## **Załącznik nr 2 do SWZ - OPIS PRZEDMIOTU ZAMÓWIENIA**

## Tytuł projektu

Usprawnienie funkcjonowania i poprawa jakości opieki medycznej w Samodzielnym Publicznym Zakładzie Opieki Zdrowotnej w Słupcy poprzez transformację cyfrową systemów informatycznych, zakup sprzętu informatycznego oraz wdrożenie rozwiązań w zakresie cyberbezpieczeństwa.

## Opis projektu:

Projekt zakłada kompleksową transformację cyfrową Samodzielnego Publicznego Zakładu Opieki Zdrowotnej w Słupcy, obejmującą integrację i rozbudowę systemów informatycznych, digitalizację dokumentacji medycznej, podniesienie poziomu cyberbezpieczeństwa oraz wdrożenie rozwiązań opartych na sztucznej inteligencji i integrację z krajowymi repozytoriami danych medycznych.

## Cele szczegółowe w projekcie:

1. Integracja i rozbudowa systemów informatycznych świadczeniodawcy (wskaźniki D21G, D21G.R1)

W ramach tego komponentu planowana jest rozbudowa systemu HIS Eskulap o dodatkowe moduły, umożliwiające rozszerzenie katalogu Elektronicznej Dokumentacji Medycznej (EDM). Celem jest zwiększenie ilości dokumentów generowanych w postaci cyfrowej i gotowych do przesyłania do Platformy P1. Jednocześnie zakupione zostanie rozwiązanie integracyjne zgodne ze standardem HL7, umożliwiające pełną interoperacyjność i płynną komunikację między systemami dziedzinowymi a systemem HIS. Działanie to znacząco usprawni zarządzanie EDM i jej indeksowanie w P1. Wdrożeniu będą towarzyszyć szkolenia personelu medycznego i administracyjnego. Dodatkowo, projekt przewiduje zakup niezbędnej infrastruktury ICT: 4 serwerów z systemami operacyjnymi i wirtualizacją, macierzy dyskowej oraz przełączników sieciowych. Te działania stworzą stabilne i bezpieczne środowisko informatyczne.

1. Digitalizacja dokumentacji medycznej istotnej z punktu widzenia leczenia i profilaktyki (wskaźniki D18G, D18G.R1)

Projekt obejmuje również działania związane z digitalizacją dokumentacji medycznej w celu zasilenia Platformy P1 wymaganymi dokumentami. Dotyczy to w szczególności kart informacyjnych z leczenia szpitalnego. Dzięki wdrożeniu odpowiednich narzędzi do konwersji dokumentacji papierowej i jej przesyłania do P1, szpital będzie mógł osiągnąć wskaźnik zaindeksowania 95% kart w centralnym repozytorium. Realizacja tego celu przyczyni się do poprawy ciągłości opieki nad pacjentem, dostępności danych medycznych dla innych świadczeniodawców i lepszego zarządzania informacją medyczną.

1. Działania zwiększające poziom cyberbezpieczeństwa szpitala (wskaźnik D21G.R2)

W odpowiedzi na rosnące zagrożenia cybernetyczne, projekt przewiduje modernizację kluczowych elementów infrastruktury bezpieczeństwa: systemu kopii zapasowych, zapory sieciowej, urządzeń brzegowych oraz oprogramowania poczty e-mail. Ponadto, planowana jest rozbudowa platformy XDR (Extended Detection and Response), pozwalającej na szybką detekcję i reakcję na incydenty bezpieczeństwa. Kompleksowe działania obejmą również przeprowadzenie końcowego audytu cyberbezpieczeństwa oraz szkolenia dla kadry kierowniczej, personelu medycznego i administracyjnego w zakresie świadomości zagrożeń i bezpiecznego korzystania z systemów informatycznych. Celem jest osiągnięcie wskaźników zgodnych z wymaganiami audytu i podniesienie poziomu odporności placówki na incydenty cybernetyczne.

1. Wdrożenie rozwiązań AI i podłączenie do centralnego repozytorium danych medycznych (wskaźnik D21G.R3)

Projekt przewiduje również integrację z Platformą Udostępniania Obrazów (PUI) i wdrożenie rozwiązań opartych na sztucznej inteligencji (np. w środowisku Eskulap NG). Dzięki integracji z systemem do prowadzenia dokumentacji obrazowej, możliwe będzie przesyłanie danych do PUI, co umożliwi ich współdzielenie z innymi jednostkami ochrony zdrowia. Rozwiązania te poszerzają zakres działalności diagnostycznej szpitala oraz umożliwiają wykorzystanie AI w analizie danych obrazowych, wspierając proces diagnostyczny.

Wdrożone narzędzia będą objęte serwisem w całym okresie trwałości projektu.

## Zakres przedmiotu zamówienia

1. INTEGRACJA I ROZBUDOWA SYSTEMÓW INFORMATYCZNYCH ŚWIADCZENIODAWCY

W ramach zadania zostanie przeprowadzona rozbudowa istniejącego systemu HIS Eskulap (Hospital Information System) o nowe moduły oprogramowania umożliwiające rozszerzenie katalogu Elektronicznej Dokumentacji Medycznej (EDM). Dodatkowe dokumenty będą tworzone i przetwarzane zgodnie ze standardem PIK HL7 CDA, co zapewni ich pełną interoperacyjność z Platformą P1 oraz centralnymi rejestrami medycznymi. Nowe typy EDM objęte rozbudową to:

* karta Diagnostyki i Leczenia Onkologicznego (e-DILO),
* opisy badań histopatologicznych i cytologicznych,
* plan leczenia onkologicznego,
* PatientSummary (e-Karta zdrowia pacjenta),
* dokumenty medycyny pracy (orzeczenia lekarskie oraz wytyczne związane z warunkami pracy),
* karta medycznych czynności ratunkowych (KMCR),
* karta medyczna lotniczego zespołu ratownictwa medycznego,
* elektroniczna karta opieki kardiologicznej.

Rozszerzenie funkcjonalności HIS pozwoli na prowadzenie i automatyczne indeksowanie szerszego zakresu dokumentacji medycznej w formie cyfrowej, co znacząco zwiększy jakość, szybkość oraz kompletność wymiany informacji medycznych między świadczeniodawcami. Ważnym komponentem zadania będzie zakup i wdrożenie oprogramowania integracyjnego zgodnego z protokołem HL7. Dzięki temu zapewniony zostanie płynny przepływ danych pomiędzy systemami dziedzinowymi i systemem HIS oraz możliwość ich bezproblemowego przesyłania do platformy P1. Wdrożone zostaną także moduły komunikujące się z rejestrami centralnymi (np. e-ZLA, e-skierowania, e-recepty), co umożliwi dalszą automatyzację procesów i poprawi efektywność pracy personelu medycznego.

Zadanie obejmuje również techniczne wzmocnienie infrastruktury IT placówki. Zostaną zakupione nowoczesne serwery wraz z systemami operacyjnymi i platformami wirtualizacyjnymi, a także macierze dyskowe i przełączniki sieciowe. Inwestycja ta umożliwi utworzenie stabilnego, wydajnego i odpornego środowiska teleinformatycznego, które zagwarantuje ciągłość działania systemów, szybki dostęp do danych oraz minimalizację ryzyka przestojów i utraty informacji. Rozbudowa systemu informatycznego HIS Eskulap uwzględni również aktualizację silnika baz danych, niezbędną do prawidłowego działania systemu i zapewnienia jego zgodności z nowoczesnymi wymaganiami dotyczącymi przetwarzania i przechowywania danych medycznych. Wszystkie wdrażane rozwiązania będą objęte wsparciem serwisowym w całym okresie trwałości projektu, co zagwarantuje ich stabilność i bezpieczeństwo.

1. DIGITALIZACJA DOKUMENTACJI MEDYCZNEJ ISTOTNEJ Z PUNKTU WIDZENIA LECZENIA I PROFILAKTYKI

W ramach zadania zostaną wdrożone kompleksowe rozwiązania umożliwiające digitalizację dokumentacji medycznej oraz zasilenie systemu P1 zgodnie z obowiązującymi wymaganiami Ministerstwa Zdrowia i Centrum e-Zdrowia.

Kluczowym elementem będzie zakup oraz wdrożenie specjalistycznego modułu integracyjnego, pozwalającego na współpracę z nowym centralnym repozytorium danych medycznych (CEZ). Moduł ten będzie wyposażony w funkcjonalności umożliwiające przetwarzanie, obróbkę i wysyłkę zeskanowanej dokumentacji medycznej (np. kart informacyjnych z leczenia szpitalnego, wyników badań, epikryz). Dokumenty te będą przesyłane w formacie zgodnym z wymogami Elektronicznej Dokumentacji Medycznej (EDM) do systemu P1. Dodatkowo, uruchomione zostaną narzędzia wspierające zbiorczą rejestrację i ponowne zaindeksowanie kart informacyjnych dotyczących hospitalizacji z lat 2023–2025. Narzędzia te będą działały niezależnie od aktualnego stanu informatyzacji dokumentacji w placówce, co umożliwi pełne włączenie danych archiwalnychdo krajowego systemu e-zdrowia. W ramach zadania zostanie również zakupiony i wdrożony dodatkowy moduł integracyjny, umożliwiający konwersję oraz transmisję do systemu P1 zdarzeń medycznych pochodzących z systemów diagnostycznych LIS (Laboratory Information System), RIS (Radiology Information System) oraz HISTO (systemy patomorfologiczne) – niezależnie od ich dostawcy. Pozwoli to na efektywne włączenie danych medycznych pochodzących z różnych źródeł do jednolitego środowiska informacyjnego szpitala oraz ich bezpieczne i zgodne z przepisami przekazanie do Platformy P1.

