1.9 Dostęp do dokumentów i elektroniczne zgody pacjenta

Przyjęte rozwiązanie dostępu do dokumentów medycznych oraz udzielania zgód dla pracownika medycznego lub podmiotu leczniczego muszą spełniać wymóg pełnej implementacji Dokumentacji integracyjnej Systemu P1 w zakresie:

1) obsługi ZM,
2) obsługi EDM,
3) nadawania dostępu do danych medycznych pacjenta (autoryzacja),
4) obsługi zgód pacjenta.

Obsługiwane są następujące tryby dostępu do dokumentów:

1) dostęp dla autora dokumentu,
2) dostęp dla pacjenta, którego dokument dotyczy,
3) dostęp w ramach kontynuacji leczenia (w obrębie podmiotu, w którym wytworzono dokument),
4) dostęp w trybie ratowania życia,
5) dostęp za zgodą pacjenta – wymaga weryfikacji zgody w systemie P1.

Weryfikacja zgód w trybie 5) może następować tylko i wyłącznie na poziomie Systemu P1.
System lokalny musi udostępniać usługi odczytu zgody pacjenta na dostęp do informacji o stanie zdrowia i odczytu zgody pacjenta na dostęp do dokumentacji medycznej zarejestrowanej w systemie P1 oraz usługi zapisu, odczytu i wyszukiwania zgód na świadczenie medyczne.

II.4.1.10 Dostęp do EDM – wymagania

Wdrożony system EDM zapewni dostęp do Elektronicznej Dokumentacji Medycznej pacjentom oraz personelowi medycznemu podmiotu leczniczego przez okres minimum 60 miesięcy..
Lokalizacja repozytorium EDM – lokalnie (Lokalne repozytorium LREDM) w podmiocie leczniczym lub w warstwie regionalnej (Regionalne repozytorium RREDM) nie może mieć wpływu na wymagane funkcjonalności w dostępie do dokumentów EDM. Lokalizacja repozytorium jest transparentna w kontekście funkcjonalności.

II.4.1.11 Skopiowanie EDM z repozytorium chmurowego do RREDM

Wykonanie kopii około 700 000 dokumentów z obecnie używanego rozwiązania repozytorium chmurowego EDM firmy Kamsoft do Regionalnego Repozytorium EDM (RREDM) budowanego w ramach Przedmiotu Zamówienia realizowanego przez Urząd Marszałkowski Województwa

Zachodniopomorskiego. Efektem przeniesienia dokumentów do regionalnego repozytorium ma być pełna kopia dokumentów elektronicznych z chmurowego rozwiązania Kamsoft do Regionalnego Repozytorium EDM Zamawiającego oraz ciągłe wysyłanie na bieżąco wytworzonej EDM jako dodatkowej kopii do regionalnego repozytorium przez okres gwarancji - 60 miesięcy.

II.4.1.12 Opis usługi – EDM dla lekarza

	EDM dla lekarza
L.p.	**Funkcjonalności minimalne**
1.	Umożliwienie pracownikowi medycznemu podmiotu leczniczego z poziomu systemu HIS dostępu do elektronicznej dokumentacji medycznej EDM wytworzonej poza podmiotem, w którym pracuje dany pracownik.
2.	Umożliwienie dostępu do elektronicznej dokumentacji medycznej EDM wytworzonej przez podmiot leczniczy pracownikom medycznym innych podmiotów.
3.	Umożliwienie pracownikom medycznym podmiotu leczniczego z poziomu systemu HIS raportowanie, wyszukiwanie i odczyt Zdarzeń Medycznych przechowywanych w systemie P1.
4.	Posiadany system HIS musi zapewniać: 1) możliwość deklaracji trybu dostępu do dokumentacji medycznej, 2) usługi odczytu zgody pacjenta na dostęp do informacji o stanie zdrowia za pośrednictwem systemu P1, 3) odczyt zgody pacjenta na dostęp do dokumentacji medycznej zarejestrowanej w systemie P1, 4) usługi zapisu, odczytu i wyszukiwania zgód na świadczenie medyczne za pośrednictwem systemu P1.
5.	Posiadany system HIS musi zapewnić korzystanie z e-Usługi przez pracowników medycznych. Interfejs użytkownika systemu HIS - pracownika medycznego musi zapewnić realizację co najmniej następujących zadań: 1) zapoznanie się z listą dokumentów pacjenta zaindeksowanych w systemie P1, z uwzględnieniem zadeklarowania trybu dostępu, 2) pobranie i wyświetlenie dokumentu medycznego pacjenta, z uwzględnieniem zadeklarowania trybu dostępu, 3) utworzenie i zapisanie dokumentu medycznego w repozytorium EDM (zgodnie z konfiguracją dla Zamawiającego – lokalnym lub regionalnym), 4) przeglądanie Zdarzeń Medycznych zarejestrowanych w systemie P1.

II.4.1.13 Opis usługi – EDM dla pacjenta

	EDM dla pacjenta
L.p	**Funkcjonalności minimalne**
1.	Integracja SSI z systemem P1 zapewni możliwość indeksowania dokumentacji medycznej wytworzonej w podmiocie leczniczym oraz raportowanie zdarzeń medycznych.
2.	Dostęp przez Pacjenta do dokumentów EDM i zdarzeń medycznych wytworzonych i przechowywanych przez podmiot leczniczy jest realizowany jedynie poprzez Internetowe Konto Pacjenta.
3.	Pacjent może pobrać całość swojej dokumentacji przechowywanej przez podmiot leczniczy i zaindeksowanej w P1 wykorzystując Internetowe Konto Pacjenta.

II.4.1.14 E-rejestracja (lokalna na stronie www podmiotu leczniczego)

L.p.	Opis wymagań
1.	Aplikacja musi umożliwiać dokonywanie rezerwacji wizyt przez pacjenta metodą zdalną, za pośrednictwem Internetu.
2.	Aplikacja WWW musi być możliwa do wyświetlenia w dowolnej przeglądarce.
3.	Zabezpieczenie komunikacji z aplikacją przez bezpieczne, szyfrowanie połączenie (HTTPS).
4.	Indywidualne konto pacjenta na portalu musi być zakładane samodzielnie przez pacjenta. Do założenia konta tymczasowego pacjent musi podać następujące dane: imię, nazwisko, PESEL (tylko w przypadku posiadania obywatelstwa polskiego), data i miejsce urodzenia, płeć ,adres typ i numer dokumentu potwierdzającego tożsamość oraz adres e-mail. Po zatwierdzeniu danych portal wysyła kod aktywacyjny na podany przez pacjenta adres e-mail. Wprowadzenie i zatwierdzenie otrzymanego kodu powoduje automatyczne aktywowanie konta pacjenta. Tak założone konto ma status konta tymczasowego aż do momentu jego aktywowania przez upoważnionego pracownika jednostki, na podstawie wniosku dostarczonego przez pacjenta. Wniosek drukowany jest bezpośrednio z aplikacji po aktywowaniu konta tymczasowego.
5.	Konto tymczasowe musi pozwalać pacjentowi na przeglądanie grafików pracy poszczególnych lekarzy oraz pozwalać na rezerwację w danym czasie tylko jednego terminu wizyty.
6.	System e-Rejestracja musi zapewnić dostęp Pacjentowi do usługi e-Rejestracji za pomocą serwisu www za pośrednictwem indywidualnego konta z wykorzystaniem Węzła Krajowego oraz loginu i hasła (do wyboru przez Pacjenta).
7.	System e-Rejestracja musi zapewnić możliwość zakładania konta Pacjenta za pomocą Węzła Krajowego lub loginu i hasła (do wyboru przez Pacjenta). W przypadku Węzła Krajowego po autentykacji Pacjenta za pomocą narzędzi autentykacyjnych udostępnianych przez Węzeł Krajowy Pacjent zostanie poproszony o uzupełnienie co najmniej: numeru telefonu i adresu e-mail (pozostałe dane zostaną pobrane z Węzła krajowego: imię, nazwisko, PESEL lub seria i nr innego dokumentu potwierdzającego tożsamość dla osób nieposiadających PESEL, data urodzenia). W przypadku loginu i hasła zostanie udostępniony na stronie głównej formularz rejestracyjny zawierający dane, które jednoznacznie identyfikują nowego użytkownika. Nowy użytkownik musi obligatoryjnie uzupełnić co najmniej: imię, nazwisko, PESEL lub seria i nr innego dokumentu potwierdzającego tożsamość dla osób nieposiadających PESEL, data