1. DZIAŁANIA ZWIĘKSZAJĄCE POZIOM CYBERBEZPIECZEŃSTWA SZPITALA

W ramach zadania zaplanowano kompleksowe działania ukierunkowane na zwiększenie poziomu cyberbezpieczeństwa infrastruktury IT oraz danych medycznych. Projektowane rozwiązania są zgodne z wymogami Krajowych Ram Interoperacyjności (KRI) oraz Dyrektywy NIS2 i obejmują modernizację systemu kopii zapasowych, zapory sieciowej, oprogramowania poczty elektronicznej, wdrożenie platformy XDR, zapory WAF, systemu DLP oraz przeprowadzenie audytu końcowego. Modernizacja systemu kopii zapasowych realizowana będzie zgodnie z zasadą 3-2-1: tworzenie trzech kopii danych, na dwóch różnych nośnikach, z jedną kopią przechowywaną poza lokalizacją źródłową. Takie podejście zapewni odporność danych na cyberataki, awarie, uszkodzenia oraz błędy ludzkie. Działanie to odpowiada na wytyczne KRI §20 ust. 2 pkt 12b i 12c, gwarantujące ochronę przed utratą i nieuprawnioną modyfikacją informacji.

Modernizacja zapory sieciowej pozwoli na kontrolę ruchu sieciowego, ochronę przed atakami typu malware, phishing oraz nieautoryzowanym dostępem. Zabezpieczy również urządzenia mobilne personelu i zapewni zgodność z KRI §20 ust. 2 pkt 8 i 12c, w zakresie bezpiecznej pracy mobilnej i zdalnej. Modernizacja oprogramowania poczty elektronicznej umożliwi ochronę przed atakami brute-force, phishingiem i spyware. Wdrożone mechanizmy bezpieczeństwa spełnią wymagania KRI §20 ust. 2 pkt 9, zapewniając ochronę przed nieuprawnionym ujawnieniem, modyfikacją czy usunięciem informacji. Platforma XDR (Extended Detection and Response) umożliwi analizę zagrożeń z wielu źródeł – poczty, punktów końcowych, serwerów i sieci – oraz automatyczne reagowanie na incydenty. Rozwiązanie to wpisuje się w wymagania Dyrektywy NIS2 oraz KRI §20 ust. 2 pkt 7b i 7c dotyczące ochrony informacji przed kradzieżą, uszkodzeniem i zakłóceniami. Zapora sieciowa WAF zostanie wdrożona celem ochrony aplikacji internetowych przed złośliwym ruchem HTTP/ S, co zapobiega przestojom, utracie danych i naruszeniu prywatności pacjentów. Zabezpieczenie to wspiera wymagania NIS2 wobec operatorów aplikacji i usług krytycznych. System DLP (Data LossPrevention) umożliwi bieżące monitorowanie i analizę incydentów bezpieczeństwa, w tym wykrywanie nieautoryzowanego dostępu czy prób wycieku danych. Spełni to wymagania KRI §20 ust. 2 pkt 13 dotyczące nadzoru nad bezpieczeństwem danych. Zwieńczeniem działań będzie przeprowadzenie końcowego audytu cyberbezpieczeństwa. Audyt obejmie kluczowe obszary infrastruktury IT: pocztę, urządzenia brzegowe, kontrolery domeny, systemy backupu, konfigurację stacji roboczych, uwierzytelnianie oraz systemy zarządzania IT. Audyt umożliwi weryfikację skuteczności wdrożonych rozwiązań i potwierdzi osiągnięcie wymaganych standardów bezpieczeństwa.

1. WDROŻENIE ROZWIĄZAŃ AI I PODŁĄCZENIE DO CENTRALNEGO REPOZYTORIUM DANYCH MEDYCZNYCH

W ramach realizacji zadania zostanie zakupiony i wdrożony moduł umożliwiający pełną integrację z Platformą Usług Inteligentnych (PUI), wspierającą obieg badań obrazowych i wyników analizy AI. Rozwiązanie to pozwoli na przesyłanie badań obrazowych (RTG, TK) bezpośrednio z systemu szpitalnego PACS/RIS do PUI, a następnie odbiór zinterpretowanych wyników analizowanych z wykorzystaniem algorytmów sztucznej inteligencji. Wdrożenie modułu integracyjnego umożliwi wysyłkę co najmniej jednego badania obrazowego do PUI, co spełni wymogi wskaźnika D21G.R3 w ramach Krajowego Planu Odbudowy i Zwiększania Odporności. Integracja zostanie zrealizowana w środowisku Eskulap NG, co zapewni pełną kompatybilność z obecnym systemem dokumentacji obrazowej i umożliwi zautomatyzowaną wymianę danych z PUI. Zastosowanie AI w analizie badań obrazowych zwiększy trafność diagnoz, skróci czas oczekiwania na wyniki oraz umożliwi szybsze podjęcie decyzji klinicznych. Algorytmy będą wspierać lekarzy w wykrywaniu zmian patologicznych, klasyfikacji obrazów oraz ocenie ryzyka pacjentów. Rozwiązania AI będą funkcjonować jako narzędzia wspomagające decyzje, nie zastępując lekarza, lecz wzmacniając jakość i bezpieczeństwo podejmowanych działań. Zadanie odpowiada na rosnące potrzeby w zakresie automatyzacji procesów diagnostycznych, cyfryzacji danych medycznych oraz interoperacyjności pomiędzy systemami placówki a krajowymi repozytoriami danych. Dzięki wdrożeniu, możliwe będzie również lepsze wykorzystanie danych medycznych w dalszej analizie statystycznej i zarządczej.

## Definicje pojęć

Strony zgodnie stwierdzają, że na potrzeby niniejszego OPZ i przyszłej Umowy dotyczącej opisanego zamówienia, wymienionym w niniejszym paragrafie pojęciom nadają znaczenie określone poniżej, oraz że użyte w tekście poniżej wymienione pojęcia, rozumiane będą w sposób poniżej zdefiniowany. Dla podkreślenia, że pojęcia te rozumiane są w sposób zdefiniowany, ich pierwsze litery będą pisane w tekście wielką literą.

Strony ustalają następujące definicje:

1. Strony – oznacza Zamawiającego i Wykonawcę.
2. Zamawiający - Samodzielny Publiczny Zakład Opieki Zdrowotnej w Słupcy z siedzibą przy ul. Traugutta 7 w Słupcy
3. Wykonawca – podmiot, który ubiega się o udzielenie zamówienia, złożył ofertę albo zawarł umowę w postępowaniu o udzielenie zamówienia publicznego prowadzonego na podstawie przepisów art. 2 ust. 1 pkt.1 ustawy z dnia 11 września 2019 roku Prawo zamówień publicznych (t.j. Dz.U. z 2024 r., poz.1320 z późn. zm.), zwanej dalej ustawą Pzp.
4. Projekt - projekt pod nazwą Usprawnienie funkcjonowania i poprawa jakości opieki medycznej w Samodzielnym Publicznym Zakładzie Opieki Zdrowotnej w Słupcy poprzez transformację cyfrową systemów informatycznych, zakup sprzętu informatycznego oraz wdrożenie rozwiązań w zakresie cyberbezpieczeństwa, na który składa się ogół zobowiązań Stron.
5. Siła Wyższa – zdarzenia i okoliczności nadzwyczajne, pochodzące z zewnątrz, niezależne od woli i intencji którejkolwiek ze stron, których następstw nie można było przewidzieć i im zapobiec mimo dochowania należytej staranności, w szczególności takie jak: wojna, zamieszki, rewolucja, strajk, trzęsienie ziemi, warunki atmosferyczne, pożary lub inne klęski żywiołowe, epidemia, pandemia, awaria prądu, zasilania, wybuchy lub wypadki transportowe.
6. Producent – podmiot zajmujący się tworzeniem, rozwijaniem i rozpowszechnianiem Aplikacji.
7. Oprogramowanie Aplikacyjne (zwane również Systemem lub Systeme, HIS) – wszelkie objęte świadczeniami wynikającymi z niniejszego Opisu Przedmiotu Zamówienia utwory w rozumieniu przepisów ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (tekst jedn.: Dz. U. z 2022 r., poz. 2509), w tym Moduły, ich Rozwinięcia i Uaktualnienia oraz Dokumentacja, jak również towarzyszące programy komputerowe.
8. Infrastruktura IT- dostarczana w ramach realizacji przedmiotu zamówienia infrastrukturaICT, szczegółowo opisana w niniejszym załączniku.
9. Gwarancja i Serwis Systemu– Oznacza całokształt świadczonych przez Wykonawcę usług (gwarancyjno-serwisowych) związanych z zapewnieniem poprawnej pracy składników będących przedmiotem zamówienia, szczegółowo określone w niniejszym dokumencie oraz w Umowie.
10. Gwarancja i Serwis Infrastruktury IT– Oznacza całokształt świadczonych przez Wykonawcę usług (gwarancyjno-serwisowych) związanych z zapewnieniem poprawnej pracy składników będących przedmiotem zamówienia, szczegółowo określone w niniejszym dokumencie oraz Umowie.
11. Aplikacja (Moduł) – wyodrębnione technicznie i funkcjonalnie programy opisane kodem źródłowym charakteryzujące się spójnym zakresem funkcjonalnym i zdefiniowaną strukturą danych, oraz technologią umożliwiającą pracę z wykorzystaniem przeglądarki internetowej, jako interfejsu użytkownika (o ile występuje), realizujące swoje funkcje w interakcji z innymi Modułami w oparciu o wspólny(e) serwer(y) aplikacji.
12. Licencja - tytuł prawny, w oparciu, o który Zamawiający będzie eksploatował Aplikacje dostarczone w ramach realizacji przedmiotu zamówienia.
13. Zadnie – element przedmiotu zamówienia, podlegający odbiorowi po wykonaniu wszystkich jego Etapów.
14. Etap - główny element części Zadania, stanowiący funkcjonalną całość, podlegająca odrębnym odbiorom.
15. Protokół Odbioru Zadania - protokół przygotowany przez Wykonawcę, będący potwierdzeniem przyjęcia przez Zamawiającego wykonanych przez Wykonawcę prac będących przedmiotem danego Zadania.
16. Protokół Odbioru Etapu – protokół przygotowany przez Wykonawcę, będący potwierdzeniem przyjęcia przez Zamawiającego wykonanych przez Wykonawcę prac będących Etapem Zadania.
17. Protokół Odbioru Końcowego - Protokół, który po podpisaniu bez zastrzeżeń przez Zamawiającego, stanowi potwierdzenie wykonania i odbioru Przedmiotu Zamówienia.
18. Protokół Dostawy - Protokół, w którym Zamawiający sprawdza ilości dostarczonego towaru i porównuje go ze stanem wykazanym w dokumentach towarzyszących dostawie.
19. Protokół Usterek - Protokół, w którym Zamawiający wskazuje zastrzeżenia co do zakresu i jakości wykonanych prac, które uniemożliwiają dokonanie odbioru wykonanych dostaw i prac.
20. Protokół Uzgodnień – dokument tworzony przez Wykonawcę i zatwierdzony przez Strony, na podstawie zapisu ze spotkania lub ustaleń zdalnych (mailowych, telefonicznych) z Zamawiającym. Dokument ten używany jest w trakcie prowadzenia analizy wymagań Zamawiającego i stanowi zobowiązanie obu Stron. Zamawiający zobowiązany jest, że wymagania zapisane w/w protokole nie zostaną zmienione, natomiast Wykonawca zobowiązany jest do realizacji zawartych w nim wymagań Zamawiającego. W przypadku zajścia konieczności wykonania zmian lub innych czynności niż te, które zostały opisane w Protokole Uzgodnień, należy utworzyć nowy Protokół Uzgodnień zawierający te zmiany. W Protokole Uzgodnień można zamieścić inne uzgodnienia, niezwiązane z wymaganiami projektu, tj. ustalenia organizacyjne
21. Motor bazy danych (MBD) – program komputerowy dedykowany do zarządzania bazami danych.
22. Baza danych – utworzone w wyniku eksploatacji Oprogramowania Aplikacyjnego dane Zamawiającego, przetwarzane w Motorze bazy danych.
23. Infrastruktura Zamawiającego – elementy systemu teleinformatycznego, z których obecnie korzysta Zamawiający takie jak m.in.: serwer, stacje robocze, sieć komputerowa, oprogramowanie systemowe (obejmujące także oprogramowanie wirtualizacyjne i programy towarzyszące) oraz infrastruktura serwerowa i oprogramowanie, które Zamawiający przewidział na potrzeby realizacji przedmiotu zamówienia.
24. Użytkownik – Osoba fizyczna posiadająca przyznane przez Zamawiającego dane identyfikacyjne umożliwiające uwierzytelnianie w Aplikacji/jach.
25. Błąd Aplikacji – powtarzalne działanie / zaniechanie, pojawiające się za każdym razem w tym samym miejscu w Module na różnych stacjach roboczych (terminalach) i prowadzące w każdym przypadku do otrzymywania nieprawidłowych wyników. Z zakresu definicji wyłącza się nieprawidłowe działanie lub brak działania Modułu powodowane przez następujące okoliczności:
26. zastosowanie / użycie Modułu w sposób niezgodny z przeznaczeniem,
27. zastosowanie / użycie Modułu w sposób niezgodny z Dokumentacją,
28. wprowadzenie przez Użytkownika nieprawidłowych danych,
29. użytkowanie Modułu na Infrastrukturze niespełniającej ogólnie przyjętych w branży norm technicznych oraz bezpieczeństwa,
30. użytkowanie Modułu, MBD lub oprogramowania systemowego na Infrastrukturze niespełniającej Minimalnych parametrów wydajnościowych bądź zaleceń Producenta Modułu, określonych dla serwerów lub wskazanej ilości stanowisk roboczych,
31. użytkowanie Motoru Bazy Danych lub oprogramowania systemowego na Infrastrukturze niespełniającej minimalnych parametrów bądź zaleceń producentów Motoru Bazy Danych lub oprogramowania systemowego, publikowanych dla wersji bazy danych lub oprogramowania systemowego, z którymi w danym momencie eksploatowany jest Moduł,
32. współpraca Modułu z Motorem Bazy Danych lub oprogramowaniem systemowym w wersjach niewspieranych przez ich producentów.
33. współpraca Modułu z Motorem Bazy Danych obciążonej innymi programami niż Oprogramowanie Aplikacyjne w szczególności dodatkowymi instancjami bazodanowymi lub funkcjami w bazach danych,
34. użytkowanie Motoru Bazy Danych lub oprogramowania systemowego na Infrastrukturze znajdującej się w pomieszczeniach z niesprawną lub niewydolną klimatyzacją lub urządzeniami utrzymującymi odpowiednią wilgotność powietrza,
35. użytkowanie Motoru Bazy Danych lub oprogramowania systemowego na Infrastrukturze znajdującej się w pomieszczeniach z niesprawną lub niewydolną instalacją elektryczną i zasilaniem elektrycznym,
36. uszkodzenia nośników danych,
37. działanie wirusa komputerowego,
38. wdrożenie Modułu wykonane w sposób wadliwy, z wyłączeniem sytuacji, w której wdrożenie było wykonywane przez Wykonawcę,
39. niewłaściwa parametryzacja Modułu lub oprogramowania systemowego i Motoru Bazy Danych, z którymi Moduł współpracuje, z wyłączeniem sytuacji, w której parametryzacja była wykonywana przez Wykonawcę,
40. wszelkie działania Zamawiającego lub osób trzecich polegające na modyfikacji Oprogramowania Aplikacyjnego, ingerencji w to Oprogramowanie, z naruszeniem warunków licencyjnych nałożonych na Zamawiającego postanowieniami Umowy lub zgodne z tymi warunkami, lecz przeprowadzone z wykorzystaniem narządzi nieudostępnionych przez Wykonawcę albo zapisanie danych w instancji bazy danych z którą współpracuje Oprogramowanie Aplikacyjne przez inne programy lub narzędzia,
41. wszelkie działania Zamawiającego lub osób trzecich ingerujące w programy, z którymi Oprogramowanie Aplikacyjne zostało zintegrowane w zakresie wywołującym skutki dla tej integracji (sterowniki laboratoryjne, interfejsy HL7, interfejsy DICOM, web service, inne),
42. niezainstalowanie przez Zamawiającego opublikowanych w serwisie Helpdesk Uaktualnień bądź obowiązkowych Rozwinięć Modułu,
43. brak zgłoszenia niepomyślnego wykonania aktualizacji Modułu i jego dalsza eksploatacja mimo pojawiania się informacji o błędach (dotyczy także logów),
44. niezastosowanie się Zamawiającego do zaleceń w zakresie eksploatacji Modułu lub jego
45. Uaktualnień bądź Rozwinięć opublikowanych przez Producenta Modułu,
46. użytkowanie Modułu z naruszeniem warunków licencyjnych nałożonych na Zamawiającego postanowieniami Umowy,
47. blokowanie funkcji Modułu przez inne oprogramowanie, np. programy antywirusowe,
48. działanie Siły Wyższej,

Szczególnymi rodzajami Błędów Aplikacji są Awarie oraz Usterki Programistyczne.

1. Awaria (błąd krytyczny) – krytyczny Błąd Aplikacji powodujący nieprawidłowość jej działania, która prowadzi do zatrzymania eksploatacji Aplikacji, utraty danych lub naruszenia ich spójności, w wyniku którego niemożliwe jest prowadzenie bieżącej działalności przy użyciu Oprogramowania Aplikacyjnego.
2. Usterka Programistyczna – Błąd Aplikacji, mimo identyfikacji którego Aplikacja nadal funkcjonuje, lecz jej eksploatacja jest uciążliwa, skomplikowana lub spowolniona, a usunięcie Błędu wymaga wykonania prac programistycznych.
3. Konsultacja – usługa świadczona przez Wykonawcę polegająca na udzielaniu Zamawiającemu wyjaśnień w kwestiach dotyczących Oprogramowania Aplikacyjnego.
4. Help Desk (HD) – serwis internetowy udostępniony przez Wykonawcę dedykowany do ewidencji i obsługi Zgłoszeń Serwisowych, udostępniania Uaktualnień Aplikacji, publikowania wymogów, informacji i procedur dotyczących Oprogramowania Aplikacyjnego, Infrastruktury IT oraz MBD.
5. Zgłoszenie Serwisowe (Zgłoszenie) – zaewidencjonowane w HD zdarzenie dotyczące Oprogramowania Aplikacyjnego lub MBD, implikujące wykonanie na rzecz Zamawiającego usługi informatycznej przez Wykonawcę na zasadach określonych w niniejszym dokumencie.
6. Użytkownik HD – zadeklarowana w Help Desk osoba fizyczna desygnowana przez Zamawiającego do bezpośredniej współpracy z Wykonawcą, w tym do dokonywania, ewidencji i edycji lub/i podglądu Zgłoszeń Serwisowych.
7. Administrator – Użytkownik, który odbył szkolenie z administracji pakietu Oprogramowania Aplikacyjnego objętego usługami uwzględnionymi w Umowie, który jest uprawniony ze Strony Zamawiającego do dokonywania Zgłoszeń Serwisowych w HD i nadawania uprawnień innym Użytkownikom HD.
8. Uaktualnienie (update) – wszelkie powszechnie udostępniane przez Producenta modyfikacje Oprogramowania Aplikacyjnego powodujące usunięcie wykrytych Błędów Aplikacji.
9. Rozwinięcie (upgrade) – wszelkie powszechnie udostępniane przez Producenta nowe wersje lub inne niż Uaktualnienie (update) modyfikacje Oprogramowania Aplikacyjnego, zmieniające dotychczasową funkcjonalność Oprogramowania Aplikacyjnego.
10. Obejście – udostępnione Zamawiającemu doraźne rozwiązanie mające na celu zminimalizowanie skutków Błędu Aplikacji, zanim zostanie całkowicie usunięty. Zastosowanie Obejścia jest zależne od woli Wykonawcy, a w wypadku jego wdrożenia przewidziane w niniejszym załączniku w punkcie: warunki brzegowe realizacji usług dla usunięcia poszczególnych Błędów Aplikacji zostają wydłużone o 50 %.
11. Czas Reakcji – okres liczony od zaewidencjonowania Zgłoszenia Serwisowego do zmiany jego statusu na zarejestrowane.
12. Czas Naprawy - czas pomiędzy Zgłoszeniem Serwisowym a usunięciem/rozwiązaniem przyczyny jego zgłoszenia.
13. Dokumentacja – towarzyszące Oprogramowaniu Aplikacyjnemu lub - odpowiednio jego Uaktualnieniom bądź Rozwinięciom, materiały zawierające opis charakterystyki oraz sposobu działania Modułu, w tym opis cech i parametrów funkcjonalnych oraz pozafunkcjonalnych niezależnie od formy ich wyrażenia oraz sposobu udostępnienia ZAMAWIAJĄCEMU.
14. Nośnik – fizyczny środek (materiał lub urządzenie) przechowujący lub przeznaczony do przechowywania w nim danych (ciągów symboli).
15. Serwis – Dział Wykonawcy/Producenta dedykowany do świadczenia Usług Serwisowych.
16. Dni robocze – dni tygodnia od poniedziałku do piątku, z wyłączeniem dni ustawowo wolnych od pracy.
17. Godziny Robocze – godziny od 08:00 do 16:00 w każdym Dniu Roboczym.
18. Zdalny dostęp – analogowe lub cyfrowe łącze wydajnej transmisji danych pomiędzy węzłem infrastruktury siedziby Wykonawcy, a węzłem infrastruktury zapewnianym przez Zamawiającego, umożliwiające realizować usługi serwisowe lub konfiguracyjne