	urodzenia, numer telefonu oraz adres e-mail. W przypadku loginu i hasła System e-Rejestracja zapewni możliwość resetu hasła przez Pacjenta bez konieczności wizyty u Zamawiającego.
8.	System umożliwia wykorzystanie certyfikatów niezbędnych do integracji z węzłem krajowym identyfikacji elektronicznej w celu integracji z systemem login.gov.pl na środowisku produkcyjnym, zgodnie z wymaganiami Ministerstwa Cyfryzacji opublikowanymi w dokumentacji na stronie mc.bip.gov.pl https://mc.bip.gov.pl/wezel-krajowy/wezel-krajowy-dokumentacja-dotyczaca-integracji-z-wezlem-krajowym.html w zakładce „Interoperacyjność MC”/ „Węzeł Krajowy - dokumentacja dotycząca integracji z Węzłem Krajowym”.
9.	Zabezpieczenie formularza tworzenia konta przed automatycznym wypełnianiem (kod CAPTCHA lub rozwiązanie alternatywne).
10.	Prezentacja i wymuszanie akceptacji regulaminu przy zakładaniu konta przez pacjenta.
11.	Automatyczne wysyłanie e-maila potwierdzającego podane dane kontaktowe.
12.	Możliwość logowania do aplikacji przy użyciu adresu e mail (lub nazwy konta) i hasła
13.	Możliwość samodzielnego wygenerowania nowego hasła przez pacjenta (opcja „Zapomniałem hasła”).
14.	Możliwość przeglądania listy poradni oraz ich dostępnych godzin pracy.
15.	Możliwość samodzielnej zmiany danych konta przez pacjenta (w szczególności danych kontaktowych i hasła).
16.	Możliwość samodzielnego planowania wizyt przez pacjenta z wyborem dnia, godziny i lekarza w określonej poradni.
17.	Możliwość zmiany terminu lub anulowania wizyty zaplanowanej przez pacjenta.
18.	Możliwość przeglądania przez pacjenta własnych wizyt planowanych i odbytych.
19.	Możliwość podglądu i wydruku danych wizyty przez pacjenta.
20.	Możliwość przeglądania i modyfikacji kont użytkowników przez administratora.
21.	Możliwość resetowania hasła pacjenta przez administratora,
22.	Możliwość przeglądania przez administratora wszystkich wizyt zaplanowanych w Rejestracji Internetowej oraz wizyt dotyczących wybranego pacjenta.
23.	Możliwość zmiany regulaminu i wymuszenia ponownego zaakceptowania go przez pacjentów.
24.	Możliwość dopasowania wyglądu strony do strony internetowej placówki.
25.	Możliwość określenia parametrów działania systemu: 1) maksymalna i minimalna liczba dni przed wizytą, kiedy można ją zaplanować lub odwołać, 2) czy mają być wysyłane powiadomienia o zbliżających się wizytach (do wyboru dla pacjenta), 3) liczba wizyt nieodbytych, po których planowanie dla pacjenta zostaje zablokowane, 4) liczby dni przed wizytą, kiedy ma być wysyłane przypomnienie o wizycie, 5) liczba wizyt planowanych możliwych do dodania przez pacjenta, 6) konieczność dodatkowego zatwierdzenia konta pacjenta przez pracownika poradni, zanim będzie mógł samodzielnie planować wizyty, 7) przedział czasowy godzin pracy poradni, na który jest możliwe planowanie wizyt przez Rejestrację Internetową,

	8) liczba wizyt, które można zaplanować w określonej poradni przez Rejestrację.
26.	Automatyczne wysyłanie powiadomień e-mail o: 1) utworzeniu konta przez pacjenta, 2) dodaniu zaplanowania wizyty, 3) zbliżającej się wizycie, 4) blokadzie konta po określonej liczbie nieodbytych wizyt, 5) zmianie hasła, 6) anulowaniu wizyty.
27.	Możliwość dodawania aktualności na stronie głównej aplikacji.
28.	Podłączenie do centralnej platformy e-zdrowia (P1) w zakresie wystawiania elektronicznych recept.
29.	Utworzenie i zapis elektronicznego dokumentu recepty oraz pakietu recept.
30.	Wydruk informacji dla pacjenta o wystawionych receptach.
31.	Przekazywanie kodów dostępowych umożliwiających automatyczną realizację recept.
32.	Przesłanie dokumentu recepty do centralnej platformy.
33.	Możliwość anulowania recepty.
34.	Pacjent korzystając z przygotowanej witryny internetowej może się zalogować, wybrać na podstawie różnych kryteriów interesującą go wizytę i zarezerwować ją.
35.	Informacja o dokonanej rezerwacji musi trafiać do systemu centralnego, gdzie wizyty z e-Rejestracji są wyraźnie oznaczone. Jednocześnie moduł korzysta z definicji tych samych grafików co system centralny.
36.	Rejestracja przez Internet musi mieć taki sam charakter i status jak rejestracja dokonana bezpośrednio w placówce medycznej.
37.	Rozwiązanie umożliwia pacjentowi wyszukanie wolnych terminów wizyt wg kryteriów: 1) lekarza lub poradni, 2) daty wizyty, 3) czasu jej trwania (od do). Do wyszukania najbliższej wolnej wizyty niezbędne jest podanie lekarza lub poradni.
38.	Wybranie kryterium poradni musi zawężać kryteria wyboru do lekarzy wyłącznie danej specjalizacji.
39.	Po wprowadzeniu kryteriów wyszukiwania funkcja musi wyświetlać listę wszystkich wolnych wizyt spełniających kryteria wraz z informacjami o typie wizyty (typy wizyt np.: prywatna, POZ, medycyna pracy, itp.). Typy wizyty są definiowane przez operatora w systemie centralnym.
40.	Rejestracja za pośrednictwem aplikacji może zostać ograniczona: 1) do wybranych poradni, lekarzy oraz gabinetów, 2) poprzez ustalenie liczby rezerwacji wprowadzanych przez pacjenta, 3) poprzez ustalenie liczby dni jakie muszą upłynąć pomiędzy kolejnymi rezerwacjami do tej samej poradni. 4) poprzez podanie maksymalnej ilości dni przed wizytą na którą pacjent może się zarejestrować.
41.	Możliwość wprowadzenia blokady rejestracji dla pacjentów z kontem tymczasowym.
42.	Możliwość zblokowania rejestracji dla pacjenta pierwszorazowego w danej poradni.
43.	Możliwość udostępniania wyłącznie części grafiku na potrzebę e-rejestracji.

44.	Możliwość wprowadzenia blokady e-rejestracji dla pacjentów, którzy nie pojawiają się na wizycie pomimo potwierdzenia terminu.
45.	Możliwość blokady rezerwacji do poradni POZ dla pacjenta, który nie posiada aktywnej deklaracji złożonej w placówce.
46.	Możliwość zaprezentowania pacjentowi wstępnego wywiadu lekarskiego, który należy uzupełnić podczas rejestracji na wizytę. (Wywiady konfigurowane administracyjnie i przypisane do poszczególnych usług)
47.	Wywiady muszą trafiać do systemu HIS jako dokumenty.
48.	Przez określony czas, minimum 7 (siedem) dni od dnia wizyty, pacjent musi mieć możliwość, aby zadać pytanie lekarzowi do odbytej wizyty. Na zdefiniowany w systemie HIS adres mailowy lekarza przychodzi informacja o pytaniu pacjenta z linkiem do udzielenia odpowiedzi (wymagana autoryzacja loginem i hasłem lekarza z systemu HIS).
49.	System musi umożliwiać pacjentowi śledzenie statusu w kolejce oczekujących zdefiniowanej w oddziale, poradni, pracowni (e-Kolejka).
50.	Pacjent musi mieć możliwość przeglądania kolejek oczekujących – prowadzonych zgodnie z wymaganiami NFZ w tym zakresie oraz osobno statusów i historii pozostałych wizyt.
51.	Możliwość zdefiniowania automatycznych powiadomień pacjenta o zbliżających się terminach wizyt oraz innych zdarzeniach medycznych (np. termin badania, wizyty, informacje o badaniach profilaktycznych) za pomocą następujących kanałów komunikacji: SMS, e-mail, wiadomości systemowe dostępne po zalogowaniu do Portalu pacjenta.
52.	Możliwość definiowania niezależnych szablonów wiadomości dla każdego typu usług /porad, z określeniem szablonu domyślnego.
53.	Możliwość konfiguracji formatu treści wiadomości do wysyłki, w tym użycie parametrów: imię i nazwisko pacjenta, numer pacjenta, data wizyty (dd-mm-yyyy), dzień wizyty (dd), miesiąc wizyty (numer w formacie mm lub słownie), rok wizyty (yyyy), godzina wizyty (HH:mm), nazwa krótka usługi.
54.	Moduł musi zapisywać w bazie danych systemu wszystkie wysłane wiadomości wraz z datą ich wygenerowania. Wiadomości te są powiązane z wizytą, usługą, pacjentem oraz wykorzystanym szablonem wiadomości.
55.	Kontrola przed ponowną wysyłką tego samego komunikatu.
56.	Możliwość zdefiniowania godziny oraz cykli w dniach, w jakich pakiety wiadomości będą generowane do wysyłki.
57.	Możliwość zdefiniowania maksymalnej długości wiadomości SMS.
58.	Generowanie wiadomości tylko do tych pacjentów, którzy posiadają uzupełniony w systemie numer telefonu komórkowego.
59.	Możliwość określenia indywidualnie dla każdego pacjenta preferowanych kanałów komunikacyjnych w przypadku powiadomień o wizytach, badaniach, zbliżającym się terminie przyjęcia do placówki wg kolejki oczekujących, informacjach o badaniach profilaktycznych.
60.	Dla pacjentów posiadających konto stałe funkcja pozwalająca na przesłanie za pośrednictwem portalu „zamówienia” na wystawienie recepty (e-Recepty) na kontynuację leczenia.
61.	Umożliwienie pacjentowi wybrania z listy leków, które były już mu wcześniej przepisywane podczas wizyty w danym podmiocie leczniczym, tych pozycji, których dotyczy „zamówienie”.
62.	Umożliwienie po zatwierdzeniu przez pacjenta wybranych leków, aby wykaz ten automatycznie trafił do lekarza. Lekarz musi mieć możliwość zatwierdzenia, według własnego uznania, tych leków wskazanych przez pacjenta, które umieszczone zostaną na recepcie. Zwrotnie pacjent musi otrzymać informację o tym, które z wnioskowanych leków zostały umieszczone na recepcie. W przypadku gdy dany podmiot leczniczy wystawia już e-

	Recepty, to pacjent może udać się już wprost do dowolnej apteki, celem realizacji recepty (podpunkt 28). Aplikacja musi pozwalać pacjentowi na przeglądanie udostępnionych pacjentowi przez dany podmiot leczniczy wyników badań. Portal musi wyświetlać wyniki badań o statusie „zatwierdzone" w systemie centralnym (wydrukowane i zatwierdzone przez diagnostę w sposób tradycyjny).

II.4.1.15 Powiadomienia

L.p.	Opis wymagań
1.	Wysyłanie wiadomości tekstowych o dowolnej treści przez e-mail lub SMS.
2.	Możliwość konfiguracji wiadomości o dowolnej treści z możliwością wykorzystania dowolnych informacji w bazie danych systemu HIS.
3.	Możliwość konfiguracji dowolnych zdarzeń powodujących wysłanie wskazanych wiadomości (np. zdarzenie czasowe, akcja użytkownika, zdarzenie bazy danych).
4.	Określanie terminu ważności wiadomości, po którym niewysłana wiadomość staje się nieważna.
5.	Określanie zalecanego czasu wysłania wiadomości w postaci przedziału godzinowego.
6.	Powiadomienia e-mail: 1) obsługa wysyłania wiadomości e-mail przez wskazane konto i serwer SMTP, 2) możliwość wysyłania plików, jako załączniki do wiadomości e-mail.

II.4.1.16 Integracja z Krajowym Systemem Elektronicznej Rejestracji na Platformie P1

Mając na uwadze prowadzone przez Centrum e-Zdrowia prace, w wyniku których planowane jest uruchomienie Systemu Elektronicznej Rejestracji (e-Rejestracji centralnej) dla poniższych świadczeń:

- świadczenia w zakresie ortopedii i traumatologii narządu ruchu,
- świadczenia w zakresie kardiologii,
- świadczenia w zakresie neurologii,
- świadczenia w zakresie endokrynologii,
- rezonans magnetyczny,
- tomografia komputerowa,

Wykonawca dokona integracji systemu Zamawiającego (zewnętrznego w stosunku do P1) celem osiągnięcia następujących funkcjonalności:

L.p.	Opis wymagań
1.	System oprogramowania Zamawiającego bezpośrednio zapisuje pacjentów na wizyty dotyczące ww. świadczeń tylko w przypadku, kiedy dla danego świadczenia nie będzie osób oczekujących na wolny termin.
2.	Wykonawca jako dostawca oprogramowania musi zapewnić integrację systemu HIS z systemem P1 w zakresie zarządzanie harmonogramami oraz wizytami w Systemie Elektronicznej Rejestracji.
3.	System oprogramowania przesyła do Systemu Elektronicznej Rejestracji (SER) harmonogram zawierający wolne sloty. Wolny slot reprezentuje termin (datę i czas) dla danego świadczenia, który Zamawiający zgłasza do Systemu Elektronicznej Rejestracji w celu umożliwienia przypisania do niego pacjenta.
4.	Podmiot może dowolnie modyfikować i usuwać przesłane harmonogramy dopóki do danego wolnego slotu nie zostanie przypisany pacjent (zapisana wizyta).
5.	Uruchamiany minimum raz dziennie algorytm w systemie SER dokonuje wyboru pacjentów zgodnie z ich zapisanymi kryteriami dostępności, ustala ich kolejność na podstawie wag a

	następnie dokonuje przypisania do poszczególnych wolnych slotów zgłoszonych w ramach harmonogramów przez Podmiot.
6.	Po zakończeniu działania algorytmu, SER wysyła powiadomienia do pacjentów, którzy zostali zapisani na wizytę podczas ostatniego uruchomienia algorytmu z informacją, do którego Podmiotu zostali zapisani oraz na jaki dzień i godzinę.
7.	System oprogramowania odpytuje SER w celu pobrania informacji o zapisanych na wizyty pacjentach i zsynchronizowania ich w swoim systemie.
8.	Po uzyskaniu danych osobowych pacjenta przez system oprogramowania Podmiotu dalsza komunikacja między Podmiotem, a pacjentem realizowana jest bez udziału Systemu Elektronicznej Rejestracji.
9.	W komunikacji z systemem P1 wymagane jest użycie rozszerzenia Web Services Security i profilu Web Services Security X.509 Certificate Token Profile.
	Uwierzytelnianie Systemu
10.	Wszystkie usługi sieciowe Systemu Elektronicznej Rejestracji są zabezpieczone z wykorzystaniem mechanizmów WS-Security. System zewnętrzny jest zobowiązany do używania pary certyfikatów wystawionych podmiotowi przez Centrum Certyfikacji P1, tj. certyfikatu do uwierzytelnienia systemu (TLS) i certyfikatu do uwierzytelnienia danych (WS-Security).
11.	Uwierzytelnienie Systemu zewnętrznego wywołującego usługę systemu P1 następuje w warstwie transportowej połączenia za pomocą protokołu TLS z obustronnym uwierzytelnieniem - oprócz uwierzytelnienia serwera przez system zewnętrzny następuje uwierzytelnienie klienta (Systemu zewnętrznego) przez serwer.
12.	Do nawiązania połączenia TLS system zewnętrzny zobowiązany jest użyć certyfikatu do uwierzytelnienia systemu wydanego przez Centrum Certyfikacji P1 (użycie przez klienta P1 klucza prywatnego powiązanego z certyfikatem do uwierzytelnienia systemu przekazanego przez CeZ w wyniku założenia konta).
	Uwierzytelnianie danych
13.	System zewnętrzny zobowiązany jest do podpisania komunikatu SOAP z użyciem certyfikatu do uwierzytelnienia danych służącego do weryfikacji złożonego podpisu cyfrowego.
14.	Po poprawnej weryfikacji podpisu cyfrowego na podstawie certyfikatu do uwierzytelnienia danych identyfikowany i uwierzytelniany jest Usługodawca, w kontekście którego realizowana będzie usługa.
15.	Po uwierzytelnieniu następuje autoryzacja, na którą składa się autoryzacja wykonania usługi oraz autoryzacja dostępu do danych. Autoryzacja wykonania usługi polega na sprawdzeniu przydzielenia do konta Usługodawcy uprawnienia związanego z wywoływaną usługą. Autoryzacja dostępu do danych wykonywana jest w określonych przypadkach i weryfikuje możliwość dostępu do danych na podstawie parametrów wywołania usługi (np. dostęp podmiotu do zarezerwowanej w nim wizyty).
16.	Za uwierzytelnienie Użytkownika końcowego Usługodawcy odpowiedzialny jest System zewnętrzny.
17.	System zewnętrzny uwierzytelnia Użytkowników końcowych, a następnie przekazuje żądania do systemu P1. Tam gdzie jest to wymagane system zewnętrzny deklaruje informacje o Użytkowniku końcowym (np. przez przekazanie identyfikatora pracownika medycznego lub pracownika administracyjnego zgodnie z ustalonym formatem).
18.	System P1 nie realizuje powtórnego uwierzytelnienia Użytkownika końcowego, w kontekście którego wykonywana jest usługa sieciowa.
19.	Scenariusz wywołania usług: a) pobranie informacji o wizytach; b) zapis pacjenta na listę oczekujących;

	c) anulowanie/zmiana zapisu pacjenta na listę oczekujących; d) zapis pacjenta na wizytę e) anulowanie / zmiana zapisu na wizytę.