## OGÓLNY OPIS PRZEDMIOTU ZAMÓWIENIA

Przedmiot zamówienia składa z następujących Zadań:

1. INTEGRACJA I ROZBUDOWA SYSTEMÓW INFORMATYCZNYCH ŚWIADCZENIODAWCY
2. DIGITALIZACJA DOKUMENTACJI MEDYCZNEJ ISTOTNEJ Z PUNKTU WIDZENIA LECZENIA I PROFILAKTYKI
3. DZIAŁANIA ZWIĘKSZAJĄCE POZIOM CYBERBEZPIECZEŃSTWA SZPITALA
4. WDROŻENIE ROZWIĄZAŃ AI I PODŁĄCZENIE DO CENTRALNEGO REPOZYTORIUM DANYCH MEDYCZNYCH

Wymienione elementy będą tworzyły cztery podstawowe zadania tworzące przedmiot zamówienia o nazwie**: Usprawnienie funkcjonowania i poprawa jakości opieki medycznej w Samodzielnym Publicznym Zakładzie Opieki Zdrowotnej w Słupcy poprzez transformację cyfrową systemów informatycznych, zakup sprzętu informatycznego oraz wdrożenie rozwiązań w zakresie cyberbezpieczeństwa.**

Jeżeli w przedmiocie zamówienia Zamawiający wskazuje markę bądź wskazane są znaki towarowe, patenty lub źródło pochodzenia (nazwa producentów lub urządzeń), postanowienia te należy odczytywać, jako określenie wymaganych cech funkcjonalnych i jakościowych, a Wykonawca ma każdorazowo prawo zastosowania rozwiązania nie gorszego niż te, które zostało zastosowane lub użyte przez Zamawiającego w niniejszym dokumencie. Wszelkie nazwy własne użyte w opisach przedmiotu zamówienia, określają wymagany standard, jakości towarów i usług. Dopuszcza się możliwość przedstawienia w ofercie rozwiązań równoważnych o walorach nie gorszych niż opisane w OPZ.

Za równoważne uznaje się rozwiązania, jak również elementy, materiały, urządzenia o właściwościach funkcjonalnych i jakościowych takich samych, które zostały określone w opisie przedmiotu zamówienia, lecz oznaczonych innym znakiem towarowym, patentem lub pochodzeniem. Przy czym istotne jest to, że produkt równoważny to produkt, który nie jest identyczny, tożsamy z produktem referencyjnym, ale posiada pewne, istotne dla Zamawiającego, zbliżone do produktu referencyjnego cechy i parametry.

Istotne dla Zamawiającego cechy i parametry, to takie, które pozwolą zachować wszystkim systemom, urządzeniom, wyrobom, parametry i cechy pozwalające przede wszystkim na prawidłową współpracę z innymi systemami i/lub urządzeniami i/lub wyrobami w sposób założony przez Zamawiającego oraz pozwalające przy tym uzyskać parametry nie gorsze od założonych w OPZ. Ciężar udowodnienia równoważności spoczywa na Wykonawcy.

## SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

1. INTEGRACJA I ROZBUDOWA SYSTEMÓW INFORMATYCZNYCH ZAMAWIAJĄCEGO
2. Termin realizacji Zadania

Wykonawca zobowiązuje się wykonać przedmiot Umowy od dnia podpisania umowy w terminach poszczególnych Etapów, które wynoszą:

Etap I – Opracowanie Analizy przedwdrożeniowej – do 15 dni kalendarzowych od daty zawarcia Umowy

Etap II – Dostawa licencji Systemu HIS - do 30 dni kalendarzowych od daty wykonania Etapu I

Etap III - Wdrożenie Systemu HIS – do 29.05.2026r

Etap IV – Dostawa i instalacja infrastruktury ICT – do 15.05.2026r

Etap V – świadczenia przez Wykonawcę na rzecz Zamawiającego Usług Gwarancji i Opieki Serwisowej w zakresie eksploatacji rozbudowywanego i modernizowanego Systemu HIS, wdrożonego przez Wykonawcę u Zamawiającego – 36 miesięcy od daty podpisania Protokołu Odbioru Końcowego.

UWAGA: Całość zadania musi zostać zrealizowana nie później niż do 29.05.2026r

1. Zakres przedmiotowy Etapu I - Opracowanie analizy przedwdrożeniowej

W celu efektywnej realizacji projektu integracji i rozbudowy System HIS, projekt powinien być realizowany zgodnie z zaproponowaną przez Wykonawcę i zaakceptowaną przez Zamawiającego metodyką projektową, zgodą ze standardami realizacji projektów, np.: PRINCE2, Agile, Waterfall, PMI lub innymi równoważnymi standardami zarządzania projektami informatycznymi. Zamawiający zezwala na łączenie zastosowanych metodyk projektowych (np. Scrum+Kaban) oraz pozostawia Wykonawcy wybór metodyki zarządzania projektem.

Wykonawca jest zobowiązany wraz z zaproponowaną metodyką dostarczyć jej kluczowe założenia zawierające minimalnie strukturę zadań (Produktów), podział obowiązków, ról w projekcie, harmonogram, opisy podstawowych procesów oraz dyscyplin projektowych.

1. Organizacja prac związanych z Projektem

W celu efektywnego prowadzenia prac projektowych, w ramach projektu w terminie 7 dni kalendarzowych od dnia podpisania Umowy zostaną powołane odpowiednie struktury projektowe, zarówno po stronie Wykonawcy, jak również po stronie Zamawiającego.

Podstawowe role w ramach powołanej struktury powinny być minimalnie:

* Kierownik Projektu po stronie Wykonawcy odpowiedzialny za całość prac projektowych,
* Kierownictwo Wdrożenia – Komitet Sterujący, w skład, którego wchodzą wyznaczone przez Zamawiającego osoby upoważnione do podejmowania istotnych decyzji projektowych,
* Kierownik Projektu po stronie Zamawiającego odpowiedzialny za prace wykonywane przez Zamawiającego,
* Zespół użytkowników kluczowych (liderów) – dla każdego Etapu osoby wskazane przez Zamawiającego, uczestniczące w realizacji przedmiotu zadania

1. Kierownictwo wdrożenia – Komitet Sterujący

W skład operacyjnego Komitetu Sterującego wchodzi Kierownik Projektu po stronie Zamawiającego oraz Kierownik Projektu po stronie Wykonawcy. Wykonawca i Zamawiający w terminie 7 dni kalendarzowych są zobowiązani do wskazania osób pełniących role Kierowników Projektu.

Komitet Sterujący jest organem pełniącym nadzór nad przebiegiem realizacji zamówienia, reagującym na pojawiające się problemy i zagrożenia. Rolą Komitetu Sterującego będzie planowanie wszystkich działań dotyczących Projektu, monitorowanie stanu jego realizacji oraz rozwiązywanie kwestii spornych, w szczególności Komitet Sterujący będzie:

* sprawował nadzór i kontrolę nad realizacją Umowy,
* rekomendował Zamawiającemu decyzje o strategicznym znaczeniu dla realizacji Umowy,
* stosownie do potrzeb, rekomendował zmiany Harmonogramu Realizacji Umowy i zakresu Umowy oraz ewentualne odstępstwa od innych jej zapisów,
* rozwiązywał ewentualne problemy powstające w wyniku realizacji Umowy.