II.4.1.17 Instruktaże stanowiskowe

1. Z uwagi na to, iż w ramach Projektu planuje się wdrożenie specjalistycznego oprogramowania i aplikacji, konieczne jest przeszkolenie personelu Zamawiającego. W związku z tym w ramach tego zadania zostaną zrealizowane instruktaże stanowiskowe.
2. Wykonawca przeprowadzi instruktaże stanowiskowe w siedzibie Zamawiającego i/lub jego placówkach.
3. Na podstawie przekazanego przez Zamawiającego wykazu osób oraz przewidywanego terminu i czasu instruktażu stanowiskowego, Wykonawca zaproponuje harmonogram jak i podział na grupy.
4. Szczegółowy harmonogram realizacji instruktaży zostanie uzgodniony na etapie Analizy Przedwdrożeniowej.
5. Harmonogramy instruktaży muszą umożliwiać informatykom Zamawiającego obecność na zajęciach z danego tematu przeznaczonych dla innych grup zawodowych, z zastrzeżeniem, że na jednych zajęciach z danego tematu może być obecny co najmniej 1 informatyk.
6. Wykonawca nie ponosi odpowiedzialności za brak uczestnictwa Użytkowników w instruktażach stanowiskowych.
7. Instruktaże stanowiskowe Użytkowników oprogramowania SSI i Administratora będą musiały spełniać minimum następujące wymagania:
   1) zajęcia muszą odbywać się w godzinach od godz. 8.00 do 15.00, lub innych za zgodą Zamawiającego,
   2) zajęcia nie będą mogły trwać dłużej niż 6 godzin dziennie.
8. Za skuteczne przeprowadzenie instruktażu stanowiskowego uważa się dostępność w ustalonym miejscu i terminie przedstawicieli Wykonawcy, gotowych przeprowadzić instruktaż zgodnie z ustalonym harmonogramem przy założeniu, że szkolenie ma również charakter warsztatów (tzn. szkolący się mają zajęcia praktyczne z obsługi przy komputerze przy założeniu jeden szkolący na jeden komputer). Zamawiający zapewni sprzęt komputerowy w ilości 4 sztuk. W przypadku gdyby była potrzeba zapewnienia większej ilości sprzętu komputerowego tak aby zakończyć wdrożenie w zadeklarowanym czasie odpowiedni sprzęt komputerowy musi dostarczyć Wykonawca. Dotyczy to w szczególności szkoleń w przypadku wymiany Systemu.
9. Wykonawca w ramach instruktażu stanowiskowego przekaże instrukcje do wdrożonego Systemu oraz materiały szkoleniowe. Instruktaże stanowiskowe muszą być prowadzone w języku polskim.
10. W ramach przeprowadzonych instruktaży stanowiskowych wymaga się:
    1) przekazania wiedzy niezbędnej do poprawnego użytkowania wdrożonego Systemu, jego zakresu funkcjonalnego,
    2) przekazania wiedzy w zakresie tworzenia i gromadzenia informacji, tworzenia i gromadzenia dokumentów, wykonywania analiz, sprawozdań i raportów.

11. Zakres instruktaży stanowiskowych musi objąć teorię i praktykę (musi być zapewniona odpowiednia liczba ćwiczeń – minimum w stosunku 50% / 50%) tak, aby personel Zamawiającego mógł podjąć samodzielnie użytkowanie wdrożonego oprogramowania SSI.
12. Gdy Wykonawca rozszerza funkcjonalność o moduły, to instruktaże stanowiskowe muszą być prowadzone w dwóch kategoriach:
    3) dla Użytkowników Oprogramowania SSI – 8 godzin,
    4) dla Administratorów – 16 godzin.
13. Liczba pracowników Zamawiającego do przeprowadzenia instruktaży stanowiskowych
    i. Lekarze Medycyny Pracy - 6 osób
    ii. Specjaliści -20 osób,
    iii. Pielęgniarki – rejestracja 1 osoba
    iv. Administratorzy – 3 osoby.
14. Administratorzy po zakończeniu instruktaży muszą w szczególności umieć wykonywać czynności administracyjne, a także instalacji Oprogramowania systemowego i narzędziowego oraz oprogramowania SSI, znać i umieć realizować procedury backupu, znać wytyczne w zakresie polityki bezpieczeństwa i umieć je stosować. Ponadto muszą znać typowe zagrożenia i problemy związane z funkcjonowaniem Systemu, a także sposoby ich wykrywania oraz przeciwdziałania. Muszą umieć instalować, konfigurować, rekonfigurować, monitorować i prawidłowo eksploatować dostarczony Sprzęt i Oprogramowanie, jak również znać jego wdrożoną konfigurację.

II.5 Wariant opcjonalny

II.5.1 Opcjonalny zakres przedmiotu zamówienia

Zamawiający zastrzega sobie możliwość skorzystania z prawa opcji zgodnie z art. 441 ustawy Pzp w odniesieniu do następującego zakresu zamówienia:

Opcja nr 1:

e-Usługa udostępniania EDM z udziałem Regionalnego Repozytorium EDM (integracja Warstwy Lokalnej z Regionalnym Repozytorium EDM). Opcja zakłada, że informacje o elektronicznej dokumentacji medycznej do P1, będzie przekazywało Repozytorium Regionalne. Integracja między repozytorium lokalnym PP a regionalnym ma służyć tylko do dalszego udostępniania EDM do P1.

Zamawiający skorzysta z Opcji nr 1 w przypadku wyłonienia wykonawcy Warstwy Regionalnej w postępowaniu o zamówienie publiczne i sporządzenia przez tego wykonawcę Dokumentacji integracyjnej zgodnie z Modelem realizacyjnym (**załącznik nr 4** do SWZ).

W pkt II.5.3 niniejszego OPZ zostały przedstawione kluczowe informacje istotne z punktu widzenia sposobu implementacji dostępu do Regionalnego Repozytorium EDM. Ogólna architektura projektu ZeZ w przypadku integracji Warstwy Lokalnej z Regionalnym Repozytorium EDM została przedstawiona w pkt II.5.2 OPZ. Opcja w realizacji przedmiotowego zakresu zamówienia może obejmować godziny wdrożeniowe. Zamawiający przez jedną godzinę wdrożeniową rozumie czas w ilości 1h (60 min) jakie Wykonawca przeznacza na wdrożenie. Zakładana pracochłonność wymagana dla realizacji tego zakresu projektu wynosi 700 godzin.

Zamawiający wskazuje maksymalną wartość opcji jako iloczyn wartości roboczogodziny podanej przez Wykonawcę w ofercie dla Opcji nr 1 oraz ilości 700 godzin. Comiesięczne rozliczenie

wynagrodzenia za wykonanie Przedmiotu Zamówienia w Opcji nr 1 odbywać się będzie na podstawie zestawienia godzin poświęconych na realizację tego zakresu w danym miesiącu, przygotowywanych przez Wykonawcę i zaakceptowanych przez Zamawiającego.

Opcja nr 2:

Dostosowanie wdrażanego oprogramowania do nowych wymagań funkcjonalnych, które w okresie realizacji zamówienia mogą być wymagane w wyniku wprowadzanych zmian organizacyjnych w obszarze informatyzacji systemu ochrony zdrowia w Polsce, w tym rekomendacji MZ/CeZ lub wymagań Zamawiającego.