1. Obowiązki Kierownika Projektu po Stronie Wykonawcy:

* Wyznaczenie osób upoważnionych do realizacji przedmiotu umowy po stronie Wykonawcy, lista osób upoważnionych zostanie przekazana Kierownikowi Projektu po stronie Zamawiającego bezzwłocznie po podpisaniu umowy oraz bezzwłocznie po każdej zmianie osób upoważnionych.
* Planowanie i nadzór nad realizacją zadań głównych oraz szczegółowych zgodnie z zatwierdzonym Harmonogramem Realizacji Umowy.
* Nadzór nad czynnościami realizowanymi w ramach przedmiotu umowy, przez osoby upoważnione.
* Zgłaszanie i zatwierdzanie gotowości do odbioru usług Kierownikowi Projektu po stronie Zamawiającego.
* Zgłaszanie potrzeby konsultacji i doradztwa w zakresie realizacji Projektu.
* Nadzór i kontrola realizacji prac i zobowiązań zgodnie z uzgodnionymi terminami.
* Prowadzenie i archiwizowanie dokumentacji zdarzeń i czynności wykonanych w ramach realizacji umowy, pozwalających na ustalenie faktów związanych m.in. ze zlecaniem, odbiorem i rozliczeniem usług.
* Zapewnienie odpowiedniego zastępstwa na czas swojej nieobecności z poinformowaniem Kierownika Projektu po stronie Zamawiającego.
* Przedkładanie informacji Kierownikowi Projektu po stronie Zamawiającego zgodnie z jego potrzebami.
* Przedkładanie wniosków, sugestii i propozycji Kierownikowi Projektu po stronie Zamawiającego zgodnie z potrzebami.
* Realizowanie we współpracy z Kierownikiem Projektu po stronie Zamawiającego wszystkich zadań związanych z procesem zarządzania realizacja zadania.
* Nadzór nad realizacją zakresu Wdrożenia.
* Zarządzanie ryzykiem, zdarzeniami, wnioskami o zmianę.
* Wspólna z Kierownikiem Projektu po stronie Zamawiającego kontrola terminowej i zgodnej z budżetem realizacji zadania, w szczególności w obszarach prac wykonywanych przez pracowników Wykonawcy.
* Analiza i rozwiązywanie problemów projektowych, które mogłyby mieć negatywny wpływ na harmonogram realizowanych zadań.
* Koordynacja przeprowadzenia odbioru prac w Projekcie.
* Podpisywanie Protokołów.

1. Obowiązki Kierownika Projektu po stronie Zamawiającego:

* Współpraca z Wykonawcą w realizacji przedmiotu umowy.
* Bezzwłoczne rozstrzyganie spraw spornych pomiędzy zespołami ze strony Zamawiającego oraz Wykonawcą w terminie nie dłuższym niż 7 dni kalendarzowych. W przypadku powstania kwestii spornych między stronami zaangażowanymi w realizację zadania, Kierownik Projektu po stronie Zamawiającego powinien być stroną rozstrzygającą o najlepszym rozwiązaniu.
* Określenie formy sprawozdań przedstawianych przez Kierownika Projektu ze strony Wykonawcy.
* Przyjmowanie i akceptacja protokołów odbioru z realizacji Etapów.
* Obowiązek formalnego zgłoszenia żądania zmiany, jeżeli uzna, że dla zapewnienia prawidłowej realizacji przedmiotu umowy konieczne jest podjęcie działań mających wpływ na ustalony zakres prac.
* Przegląd, zgłaszanie uwag, akceptacja oraz odbiór poszczególnych Etapów od Wykonawcy.
* Kontrola jakości Wdrożenia i realizacji poszczególnych etapów poprzez ciągłą kontrolę jakości dostarczanych projektów oraz podejmowanych decyzji.
* Nadzór nad pracownikami Zamawiającego oddelegowanymi do projektu w szczególności weryfikacja zadań przewidzianych dla rzeczonych do wykonania oraz rozstrzyganie sporów pomiędzy pracownikami.
* Zarządzanie komunikacją - zapewnienie odpowiedniego procesu informacyjnego dotyczącego prowadzonych prac i ich wyników.
* Zarządzanie ryzykiem - w ścisłej współpracy z Kierownikiem Projektu po stronie Wykonawcy.
* Zapewnienie zasobów ze strony Zamawiającego koniecznych do terminowego i zgodnego z założeniami wykonania prac.

1. Przygotowanie Dokumentacji

W ramach procesu prac Wykonawca opracuje dla Zamawiającego Dokumentację Przedmiotu Zamówienia (zwaną dalej Dokumentacją), która składa się z nw. zakresów:

* Dokumentacja Analizy Przedwdrożeniowej (DAP)
* Dokumentacja Powykonawcza

Dokumentacja powyższa będzie zawierać bazowe zapisy opisujące budowane rozwiązania, procesy oraz sposób organizacji prac, dostaw, instalacji i wdrożenia. Na podstawie zapisów w Dokumentacji będą prowadzone i odbierane poszczególne etapy realizowane w ramach Przedmiotu zamówienia. Dokumenty te wraz ze Specyfikacją Warunków Zamówienia wraz z załącznikami (dalej zwanych SWZ) będą stanowiły podstawę do weryfikacji realizacji zadania i jego poszczególnych etapów w trakcie odbiorów.

Wykonawca opracuje w terminie 14 dni od daty udostępnienia danych i dostępów, Dokumentację Analizy Przedwdrożeniowej (DAP). Zamawiający dokona akceptacji DAP w terminie 5 Dni roboczych od dnia jej przekazania przez Wykonawcę, co Strony potwierdzą odpowiednim Protokołem albo w tym samym terminie zgłosi zastrzeżenia do DAP, które są wiążące dla Wykonawcy. Zatwierdzona DAP stanowi dokument wiążący dla Stron.

Analiza przedwdrożeniowa, którą należy rozumieć jako zakres czynności do wykonania przez Wykonawcę ma na celu analizę środowiska biznesowego i informatycznego Zamawiającego. W wyniku przeprowadzenia Analizy przedwdrożeniowej Wykonawca przedstawi Zamawiającemu Dokumentację Analizy Przedwdrożeniowej (zwana dalej DAP), na podstawie, której będzie realizowany organizacyjnie i technicznie Przedmiot Zamówienia.

1. Dokumentacja Analizy Przedwdrożeniowej DAP

DAP powinna określać w poszczególnych obszarach co najmniej:

ZARZĄDCZY

* Harmonogram Realizacji Umowy,
* plan i sposób komunikacji Stron,
* zarządzenie ryzykiem,
* zarządzanie zmianą.

INFRASTRUKTURA

* analiza parametrów Infrastruktury udostępnionej przez Zamawiającego do celów realizacji Przedmiotu Zamówienia,
* przygotowanie planu reinstalacji /rekonfiguracji Infrastruktury Zamawiającego (serwerowej i sieciowej),
* opis instalacji Infrastruktury IT
* plan wykonania usług związanych z montażem i konfiguracją dostarczanej Infrastruktury IT
* zakres instalacji oraz konfiguracji oprogramowania
* plan instruktażu dla administratorów

HIS

* podział Przedmiotu Zamówienia na Produkty,
* architekturę HIS
* jednoznacznie określone założenia integracji z innymi systemami informatycznymi, które posiada Zamawiający,
* szczegółową specyfikację oprogramowania objętego zakresem umowy,
* ustawienia konfiguracyjne oprogramowania wchodzącego w skład HIS,
* lista Produktów lub/oraz ich komponentów, które będę podlegały osobnym odbiorom,
* zakres szkoleń.

1. Dokumentacja powykonawcza

Warunkiem dokonania odbioru Etapu IIIbędzie 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.

W dokumentacji muszą być zawarte opisy wszelkich cech, właściwości i funkcjonalności pozwalających na poprawną z punktu widzenia technicznego administrację i eksploatację rozwiązań.

W szczególności dokumentacja ta powinna zawierać następujące elementy:

Wymogi ogólne:

1. Pełna charakterystyka i opis sposobu licencjonowania Aplikacji oraz oprogramowania towarzyszącego (ewentualnie umowa licencyjna),
2. Opis architektury technicznej:

* Wyszczególnienie oraz opis minimalnych wymagań sprzętowych, systemowych i aplikacyjnych wymaganych do poprawnej pracy Aplikacji zgodnie z wymaganiami wydajności, funkcjonalności i bezpieczeństwa.
* Objaśnienie wykonanej rekonfiguracji wdrożonego Systemu.
* Opis zainstalowanej bazy danych.

1. Dokumentacja administracyjna związana z poprawną eksploatacją:

* opis (w postaci procedur lub instrukcji) wszystkich rutynowych czynności administracyjnych dla Aplikacji i Systemu informatycznego (dziennych, tygodniowych, miesięcznych itp.),
* opis procedury tworzenia/odtwarzania kopii bezpieczeństwa operacyjnego i kopii zapasowych oraz odtwarzania/kreowania z kopii wszystkich komponentów aplikacji i środowiska (bazy danych, komponenty serwera aplikacji, klienta itp.),
* opis zalecanego trybu backupu aplikacji i elementów infrastruktury software’owej, oraz zakres danych podlegających backupowi.

1. Dokumentacja wdrożeniowa:

* instrukcje obsługi i instrukcje użytkowania dla wersji dostarczonego oprogramowania z podziałem na poszczególne moduły.
* w zakresie obszarów administratora dokumentacja powinna zawierać dodatkowo co najmniej:
* opis podstawowych ról użytkowników,
* opis zarządzania uprawnieniami użytkownika.
* opis sposobu przetwarzania danych oraz wykaz zbiorów danych osobowych.