Zamawiający skorzysta z Opcji nr 2 w przypadku wejścia w życie wytycznych lub rekomendacji MZ/CeZ, sugerujących konieczność osiągnięcia nowych funkcjonalności, nieprzewidzianych w pierwotnym przedmiocie zamówienia. Przez dostosowanie wdrażanego systemu oprogramowania, Zamawiający rozumie zapewnienie usług rozwojowych rozumianych jako pula godzin rozwojowych do dyspozycji Zamawiającego na modyfikacje, których nie dało się przewidzieć na etapie przygotowywania SWZ. Zamawiający przez jedną godzinę rozwojową rozumie czas w ilości 1h (60 min) jakie Wykonawca przeznacza na wdrożenie zgłoszonej przez Zamawiającego modyfikacji realizując m.in. takie usługi jak: analiza wymagań, prace programistyczne, wdrożenie.

Zamawiający wskazuje maksymalną wartość opcji jako iloczyn wartości roboczogodziny podanej przez Wykonawcę w ofercie dla Opcji nr 2 oraz ilości 350 godzin. Comiesięczne rozliczenie wynagrodzenia za wykonanie Przedmiotu Zamówienia w Opcji nr 2 odbywać się będzie na podstawie zestawienia godzin poświęconych na realizację tego zakresu w danym miesiącu, przygotowywanych przez Wykonawcę i zaakceptowanych przez Zamawiającego.

W formularzu ofertowym Wykonawca musi wycenić zamówienie podstawowe oraz zamówienie opcjonalne w obu opcjach.

II.5.2 Ogólna architektura projektu ZeZ w przypadku integracji Warstwy Lokalnej z Regionalnym Repozytorium EDM

W odniesieniu do poszczególnych e-usług w zależności od uwarunkowań implementacji wymagany jest następujący poniżej omówiony zakres prac.

Dla e-usług założono i przyjęto udział obecnych i planowanych rozwiązań zarówno na poziomie centralnym, na poziomie warstwy regionalnej - Województwa Zachodniopomorskiego oraz na poziomie warstwy lokalnej - Zamawiającego:

1) Poziom centralny, w tym w szczególności P1 w zakresie:
   a) Internetowe Konto Pacjenta (IKP),
   b) rejestr Elektroniczna Dokumentacja Medyczna (EDM) w obecnym i dalszych rozszerzeniach zakresu stosowania dla kolejnych dokumentów medycznych (od 25 kwietnia 2020 r. EDM stanowią również m.in. opisy badań diagnostycznych innych niż laboratoryjne, a od 25 kwietnia 2021 r. są to także wyniki badań laboratoryjnych wraz z opisem),
   c) Zdarzenia Medyczne,
   d) zgody Pacjenta,
   e) kolejne e-usługi planowane do uruchomienia w przyszłości, m.in. e-Rejestracja, e-Wizyty, zamawianie e-Recept,

f) uwierzytelnianie z wykorzystaniem Węzła Krajowego Identyfikacji Elektronicznej poprzez: Profil zaufany (PZ), e-dowód oraz mojeID - przy pomocy banku lub innego dostawcy tożsamości.

2) Warstwa regionalna w zakresie:

Platforma regionalna (www) o następującym zakresie funkcjonalnym:

a) Regionalne Repozytorium EDM,
b) Portal Projektu ZeZ,
c) Systemy analityczne:
   1. System Analiz Zarządczych
   2. System Analiz Sprawozdawczych
   3. Platforma zakupowa SPZOZ/Grupowe zamówienia

Warstwa regionalna wspiera i uczestniczy w świadczeniu usług oraz zapewnia udostępnianie EDM dla pacjenta i innym podmiotom leczniczym.

3) Warstwa lokalna na poziomie Partnera (Zamawiającego):

a) integracja z krajowym Systemem Elektronicznej Rejestracji na Platformie P1,
b) e-Rejestracja lokalna przez stronę www w powiązaniu z e-Rejestracją centralną (SER),
c) lokalne repozytorium EDM,
d) integracja z Regionalnym Repozytorium EDM,
e) EDM i zdarzenia medyczne dla pacjenta (poprzez IKP)
f) EDM i zdarzenia medyczne dla lekarza,
g) przesyłanie indeksów EDM oraz danych o zdarzeniach medycznych do P1,
h) odczyt i zapis zgód pacjenta na potrzeby integracji z P1.

Warstwa lokalna świadczy usługi dla pacjentów z zastosowaniem poziomu centralnego oraz warstwy regionalnej.

Rejestr oraz repozytorium EDM wskazane na poziomie centralnym i w warstwach regionalnej i lokalnej, rozumiane są następująco:

- źródłem danych dla dokumentacji EDM (Document Source) jest system części białej (HIS, LIS, RIS) w podmiocie leczniczym,
- dokumenty EDM są składowane i archiwizowane w repozytorium lokalnym podmiotu leczniczego;
- informacje opisujące dokumentację medyczną (metadane, indeksy) oraz wskazujące gdzie przechowywana jest właściwa dokumentacja zawarte są w Rejestrze EDM w P1 w ramach Krajowej Domeny (IHE XDS.b),
- informacje do Rejestru EDM są przekazywane bezpośrednio przez podmiot leczniczy,
- **Regionalne Repozytorium EDM jest zasilane dokumentami EDM z lokalnego repozytorium EDM podmiotu leczniczego (Zamawiającego) - Partnera Projektu ZeZ;**
- **Regionalne Repozytorium pełni rolę Document Repository EDM podmiotu leczniczego (Zamawiającego) - Partnera Projektu ZeZ;**
- **kierowanie zapytań o dokumentację EDM z wykorzystaniem rejestru EDM w P1 oraz zgody pacjenta od innych świadczeniodawców odbywa się do Regionalnego Repozytorium,**
- **udostępnianie EDM dla zewnętrznych użytkowników (pacjentów i pracowników medycznych) odbywa się z Regionalnego Repozytorium EDM poprzez Internetowe**

Konto Pacjenta w systemie P1 (dla pacjentów) lub poprzez systemy dziedzinowe, w tym HIS (dla pracowników medycznych).

Uwagi:

- warstwa regionalna nie prowadzi rejestru (indeksów) EDM. Indeksowanie EDM w P1 prowadzone jest przez Partnera Projektu ZeZ;
- Indeks Pacjenta nie jest wymagany na poziomie regionalnym;
- **raportowanie/przekazywanie informacji o Zdarzeniach Medycznych będzie realizowane przez podmiot leczniczy lokalnie ze wskazaniem Regionalnego Repozytorium jako Document Repository EDM;**
- **wdrożenie Regionalnego Repozytorium jako repozytorium uczestniczącego w wymianie i udostępnianiu dokumentacji EDM nie wyklucza możliwości przełączenia i wskazania jako Dokument Repository w rejestrze EDM P1 repozytorium lokalnego Partnera Projektu. Zapewnia redundantność zapisu danych EDM oraz jedno miejsce w Systemie udostępniania danych;**
- podmiot leczniczy wdraża e-Rejestrację lokalną, do której dostęp zapewniony będzie poprzez stronę (witrynę) www podmiotu leczniczego;
- systemy oprogramowania Zamawiającego zostaną zintegrowane z Systemem Elektronicznej Rejestracji na Platformie P1.

II.5.3 Struktura repozytoriów EDM (repozytorium regionalne oraz lokalne) w przypadku budowy Regionalnego Repozytorium EDM

Architektura systemu Zachodniopomorskie e-Zdrowie zaprezentowana jest szeroko w dokumencie *Model realizacyjny ZeZ* oraz w wersji skróconej w dokumencie stanowiącym **załącznik nr 4** do SWZ. Rozdział II.5.2 OPZ zawiera natomiast skrócony opis w kontekście założonej logiki procesów systemu ZeZ.

Poniżej przedstawione zostały kluczowe informacje istotne z punktu widzenia sposobu implementacji dostępu do repozytorium dokumentacji EDM.

Podstawowym założeniem Projektu jest wdrożenie i użytkowanie przez podmiot leczniczy (Zamawiającego) - Partnera w Projekcie ZeZ dwóch repozytoriów: lokalnego i regionalnego.

1. Repozytorium lokalne EDM (LREDM) – jest to repozytorium podstawowe - *primary*.
   Założenia:
   - repozytorium jest wdrożone i użytkowane w systemie dziedzinowym HIS lokalnym;
   - repozytorium lokalne zasilane jest na bieżąco danymi - dokumentami EDM z systemów dziedzinowych: HIS, LIS, PACS/RIS i innych wymaganych w przyszłości, w zależności od listy definiowanych przez resort zdrowia dokumentów EDM;
   - użytkowanie repozytorium wymaga alokowania lokalnych zasobów obliczeniowych: serwer bazy danych, macierz dyskowa, oraz dla bezpieczeństwa danych system archiwizacji i backupu;
   - możliwe są również – jednak nie implementowane w chwili obecnej w Projekcie ZeZ – rozwiązania typu IaaS lub PaaS.
2. Repozytorium regionalne EDM (RREDM) – jest to repozytorium - *secondary*.
   Założenia:
   - repozytorium to jest zasilane danymi z repozytorium lokalnego w trybie replikacji on-line;

- wdrożenie i użytkowanie repozytorium w oparciu o zasoby infrastrukturalne dostępne w warstwie regionalnej.

3. Kluczowe założenia architektury:
   - repozytorium lokalne nie bierze udziału w wymianie dokumentów EDM z P1;
   - wymiana oraz udostępnianie dokumentacji EDM z innymi podmiotami leczniczymi jak również jej udostępnianie odbywa się jedynie z wykorzystaniem Repozytorium regionalnego - zasobów warstwy regionalnej, przy czym dostęp do własnej dokumentacji pacjent uzyska jedynie poprzez IKP (w przyszłości);
   - rozwiązanie gwarantuje zwiększony poziom dostępności dokumentacji EDM, zwiększoną odporność systemu na awarie;
   - podmiot leczniczy jest właścicielem dokumentacji EDM (kustoszem w rozumieniu Dokumentacji integracyjnej EDM wydanej CeZ) – rozwiązanie gwarantuje możliwość ew. przyszłej migracji repozytorium do planowanej chmury publicznej lub innego systemu bez utraty integralności danych.

Uwaga: W zależności od przyjętego przez wykonawcę Rozwiązania w Warstwie Regionalnej, możliwa jest zmiana funkcjonalności w odniesieniu do zadań lokalnego REDM oraz regionalnego REDM (nie wyklucza możliwości przełączenia i wskazania jako Document Repository w rejestrze EDM P1 repozytorium lokalnego Partnera Projektu).

Szczegółowe założenia oraz sposób implementacji rozwiązania wdrożonego lokalnie systemu oprogramowania dziedzinowego z warstwą regionalną, w tym integracja repozytorium lokalnego oraz regionalnego) zawiera *Dokumentacja integracyjna oprogramowania warstwy lokalnej z warstwą regionalną*. Wymagana minimalna zawartość dokumentacji:

1. Architektura systemu
   1.1. Założenia w zakresie udostępniania i wymiany EDM – koncepcja
      - zakres i format wymienianej dokumentacji medycznej,
      - zakres metadanych wykorzystywanych do wyszukiwania wymienianych dokumentów,
      - zasady bezpieczeństwa i poufności wymiany dokumentów medycznych,
      - standardy komunikacji,
      - niezbędne wymagania infrastrukturalne.
   1.2. Opis architektury logicznej odzwierciedlającej poszczególne zasoby pomiędzy strukturami integrowanych obszarów
   1.3. Punkty dostępowe do każdego z podsystemu przypisanej struktury
   1.4. Opisanie możliwych wyników odpowiedzi wraz z ich znaczeniem i możliwym scenariuszem
   1.5. Opis mechanizmów dot. interwalów czasowych zasilania w dane wraz ze scenariuszami zapasowymi
   1.6. Opis możliwych interfejsów wraz z określeniem możliwych scenariuszy użycia
   1.7. Wskazanie modeli transakcji i opisanie poszczególnych typów
   1.8. Obiekty używane w transakcjach i ich znaczenie
   1.9. Struktura domen XDS w projekcie
2. Warstwy i komponenty warstwy regionalnej
   2.1. Regionalne repozytorium dokumentów medycznych
   2.2. Walidator dokumentów
   2.3. Komponent administracyjny
   2.4. Regionalne repozytorium zdarzeń na potrzeby audytu
3. Zasady przynależności podmiotów leczniczych do repozytorium regionalnego

3.1. Procedura nadawania uprawnień dostępu do repozytorium
3.2. Przebieg procedury nadawania uprawnień dostępu

4. Podstawowe operacje
4.1. Rejestracja repozytorium podmiotu leczniczego
4.2. Rejestracja danych dostępowych repozytorium podmiotu leczniczego
4.3. Przekazywanie dokumentów medycznych do repozytorium i ich rejestracja w P1
4.4. Wyszukiwanie dokumentów w rejestrze dokumentów P1 i ich pobieranie z repozytorium regionalnego

5. Zasady operacyjne
5.1. Zasady aktualizacji i udostępniania nowej wersji systemu
5.2. Zasady przechowywania i retencji danych oraz logów
5.3. Zasady postępowania w przypadku niedostępności systemu
5.4. Odtwarzanie po awarii

6. Diagramy przepływu danych oraz transakcji/komunikacji

Wykonawca warstwy regionalnej zobowiązany jest do przygotowania a następnie udostępnienia ww. Dokumentacji integracyjnej. Po wyłonieniu wykonawcy Warstwy Regionalnej zostanie ona przekazana Wykonawcy Przedmiotu Zamówienia. Planowane jest aby wykonawca Warstwy Regionalnej przygotował dokumentację integracyjna w ciągu 3 miesięcy od podpisania umowy.

Wykonawca musi zagwarantować gotowość wdrażanego Systemu do integracji z Warstwą Regionalną o architekturze oraz regułach biznesowych opisanych w OPZ.

Rozdział III. Gwarancja

Wykonawca musi skalkulować w oferowanej cenie: koszt licencji, wsparcie techniczne wraz z aktualizacjami, serwisem SSI, konserwacjami, konsultacjami(gwarancję), koszt wdrożenia, koszt nadzoru autorskiego.

III.1.1 Okres gwarancji

1. Wykonawca w ramach realizacji Przedmiotu Zamówienia udzieli Zamawiającemu gwarancji jakości (dalej zwanej „gwarancją") na niniejszy Przedmiot Zamówienia:

a) Modernizacja sieci teleinformatycznej i serwerowni w zakresie:

Poz. OPZ	Opis**	Okres gwarancji (minimalny)*
Rozdział II.1	**Modernizacja sieci teleinformatycznej**	
II.1.1	Poprawa stanu technicznego Serwerowni	60 miesięcy
II.1.2	Urządzenie zabezpieczające UTM	60 miesięcy

b) Infrastruktura serwerowa w zakresie:

Poz. OPZ	Opis**	Okres gwarancji (minimalny)*
Rozdział II.2	**Infrastruktura serwerowa i sieciowa**	
II.2.1	Pamięć masowa NAS	60 miesięcy

c) Oprogramowanie systemowe i narzędziowe w zakresie:

POZ. OPZ	Opis**	Okres gwarancji (minimalny)*
ROZDZIAŁ II.3	**OPROGRAMOWANIE SYSTEMOWE I NARZĘDZIOWE**	
II.3.1	Serwerowy system operacyjny	----------
II.4.1	Oprogramowanie antywirusowe	60 miesięcy

* W czasie obowiązywania gwarancji Wykonawca zobowiązany jest do udostępnienia Zamawiającemu nowych wersji BIOS, firmware i sterowników (na płytach CD lub stronach internetowych).
** W przypadku awarii nośników pozostają one własnością Zamawiającego.

d) dostawa i wdrożenie Szpitalnego Systemu Informatycznego:

Poz. OPZ	Opis	Okres gwarancji i nadzoru autorskiego (minimalny)
II.5	Szpitalny System Informatyczny	60 miesięcy

e) Opcjonalny zakres zamówienia:

Poz. OPZ	Opis	Okres gwarancji i nadzoru autorskiego (minimalny)
II.6	Integracja Warstwy Lokalnej z Repozytorium Regionalnym EDM	60- miesięcy

2. Bieg terminów gwarancji określonych w ust. 1 będzie rozpoczynać się z dniem podpisania Protokołu Odbioru danego Etapu, a w przypadku Etapu 3 od podpisania Protokołu Odbioru Końcowego bez uwag przez Zamawiającego.
3. Naprawy gwarancyjne muszą być realizowane przez serwis producenta lub Autoryzowanego Partnera Serwisowego Producenta.