1. Zakres przedmiotowy Etapu II - Dostawa licencji systemu HIS
2. Wykaz Licencji Systemu HIS objętych przedmiotem Umowy:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Lp. | Nazwa modułu | Ilość | Rodzaj licencji | Okres |
|  | MODUŁ BLOK OPERACYJNY | Open | RU | bezterminowa |
|  | MODUŁ PULPIT PIELĘGNIARSKI | OPEN | RU | bezterminowa |
|  | MODUŁ PULPIT AMBULATORYJNY | OPEN | RU | bezterminowa |
|  | MODUŁ PULPIT REJESTRACYJNY | OPEN | RU | bezterminowa |
|  | ORDYNACJA LEKARSKA | OPEN | RU | bezterminowa |
|  | EDM: Wyniki i opisy badań histopatologicznych | 1 | SRW | bezterminowa |
|  | EDM: Wyniki i opisy badań cytologiczny | 1 | SRW | bezterminowa |
|  | EDM: Karta diagnostyki i leczenia onkologicznego - e-DILO | 1 | SRW | bezterminowa |
|  | EDM: Plan leczenia onkologicznego | 1 | SRW | bezterminowa |
|  | EDM: PatientSummary (karta zdrowia pacjenta) | 1 | SRW | bezterminowa |
|  | EDM: Karta opieki kardiologicznej (e-KOK) | 1 | SRW | bezterminowa |
|  | RZM API | 1 | SRW | bezterminowa |
|  | EDM GATEWAY | 1 | SRW | bezterminowa |
|  | Wieloskładnikowe uwierzytelnianie | 1 | SRW | bezterminowa |

1. Warunki licencji:
2. Zamawiający oczekuje udzielenia licencji dla poszczególnych Aplikacji, których przedmiotem będą odpowiednio:
   * Równoczesny użytkownik (RU) - Zamawiający jest uprawniony do korzystania z danego modułu oprogramowania w ramach posiadanej sieci komputerowej równocześnie przez maksymalnie taką liczbę użytkowników, na jaką została udzielona,
   * Open – Zamawiający jest uprawniony do korzystania z danego modułu oprogramowania w ramach posiadanej sieci komputerowej przez nieograniczoną liczbę użytkowników,
   * Serwerowa (SRW) - Zamawiający jest uprawniony do korzystania z danego modułu oprogramowania na maksymalnie takiej liczbie serwerów, na jaką została udzielona przez nieograniczoną liczbę użytkowników na nieograniczonej liczbie komputerów lub terminali. Licencja reglamentuje także systemy operacyjne serwera do liczby tożsamej z ilością serwerów, na które została udzielona,
   * System (SYS) - Licencja SYS jest licencją umożliwiającą wykorzystanie oprogramowania w kontekście integracji z jednym, określonym systemem zewnętrznym.
3. Licencja na korzystanie z Systemu, rozwinięć, uaktualnień i dokumentacji udzielona zostanie Zamawiającemu na następujących zasadach:
   * w zakresie Systemu, rozwinięć, uaktualnień – obejmuje prawo trwałego lub czasowego zwielokrotniania programów komputerowych w pamięci komputera z prawem do zmian w konfiguracji Systemu (bez ingerencji w kod źródłowy) w zakresie, w jakim jest to niezbędne do korzystania z Systemu zgodnie z jego przeznaczeniem i funkcjonalnością określoną w dokumentacji, nie mniejszą niż w OPZ,
   * w zakresie dokumentacji – obejmuje prawo zwielokrotniania egzemplarzy dokumentacji, w zakresie, w jakim jest to niezbędne do zgodnego z postanowieniami dokumentów licencyjnych korzystania z Systemu, a także prawo do umieszczania dokumentacji przeznaczonej dla użytkowników Systemu w Intranecie.
4. Licencja nie może wprowadzać ograniczenia na tzw. „nazwanych użytkowników”
5. Licencją objęte zostaną również wszelkie poprawki i aktualizacje Systemu pojawiające się w trakcie obowiązywania przedmiotowej Umowy a także w trakcie następnych umów serwisowych.
6. Wykonawca zobowiązany jest udzielić licencji na System, jego rozwinięcia i uaktualnienia oraz towarzyszącą dokumentację na czas nieoznaczony.
7. Zakres przedmiotowy Etap III - Wdrożenie systemu HIS
8. Usługi Wdrożeniowe
9. Wdrożenie należy rozumieć jako szereg uporządkowanych i zorganizowanych działań mających na celu wykonanie Przedmiotu Zamówienia.
10. Wykonawca umożliwi Zamawiającemu udział we wszystkich pracach realizowanych przez Wykonawcę w ramach realizacji Przedmiotu Zamówienia (m.in. w czasie dostaw, instalacji, konfiguracji i pozostałych elementach wdrożenia).
11. Wykonawca zobowiązany jest przeprowadzić dostawy Przedmiotu Zamówienia w dokładnych terminach i godzinach uzgodnionych z Zamawiającym z uwzględnieniem postanowień Harmonogramu realizacji Projektu uzgodnionego w ramach DAP.
12. Wdrożenie będą realizowane w ramach powołanych do tego celu struktur organizacyjnych po stronie Wykonawcy i Zamawiającego wskazanych w DAP.
13. Wykonawca zorganizuje prace tak, aby w maksymalnym stopniu nie zakłócać ciągłości funkcjonowania prac u Zamawiającego. 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.
14. Wykonawca musi uwzględnić, że wszystkie prace wykonywane będą w użytkowanych obiektach przy dużym ruchu pracowników i chorych, tzn. organizacja prac powinna przede wszystkim zapewniać bezpieczeństwo przebywających w oddziałach pracowników i chorych oraz zachowanie ciszy nocnej w godzinach właściwych dla Zamawiającego.
15. 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).
16. Oprogramowanie aplikacyjne musi zostać zainstalowane przez Wykonawcę w szczególności z wykorzystaniem Sprzętu dostarczanego przez Wykonawcę w ramach Etapu IV oraz w środowiskach informatycznych Zamawiającego. Oprogramowanie aplikacyjne musi zostać zainstalowane i skonfigurowane w sposób kompleksowy na wszystkich stanowiskach komputerowych Zamawiającego.
17. Zamawiający na potrzeby realizacji przedmiotu zamówienia przewidział infrastrukturę serwerową i oprogramowanie i dostosuje sprzęt spełniający minimalne warunki techniczne zalecane przez dostawcę oprogramowania.
18. Instruktaże stanowiskowe
19. 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.
20. Wykonawca przeprowadzi instruktaże stanowiskowe w siedzibie Zamawiającego, z możliwością zdalnych połączeń do szkoleń. Zamawiający udostępni pomieszczenie oraz sprzęt celem przeprowadzenia instruktaży stanowiskowych.
21. Na podstawie przekazanego przez Zamawiającego wykazu osób oraz przewidywanego terminu i czasu instruktażu stanowiskowego, Wykonawca zaproponuje harmonogram jak i podział na grupy -szczegółowy harmonogram realizacji instruktaży zostanie uzgodniony na etapie Analizy Przedwdrożeniowej.
22. 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 powinien być obecny co najmniej 1 informatyk.
23. Wykonawca nie ponosi odpowiedzialności za brak uczestnictwa użytkowników w instruktażach stanowiskowych.
24. Instruktaże stanowiskowe użytkowników Systemu HIS i administratora będą musiały spełniać minimum następujących wymagania:

* zajęcia powinny odbywać się w godzinach od godz. 8.00 do 15.00 od poniedziałku do piątku z wyłączeniem dni ustawowo wolnych od pracy;
* zajęcia nie będą mogły trwać dłużej niż 6 godzin dziennie.

1. Za skuteczne przeprowadzenie instruktażu stanowiskowego uważa się dostępność w ustalonym miejscu i terminie przedstawicieli Wykonawcy, gotowych przeprowadzić instruktaż zgodnie z ustalonym harmonogramem.
2. Wykonawca w ramach instruktażu stanowiskowego przekaże instrukcje do wdrożonego Systemu oraz materiały szkoleniowe. Instruktaże stanowiskowe będą prowadzone w języku polskim W ramach przeprowadzonych instruktaży stanowiskowych wymaga się:

* przekazania wiedzy niezbędnej do poprawnego użytkowania wdrożonego Systemu, jego zakresu funkcjonalnego,
* przekazania wiedza w zakresie tworzenia i gromadzenia informacji, tworzeniem i gromadzeniem dokumentów, wykonywaniem analiz, sprawozdań i raportów.

1. 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 działania użytkowania wdrożonego Systemu HIS.
2. Instruktaże stanowiskowe będą prowadzone w dwóch kategoriach:

* dla użytkowników Systemu HIS – do150 godzin
* dla administratorów – do10godzin

1. Szacowana liczba pracowników Zamawiającego planowanych do instruktaży stanowiskowych osób personelu Zamawiającego i 2 administratorów, w tym:

* lekarze – 83
* pielęgniarki, położne –198
* sekretarki medyczne i statystyka medyczna - 21
* pozostali pracownicy administracyjni – 8
* administrator systemu – 2

1. Po ukończeniu instruktaży stanowiskowych uczestnicy mają w szczególności umieć posługiwać się w pełni samodzielnie wdrożonym Systemem HIS i jego Modułami odpowiednio do swojej roli, a także znać i rozumieć ich funkcjonowanie w Systemie.
2. Administratorzy po zakończeniu instruktaży muszą w szczególności umieć wykonywać czynności administracyjne a także instalacji oprogramowania systemowego i narzędziowego oraz Sytemu HIS, znać i umieć realizować procedury backupu, znać wytyczne w zakresie polityki bezpieczeństwa i umieć je stosować. Ponadto powinni znać typowe zagrożenia i problemy związane z funkcjonowaniem Systemu, a także sposoby ich wykrywania oraz przeciwdziałania. Powinni umieć instalować, konfigurować, rekonfigurować, monitorować i prawidłowo eksploatować dostarczony Sprzęt i Oprogramowanie, jak również znać jego wdrożoną konfigurację.
3. Wymagania funkcjonalne systemu HIS