III.1.2 Zakres gwarancji i nadzoru autorskiego dostarczonego Oprogramowania aplikacyjnego

Nazwa	Opis
Serwis SSI	1. W okresie gwarancji Wykonawca będzie zobowiązany do nieodpłatnego usuwania Wad Przedmiotu Zamówienia rozumianych jako Błąd, Awaria lub Usterka zgodnie z definicjami wskazanymi w Słowniku. 2. Przyjęcie zgłoszenia Wady przez Wykonawcę, odbywać się będzie poprzez dostępny on-line System Zgłaszania i przyjmowania uwag oraz Wad (dalej zwany Systemem Zgłoszeń lub SZ) przy czym:

	1) System Zgłoszeń dostarczy Wykonawca (będzie on utrzymywany i administrowany przez Wykonawcę), wpisu zgłoszenia do SZ będzie dokonywał Zamawiający, 2) za skuteczne przyjęcie zgłoszenia Wady uważać się będzie wprowadzenie przez Zamawiającego wpisu do SZ zawierającego opis zgłaszanej Wady i termin jej zgłoszenia; w razie trudności z dostępem on-line do SZ, zgłoszenia Wady mogą odbywać się także telefonicznie pod ustalonym numerem telefonu lub pisemnie na formularzu przesyłanym na ustalony adres e-mail, opcjonalnie faksem, których numery i adresy zostaną podane przez Wykonawcę w terminie 15 dni roboczych od dnia podpisania Umowy wraz ze wzorem formularza zgłoszenia Wady. 3. W przypadku, w którym wykonanie Umowy związane będzie z modernizacją lub rozbudową istniejącego oprogramowania (niniejszy OPZ zawiera dla aplikacji specyfikację funkcjonalną), gwarancja obejmuje całość oprogramowania modernizowanego lub rozbudowywanego.
Konserwacja	1. Realizacja Przedmiotu Zamówienia zapewni Zamawiającemu poprawę jakości oraz poszerzenie zakresu funkcjonalnego Oprogramowania aplikacyjnego, jak również dostosowanie tego oprogramowania do zmian czynników wewnętrznych organizacji Zamawiającego oraz zewnętrznych, będących efektem nowelizacji uwarunkowań prawnych. 2. W ramach Konserwacji Wykonawca zagwarantuje: 1) prowadzenie rejestru zgłaszanych przez Użytkowników błędów i wad ww. Oprogramowania aplikacyjnego 2) wprowadzanie do ww. Oprogramowania aplikacyjnego nowych funkcji oraz usprawnień już istniejących, stanowiących wynik prac rozwojowych producenta, 3) wprowadzanie do ww. Oprogramowania aplikacyjnego zmian stanowiących konsekwencję wejścia w życie nowych aktów prawnych lub aktów prawnych zmieniających obowiązujący stan prawny, opublikowanych w postaci ustaw, rozporządzeń, itp. 4) wprowadzanie do oprogramowania aplikacyjnego zmian wymaganych przez wyszczególnione poniżej podmioty, w stosunku do których Zamawiający ma obowiązek prowadzenia sprawozdawczości, w szczególności: a) Ministerstwa Zdrowia, b) NFZ, c) Centrów Zdrowia Publicznego. 5) wprowadzanie w trybie pilnym do ww. Oprogramowania aplikacyjnego zmian i poprawek usuwających stwierdzone błędy i luki we wbudowanych mechanizmach i funkcjach zabezpieczeń, 6) gotowość do odpłatnego wykonania na zlecenie Zamawiającego zaproponowanych przez niego modyfikacji ww. Oprogramowania aplikacyjnego.
Konsultacje	Świadczenie Zamawiającemu usługi pomocy technicznej i eksploatacyjnej w odniesieniu do ww. Oprogramowania aplikacyjnego, w dni robocze w godzinach od 8.00 do 15.00 w języku polskim.

III.1.3 Reżimy realizacji serwisu

W okresie gwarancji Wykonawca będzie zobowiązany do nieodpłatnego usuwania Wad Przedmiotu Zamówienia (dotyczy infrastruktury sieci teleinformatycznej, infrastruktury serwerowej oraz sieciowej) rozumianych jako Awaria lub Błąd lub Usterka zgodnie z definicjami, jak poniżej:

1) **Awaria w Infrastrukturze -** Kategoria Wady w Infrastrukturze Sprzętowej powodująca brak działania lub niepoprawne działanie Przedmiotu Zamówienia u Zamawiającego, uniemożliwiająca jego użytkowanie. Sytuacja, w której Sprzęt w ogóle nie funkcjonuje lub nie jest możliwe realizowanie istotnych funkcjonalności Komponentów/Produktów Przedmiotu Zamówienia,

2) **Usterka w Infrastrukturze-** Należy przez to rozumieć kategorię Wady w Infrastrukturze Sprzętowej oznaczającą funkcjonowanie niezgodne z Dokumentacją, SWZ, Umową lub OPZ, nie wpływającą istotnie na funkcjonowanie dostarczanego rozwiązania u Zamawiającego, utrudniającą pracę Użytkownikowi Zamawiającego.

Tabela 1. Gwarancja dla Infrastruktury modernizacji pomieszczenia serwerowni:

KWALIFIKACJA ZGŁOSZENIA WADY	OKRES DOSTĘPNOŚCI WYKONAWCY	ROZWIĄZANIE ZASTĘPCZE	CZAS REAKCJI WYKONAWCY	CZAS NAPRAWY
AWARIA	24/7/365	niezwłocznie, nie później niż 12 godzin od czasu przyjęcia zgłoszenia	niezwłocznie, nie później niż 4 godziny od czasu przyjęcia zgłoszenia	niezwłocznie, nie później niż 24 godziny od czasu przyjęcia zgłoszenia
USTERKA	24/7/365	----------	niezwłocznie, nie później niż 24 godziny od czasu przyjęcia zgłoszenia	niezwłocznie, nie później niż 7 dni od czasu przyjęcia zgłoszenia

1) Poprawa techniczna Serwerowni:

Tabela 2. Gwarancja dla Infrastruktury serwerowej:

KWALIFIKACJA ZGŁOSZENIA WADY	OKRES DOSTĘPNOŚCI WYKONAWCY	ROZWIĄZANIE ZASTĘPCZE	CZAS REAKCJI WYKONAWCY	CZAS NAPRAWY
AWARIA	24/7/365	niezwłocznie, nie później niż 12 godzin od czasu przyjęcia zgłoszenia	niezwłocznie, nie później niż 4 godziny od czasu przyjęcia zgłoszenia	niezwłocznie, nie później niż 24 godziny od czasu przyjęcia zgłoszenia
USTERKA	24/7/365	niezwłocznie, nie później niż 3 dni od czasu przyjęcia zgłoszenia	niezwłocznie, nie później niż 24 godziny od czasu przyjęcia zgłoszenia	niezwłocznie, nie później niż 8 dni od czasu przyjęcia zgłoszenia

1) Pamięć masowa NAS

Tabela 3. Gwarancja dla pozostałej Infrastruktury serwerowej i sieciowej (w tym przełączniki LAN i UTM-y):

KWALIFIKACJA ZGŁOSZENIA WADY	OKRES DOSTĘPNOŚCI WYKONAWCY	ROZWIĄZANIE ZASTĘPCZE	CZAS REAKCJI WYKONAWCY	CZAS NAPRAWY
AWARIA	24/7/365	niezwłocznie nie później niż 2 dni od dnia przyjęcia zgłoszenia	niezwłocznie, nie później niż 4 godziny od czasu przyjęcia zgłoszenia	niezwłocznie nie później niż 4 dni roboczych od dnia przyjęcia zgłoszenia
USTERKA	24/7/365	niezwłocznie nie później niż 3 dni roboczych od dnia przyjęcia zgłoszenia	niezwłocznie, nie później niż 24 godziny od czasu przyjęcia zgłoszenia	niezwłocznie nie później niż 8 dni roboczych od dnia przyjęcia zgłoszenia

Tabela 4. Gwarancja dla Szpitalnego Systemu Informatycznego:

KWALIFIKACJA ZGŁOSZENIA WADY	OKRES DOSTĘPNOŚCI WYKONAWCY	ROZWIĄZANIE ZASTĘPCZE	CZAS REAKCJI WYKONAWCY	CZAS NAPRAWY
AWARIA	24/7/365	W CZASIE NAPRAWY, dopuszczalne rozwiązanie umożliwiające przekwalifikowanie na Błąd	niezwłocznie, nie później niż 4 godzin od czasu przyjęcia zgłoszenia	niezwłocznie, nie później niż 24 godziny od czasu przyjęcia zgłoszenia
BŁĄD	W dni robocze pomiędzy 8 a 16 Zgłoszenie przesłane po 16 traktowane jest jak zgłoszenie przyjęte w następnym dniu roboczym o 8.00	W CZASIE NAPRAWY, dopuszczalne rozwiązanie umożliwiające przekwalifikowanie na Usterkę	niezwłocznie nie później niż 24 godziny od czasu przyjęcia zgłoszenia	niezwłocznie nie później niż 10 dni roboczych od dnia przyjęcia zgłoszenia
USTERKA	W dni robocze pomiędzy 8 a 16	nie dotyczy	niezwłocznie nie później niż 5 dni	niezwłocznie nie później niż