Pulpit Ambulatoryjny

|  |  |
| --- | --- |
| **Lp.** | **WYMAGANIA PODSTAWOWE:** |
|  | Pulpit umożliwia lekarzom prosty i w pełni konfigurowalny dostęp do najważniejszych elementów wizyty oraz dokumentacji medycznej wielu pacjentów odwzorowując metodykę pracy użytkownika. |
|  | **OBSŁUGA PORADNI** |
|  | Aplikacja posiada menu górne, które zawiera co najmniej następujące pozycje: |
|  | wizyty (wraz z szybką informacją w postaci liczby informującej o pacjentach czekających na wizytę do realizacji), |
|  | lista konsultacji (wraz z szybką informacją w postaci liczby konsultacji czekających na obsłużenie), |
|  | lista zadań (lista wizyt posiadających braki w ewidencji danych tj. rozpoznanie, procedura medyczna, opis wizyty, procedura rozliczeniowa wraz z szybką informację w postaci liczby takich wizyt), |
|  | lista dokumentów EDM (wraz z szybką informacją w postaci liczby dokumentów oczekających na podpisanie). |
|  | Pozycje w menu górnym reprezentują podstawowe konteksty pracy lekarza: |
|  | Wizyty - podczas pracy z pacjentami lekarz może oglądać i ewidencjonować dokumentację medyczną pacjenta, |
|  | Konsultacje - lekarz ma podgląd dokumentacji w celu wykonania konsultacji lekarskiej, |
|  | Dokumenty EDM - lekarz ma podgląd powstającej elektronicznej dokumentacji medycznej. |
|  | Zadania - podgląd podstawowych zadań do wykonania przez lekarza wygenerowanych na podstawie konfiguracji systemu: |
|  | \* Uzupełnienie braków w ewidencji - brak opisu wizyty, rozpoznania, procedury medycznej lub procedury rozliczeniowej. |
|  | Po wyborze z menu górnego odpowiedniego kontekstu, aplikacja prezentuje listę danych w ramach kontekstu z możliwością przełączania między trybami: pełna lista (prezentowana na całej szerokości ekranu), skrócona lista z obszarem roboczym (lista prezentowana jest tylko z lewej strony ekranu), tylko obszar roboczy. |
|  | Z obszarów roboczych możliwe jest przejście do ekranów szczegółowych umożliwiających podgląd i ewidencję danych dziedzinowych. |
|  | Pulpit wykorzystuje tzw. pływający przycisk (ang. floatingbutton). Przycisk ten zapewnia szybki dostęp do akcji w systemie. Razem z menu górnym umożliwia szybką i łatwą nawigację pomiędzy podstawowymi kontekstami pracy lekarza oraz ewidencją danych dziedzinowych w ekranach szczegółowych. |
|  | Ustawienia użytkownika obejmują personalizację aplikacji w zakresie obszaru roboczego (szczegóły w wymaganiach dotyczących obszaru roboczego) oraz możliwość importu certyfikatu ZUS służącego do podpisywania elektronicznej dokumentacji medycznej (certyfikat ZUS - podpisywanie z wykorzystaniem sposobu potwierdzania pochodzenia oraz integralności danych dostępnego w systemie teleinformatycznym udostępnionym bezpłatnie przez Zakład Ubezpieczeń Społecznych). |
|  | Możliwość przełączenia (przechwytywania) sesji na innym stanowisku roboczym - użytkownik systemu zmieniający miejsce pracy może na dowolnym komputerze kontynuować wcześniej utworzoną sesję na innym komputerze zachowując ciągłość pracy. |
|  | WYMAGANIA DOTYCZĄCE KONTEKSTU WIZYTY |
|  | Po wyborze z menu górnego pozycji wizyty, aplikacja prezentuje wykaz pacjentów w poradni zmożliwością przełączania między trybami: pełna lista pacjentów (prezentowana na całej szerokości ekranu), skrócona lista pacjentów (prezentowana jest tylko z lewej strony ekranu), chowana lista pacjentów (prezentowana z lewej strony, chowająca się po wybraniu pacjenta). |
|  | Aplikacja zapewnia pełny widok listy pacjentów, prezentuje dane w zakresie co najmniej: |
|  | nr wizyty, |
|  | nr kartoteki, |
|  | nazwisko, |
|  | imię, |
|  | PESEL, |
|  | data wizyty, |
|  | data wizyty do, |
|  | lekarz przyjmujący, |
|  | poradnia |
|  | specjalne statusy pacjenta, |
|  | decyzja. |
|  | Lista pacjentów podzielona jest na pacjentów do obsłużenia, w trakcie realizacji oraz obsłużonych w danym dniu. |
|  | Aplikacja prezentuje skrócony widok listy pacjentów prezentuje dane w zakresie co najmniej: |
|  | imię, |
|  | nazwisko, |
|  | PESEL, |
|  | specjalne statusy pacjenta. |
|  | Lista pacjentów podzielona jest na pacjentów do obsłużenia, w trakcie realizacji oraz obsłużonych w danym dniu. |
|  | Moduł umożliwia wyszukiwanie pacjentów na listach pacjentów minimum według następujących filtrów: |
|  | imię, |
|  | nazwisko, |
|  | PESEL, |
|  | nr wizyty, |
|  | nr kartoteki, |
|  | lekarz przyjmujący, |
|  | data wizyty (zakres od-do), |
|  | data urodzenia pacjenta (zakres od-do), |
|  | decyzja. |
|  | Moduł posiada możliwość sortowania pacjentów na liście minimum według następujących kryteriów: |
|  | nr wizyty, |
|  | nr kartoteki, |
|  | nazwisko i imię pacjenta, |
|  | lekarz przyjmujący, |
|  | data wizyty, |
|  | data urodzenia. |
|  | Moduł umożliwia grupowanie pacjentów na liście minimum według następujących kryteriów: |
|  | według data wizyty, |
|  | według lekarza przyjmującego, |
|  | według decyzji. |
|  | Moduł podczas wszystkich operacji na pacjencie prezentuje tzw. belkę z elementarnymi danymi pacjenta obejmującymi co najmniej: |
|  | imię i nazwisko, |
|  | PESEL, |
|  | płeć, |
|  | wiek, |
|  | status weryfikacji eWUŚ, |
|  | grupa krwi, |
|  | rozpoznanie zasadnicze, |
|  | specjalny status pacjenta, |
|  | alergie pacjenta, |
|  | Chowana lista pacjentów może być ukrywana i ujawniana poprzez najechanie na lewą stronę ekranu. |
|  | Dane w obszarze roboczym prezentowane są w oparciu o dane źródłowe pochodzące z HIS, w zależności od wdrożonych zakresów funkcjonalnych HIS. Przy założeniu, że dany zakres funkcjonalny HIS stanowi przedmiot projektu system umożliwia odpowiednio: |
|  | udostępnianie danych zleconych badań diagnostycznych i ich wyników (Pracownia Diagnostyczna), |
|  | udostępnianie danych zleconych badań laboratoryjnych i ich wyników (Laboratorium), |
|  | udostępnianie danych zleconych badań bakteriologicznych i danych o ich wykonaniu (Bakteriologia), |
|  | udostępnianie danych zleconych badań histopatologicznych i danych o ich wykonaniu (Histopatologia). |
|  | Określenie Specjalnych Statusów Pacjenta (SSP) np. pacjent COVID, pacjent z zakażeniem szpitalnym. Statusy nadawane przez użytkownika systemu. |
|  | Możliwe specjalne statusy pacjenta nadawane przez użytkowników systemu konfigurowane przez administratora systemu. |
|  | Możliwość przypisania wielu SSP dla pacjenta. |
|  | Nadanie statusu SSP może powodować przesłanie poprzez wewnętrzny system komunikacyjny zdefiniowanej wiadomości do określonego użytkownika ZSI. |
|  | SSP prezentowane są na karcie pacjenta oraz podczas zbiorczego widoku list pacjentów w pulpicie ambulatoryjnym. |
|  | System umożliwia filtrowanie danych wyświetlanych w dziedzinowych blokach danych na podstawie zakresów: |
|  | tylko bieżąca wizyta, |
|  | wszystkie świadczenia, |
|  | System umożliwia filtrowania danych na podstawie zakresów w co najmniej poniższych dziedzinowych blokach danych: |
|  | skierowania na badania diagnostyczne, |
|  | wyniki badań diagnostycznych, |
|  | skierowania na badania laboratoryjne, |
|  | wyniki badań laboratoryjnych, |
|  | skierowania na badania histopatologiczne, |
|  | wyniki badań histopatologicznych, |
|  | skierowania na badania bakteriologiczne, |
|  | wyniki badań bakteriologicznych, |
|  | konsultacje lekarskie, |
|  | rozpoznania, |
|  | dokumenty EDM, |
|  | zrealizowane procedury medyczne, |
|  | eRecepta, |
|  | eSkierowania, |
|  | zaświadczenia. |
|  | Szczególnym rodzajem bloku danych jest widok, który prezentuje historię leczenia danego pacjenta w pojedynczym oknie na osi czasu w układzie chronologicznym, w postaci rozwijanego drzewa wszystkich zdarzeń medycznych. |
|  | Widok historii leczenia umożliwia filtrowanie według wybranego przez użytkownika: |
|  | rodzaju zdarzeń medycznych (np. skierowania, wyniki, obserwacje), |
|  | czasu wystąpienia zdarzenia. |
|  | Wybór bloku dziedzinowego (lub zdarzenia medycznego z osi czasu) powoduje wywołanie odpowiedniego widoku prezentującego dane szczegółowe poszczególnych obszarów merytorycznych. |
|  | WYMAGANIA DOTYCZĄCE EKRANÓW SZCZEGÓŁOWYCH |
|  | Ekrany szczegółowe są uruchamiane poziomu obszaru roboczego lub poprzez tzw. pływający przycisk (ang. floatingbutton). Poza prezentacją danych szczegółowych dotyczących wybranego dziedzinowego bloku danych, ekrany szczegółowe umożliwiają także ewidencję danych (funkcja ta zależna jest od uprawnień użytkownika i dziedzinowego bloku danych). |
|  | System umożliwia ewidencję danych co najmniej w ekranach szczegółowych: |
|  | szczegóły wizyty, |