KWALIFIKACJA ZGŁOSZENIA WADY	OKRES DOSTĘPNOŚCI WYKONAWCY	ROZWIĄZANIE ZASTĘPCZE	CZAS REAKCJI WYKONAWCY	CZAS NAPRAWY
	Zgłoszenie przesłane po 16 traktowane jest jak zgłoszenie przyjęte w następnym dniu roboczym o 8		roboczych od dnia przyjęcia zgłoszenia	30 dni roboczych od dnia przyjęcia zgłoszenia

1. Dopuszcza się zmianę kwalifikacji zgłoszenia Wady, po uprzedniej zgodzie Zamawiającego. Do czasu potwierdzenia zmiany kwalifikacji, uznaje się za obowiązującą kwalifikację pierwotną.
2. Czasy naprawy mogą być inne niż wskazane w powyższych tabelach, jeżeli Zamawiający zaakceptuje zmianę kwalifikacji zgłoszenia, o której mowa w ust. 1 powyżej.
3. W przypadku braku możliwości usunięcia Wady lub przedstawienia rozwiązania zastępczego zdalnie, Wykonawca zobowiązany jest do świadczenia gwarancji bezpośrednio w lokalizacji Zamawiającego.
4. Usunięcie Wady Oprogramowania, nastąpi poprzez przekazanie poprawki lub nowej wersji. Każda nowa poprawka lub nowa wersja musi posiadać unikalny numer.
5. System informatyczny w obszarze e-usług musi spełniać wymagania Web Content Accessibility Guidelines (WCAG 2.0), z uwzględnieniem poziomu AA, określonych w załączniku pn. „Wytyczne dla dostępności treści internetowych 2.1 stosowane dla stron internetowych i aplikacji mobilnych w zakresie dostępności dla osób niepełnosprawnych” do ustawy z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych (Dz.U. z 2019 r. poz. 848 ze zm.).
6. Wykonawca w okresie trwania gwarancji, do 5 (piątego) dnia każdego miesiąca, przedstawi Zamawiającemu raport zawierający co najmniej: numer zgłoszenia, kwalifikację zgłoszenia, godzinę i datę zgłoszenia, temat zgłoszenia, status zgłoszenia, godzinę i datę usunięcia Wady, czas naprawy, czas wykonywania Serwisu Oprogramowania.

III.1.4 Pozostałe ustalenia

1. System Zgłoszeń, który zostanie udostępniony przez Wykonawcę, musi dodatkowo pozwalać na prowadzenie rejestru kontaktów z Zamawiającym obejmującego w szczególności wykonane czynności gwarancyjne, ewidencję wszystkich zgłoszeń gwarancyjnych, opis zmian w konfiguracji Oprogramowania. Prowadzenie rejestru zgłoszeń jest obowiązkiem Wykonawcy.
2. Zamawiający przekaże Wykonawcy, zgodnie ze stanem swojej wiedzy, informacje o aktach prawa wewnętrznego obowiązującego u Zamawiającego, które mają zastosowanie w realizacji niniejszej Umowy.
3. Gwarancja i serwis na urządzenia muszą być świadczone przez firmę autoryzowaną przez producenta w przypadku, gdy Wykonawca nie posiada takiej autoryzacji.
4. Zamawiający ustala procedurę zdalnego dostępu Wykonawcy do Oprogramowania:
   1) Wykonawca drogą elektroniczną poprzez e-mail, prześle Zamawiającemu wniosek o uzyskanie zdalnego dostępu do Oprogramowania, wskazując co najmniej:
      a) imię i nazwisko pracownika Wykonawcy, któremu zostanie przyznany dostęp,

b) nazwa i adres IP zasobu (bazy danych/oprogramowania), który zostanie udostępniony,

c) usługi sieciowe, które zostaną udostępnione,

d) okres , na który będzie aktywowany dostęp,

e) numer zgłoszenia gwarancyjnego,

f) przyczyna złożenia wniosku,

g) opis czynności, które zostaną wykonane,

h) imię i nazwisko pracownika Wykonawcy uprawnionego do złożenia wniosku.

2) Osoba wyznaczona przez Zamawiającego zaopiniuje wniosek i w formie elektronicznej poprzez e-mail odpowie, podając informację o zgodzie lub jej braku.

3) Po zakończeniu prac Wykonawca ma obowiązek przesłać Zamawiającemu raport z wykonanych prac z wykorzystaniem zdalnego dostępu, podając czas ich trwania i zakres.

4) Każdy zdalny dostęp do Oprogramowania musi być przez Wykonawcę odnotowany w Systemie Zgłoszeń.

5) Dostęp do zasobów Zamawiającego musi być zgodny z obowiązującą u niego polityką bezpieczeństwa. Zamawiający udostępni procedury bezpieczeństwa Wykonawcy, którego oferta zostanie wybrana jako najkorzystniejsza, po podpisaniu Umowy.

6) W przypadku dostarczenia nowej lub zmodyfikowanej wersji Oprogramowania wymagającego aktualizacji lub wymiany Oprogramowania dostarczonego w ramach Przedmiotu Zamówienia, Wykonawca w ramach gwarancji ma obowiązek wymiany lub aktualizacji także tego Oprogramowania.

5. W ramach gwarancji Wykonawca zobowiązuje się do:

1) wykonywania modyfikacji bez wezwania lub na pisemne zgłoszenie Zamawiającego w celu dostosowania wszystkich elementów Oprogramowania SSI do obowiązujących przepisów prawnych,

2) przekazywania Zamawiającemu informacji o nowych wersjach oprogramowania drogą elektroniczną na wskazany adres e-mail Zamawiającego,

3) udostępniania nowych wersji Oprogramowania poprzez ustaloną witrynę internetową, w szczególności związanych z wejściem w życie nowych przepisów prawa lub zawierających nowe funkcjonalności, w szczególności związane z rozliczeniami z NFZ; w przypadku w którym udostępnianie następować będzie w związku ze zmianą przepisów prawa, Wykonawca zobowiązany będzie do udostępnienia nowej wersji Oprogramowania na nie mniej niż 14 (czternaście) dni przed dniem wejścia w życie tych przepisów; udostępniania nowych wersji Oprogramowania poprzez ustaloną witrynę internetową, w szczególności związanych z wejściem w życie nowych przepisów prawa lub zawierających nowe funkcjonalności, w szczególności związane z rozliczeniami z NFZ; w przypadku, gdy przepisy te będą wchodziły w życie w terminie krótszym niż 14 dni od daty ich publikacji, Wykonawca jest zobowiązany do udostępnienia nowej wersji Oprogramowania niezwłocznie, w terminie nie później jak 3 (trzy) dni robocze od ich publikacji,

4) wysyłania na adres korespondencyjny Zamawiającego nośnika CD/DVD zawierającego nową wersję Oprogramowania, na pisemne żądanie wniesione przez Zamawiającego - każda nowa wersja musi posiadać unikalny numer,

5) wraz z nową wersją Oprogramowania Wykonawca zobowiązany jest do przekazania nowej wersji Dokumentacji wraz z procedurą instalacji Oprogramowania oraz informacją o parametryzacji i konfiguracji,

6) udzielanie konsultacji, porad, dodatkowej konfiguracji, tworzenia nowych raportów, wsparcia technicznego w zakresie wdrożenia oraz użytkowania oprogramowania SSI, przy czym:

   a) prace będą świadczone w dni robocze w godzinach od 8 do 16 w języku polskim, w siedzibie Zamawiającego lub za uzgodnieniem Stron, jako prace świadczone zdalnie,

   b) tryb zgłaszania: telefonicznie, e-mail, faxem lub poprzez System Zgłoszeń; konsultacje i porady będą udzielane na bieżąco podczas rozmowy telefonicznej lub w postaci elektronicznej, jednak nie później niż w ciągu 3 (trzech) dni roboczych od skierowania zapytania. Jeżeli nie jest możliwe wykonanie zadania w ciągu 3 (trzech) dni roboczych, Wykonawca uzgodni z Zamawiającym inny termin konsultacji lub porady, jeżeli Zamawiający wyrazi na to zgodę.

Uwaga:

W przypadku zapisu terminu, jako:

1) dzień roboczy należy rozumieć każdy dzień od poniedziałku do piątku z wyłączeniem dni ustawowo wolnych od pracy,

2) godziny robocze należy rozumieć godziny od 8.00 do 15.00 w każdym Dniu Roboczym.

W innych przypadkach „dzień” należy rozumieć jako dzień kalendarzowy.