|  | karta pacjenta (minimum w zakresie adresu oraz danych o zawodzie i zatrudnieniu), |
|  | skierowania na badania diagnostyczne, |
|  | skierowania na badania laboratoryjne, |
|  | skierowania na badania histopatologiczne, |
|  | skierowania na badania bakteriologiczne, |
|  | konsultacje lekarskie, |
|  | rozpoznania, |
|  | eRecepta, |
|  | eSkierowania, |
|  | zaświadczenia. |
|  | W ekranach szczegółowych aplikacja umożliwia podzielenie ekranu w celu jednoczesnego wprowadzania danych i wyświetlaniem danych z innej dziedziny (w zakresach dostępnych ekranów szczegółowych). Przykładowym oczekiwanym efektem są np.: |
|  | system umożliwia jednoczesne wprowadzanie danych dotyczących wizyty oraz wystawiania skierowania laboratoryjnego, |
|  | system umożliwia jednoczesne wprowadzenie danych dotyczących wizyty i wystawiania eRecepty. |
|  | WYMAGANIA DOTYCZĄCE PŁYWAJĄCEGO PRZYCISKU |
|  | Użytkownik ma możliwość z każdego miejsca pracy w systemie łatwego przejścia do akcji dostępnych w systemie poprzez kliknięcie pływającego przycisku (ang. floatingbutton). |
|  | Na dostępne akcje składają się: |
|  | przejścia do ekranów szczegółowych (co najmniej do eRecepty, eSkierowania). |
|  | Dostępne akcje wyświetlane po kliknięciu pływającego przycisku są podzielone na trzy zbiory: |
|  | wszystkie dostępne akcje, |
|  | najczęściej wykorzystywane przez użytkownika akcje, |
|  | akcje powiązane z bieżącym ekranem. |
|  | W ramach listy najczęściej używanych akcji, wyświetlanej poprzez kliknięcie na pływający przycisk, użytkownik ma możliwość wyszukania interesującej go akcji po jej nazwie. |
|  | WYMAGANIA DOTYCZĄCE KOMUNIKATORA |
|  | Użytkownik ma dostęp do powiadomień generowanych przez wewnętrzny system komunikacji. |
|  | Obsługa powiadomień nie blokuje bieżącej pracy użytkownika za wyjątkiem powiadomień wymuszających taką blokadę. |
|  | System informuje użytkownika o liczbie nieprzeczytanych powiadomień. |
|  | Z poziomu pulpitu ambulatoryjnego system umożliwia obsługę powiadomień: |
|  | systemowych (np. informacja o pojawieniu się wyniku do zleconego badania, informacja o konieczności udzielenia konsultacji), |
|  | przysłanych przez administratora (np. informacja o aktualizacji sytemu HIS), |
|  | przysłanych przez innych użytkowników (np. w postaci wewnętrznego komunikatora). |
|  | WYMAGANIA DOTYCZĄCE KONTEKSTU DOKUMENTÓW |
|  | Po wyborze z menu górnego pozycji Dokumenty EDM, aplikacja prezentuje wykaz dokumentów EDM z możliwością przełączania między trybami: pełna lista dokumentów (prezentowana na całej szerokości ekranu), skrócona lista dokumentów (prezentowana jest tylko z lewej strony ekranu). |
|  | Moduł umożliwia wyszukiwanie dokumentów EDM po nazwie. |
|  | Możliwość ograniczania listy dokumentów według zakresów. |
|  | Moduł umożliwia filtrowanie dokumentów. Dostępne filtry: |
|  | podpisany, |
|  | do podpisu, |
|  | aktualne. |
|  | Dla każdego dokumentu EDM moduł prezentuje: |
|  | dane o autorze dokumentu, |
|  | czy dokument jest podpisany, |
|  | dane pracownika, który podpisał dokument, |
|  | cel podpisu, |
|  | datę podpisu, |
|  | podgląd dokumentu. |
|  | Aplikacja umożliwia wydruk dokumentu EDM. |
|  | ROZBUDOWANE WYMAGANIA DOTYCZĄCE EKRANÓW SZCZEGÓŁOWYCH W ZINTEGROWANYM PULPICIE LEKARSKIM: |
|  | **Szczegóły wizyty** |
|  | Moduł umożliwia ewidencje danych dotyczących wizyty w zakresie opisu wizyty, rozpoznań, procedur medycznych oraz procedur rozliczeniowych. |
|  | Moduł umożliwia wydanie decyzji dla wizyty w poradni. |
|  | Moduł umożliwia przypisanie grupy JGP dla wizyty podczas zamykania wizyty w sposób automatyczny. |
|  | Moduł umożliwia automatyczne wygenerowanie dokumentu Karty ambulatoryjnej podczas kończenia wizyty w poradni. |
|  | Moduł umożliwia podgląd zaplanowanych wizyt pacjenta w poradni. |
|  | Moduł umożliwia podgląd eSkierowania na podstawie którego przyjmowany jest pacjent. |
|  | Moduł umożliwia kopiowanie rozpoznań z dowolnej wizyty w poradni. |
|  | Moduł umożliwia kopiowanie procedur z dowolnej wizyty w poradni. |
|  | Moduł umożliwia przypisania zaległej procedury medycznej z wykonania badań diagnostycznych dla aktualnej wizyty. |
|  | Moduł umożliwia wykorzystywanie szablonów podpowiedzi dla opisów wizyt. |
|  | Moduł umożliwia wykorzystywanie szablonów wizyty, które pozwalają po wyborze szablonu wstawienie rozpoznania, procedur medycznych, opisu wizyty. |
|  | Moduł umożliwia ewidencjonowanie leków i alergii pacjenta. |
|  | Moduł umożliwia dodawanie zestawów procedur medycznych np. procedura porada, w której skład wchodzi kilka procedur ICD-9. |
|  | Moduł umożliwia ewidencje danych na szczegółach wizyty oraz podgląd historii choroby pacjenta na jednym ekranie. |
|  | Moduł umożliwia podgląd karty pacjenta. |
|  | Moduł umożliwia edycję karty pacjenta w zakresie danych adresowych pacjenta. |
|  | **Konsultacje lekarskie** |
|  | Użytkownik posiada możliwość przeglądania konsultacji lekarskich wybranego pacjenta. |
|  | Na liście konsultacji system prezentuje dla każdej konsultacji jej status oraz pilność. |
|  | Moduł umożliwia wysłanie prośby o konsultację do danej jednostki z wskazaniem lekarza konsultującego lub bez wskazania lekarza. |
|  | Możliwość oznaczenia konsultacji jako pilnej. |
|  | Moduł umożliwia przyjęcie konsultacji do opisu. |
|  | **Rozpoznania** |
|  | Użytkownik systemu posiada możliwość przeglądania rozpoznań wybranego pacjenta w postaci listy: |
|  | z aktualnej wizyty, |
|  | z poprzednich wizyt. |
|  | Użytkownik ma możliwość dodawania informacji dotyczących: |
|  | rozpoznań pacjenta, |
|  | karty zgłoszenia choroby zakaźnej, |
|  | karty psychiatrycznej. |
|  | rozpoznań dodatkowych VY i \*\*. |
|  | Możliwość ewidencji rozpoznań pacjenta. |
|  | Możliwość kopiowania rozpoznań z poprzednich świadczeń pacjenta (pobyty, wizyty). |
|  | Poza kodem i opisem wg ICD-10 użytkownik systemu może dodać własny opis rozpoznania jako uszczegółowienie rozpoznania. |
|  | **Zrealizowane procedury medyczne** |
|  | Możliwość filtrowania listy procedur medycznych według minimum: |
|  | dat realizacji procedur, |
|  | pokaż wszystkie, |
|  | pokaż procedury ICD-9 PL. |
|  | Możliwość wyszukiwania na liście procedur według symbolu czy nazwy procedury. |
|  | **Skierowania na badania** |
|  | Moduł prezentuje listę zleconych badań wraz z informacją o statusie skierowania w postaci osi statusów (materiał do pobrania, aktualne, zrealizowane) i jego pilności. |
|  | Dla każdego skierowania system prezentuje dane szczegółowe. |
|  | Użytkownik ma możliwość powtórzenia danego skierowania lub skopiowania badań z poprzedniego skierowania. |
|  | W ramach skierowania laboratoryjnego i diagnostycznego moduł umożliwia przetwarzanie danych dotyczących rozpoznań i informacji dodatkowych. |
|  | W ramach skierowania laboratoryjnego możliwość zlecenia cyklicznego (wystawienie jednego skierowania powoduje wystawienie N skierowań w określonym interwale czasu np. 5 skierowań z tymi samymi badanami co 24 godziny). |
|  | **Wyniki zleconych badań** |
|  | Moduł prezentuje listę wyników do zleconych badań. |
|  | Dla każdego wyniku badań system prezentuje dane szczegółowe wyniku. |
|  | Możliwość wykonania analizy retrospektywnej dla konkretnych badań w ramach wyników laboratoryjnych. |
|  | Możliwość generacji wykresu w ramach analizy retrospektywnej w ramach wyników laboratoryjnych. |
|  | Możliwość wyszukiwania wyników badań laboratoryjnych po nazwie badania lub grupy badań np. Morfologia. |
|  | eRecepta |
|  | Moduł prezentuje listę wystawionych recept zarówno elektronicznych jak i papierowych. |
|  | Moduł umożliwia dodanie nowej eRecepty a w przypadku niepowodzenia w komunikacji z systemem centralnym, również w wersji papierowej. |
|  | Możliwość wydruku informacji o wystawionej eRecepcie dla pacjenta. |
|  | eSkierowania |
|  | Moduł prezentuje listę wystawionych skierowań, zarówno elektronicznych jak i papierowych. |
|  | Moduł umożliwia dodanie nowego skierowania elektronicznego a w przypadku niepowodzenia w komunikacji z systemem centralnym, również w wersji papierowej. |
|  | Możliwość wydrukowania informacji o wystawionym eSkierowaniu dla pacjenta. |
|  | Możliwość podglądu aktualnego statusu eSkierowania po stronie platformy P1 - możliwość podglądu czy eSkierowanie zostało zrealizowane przez pacjenta. |
|  | Dokumenty EDM |
|  | Moduł prezentuje listę dokumentów EDM wystawionych dla pacjenta. |
|  | Moduł pozwala na wydruk dokumentu EDM. |
|  | Moduł umożliwia podpisanie dokumentu EDM za pomocą certyfikatu ZUS (wykorzystaniem sposobu potwierdzania pochodzenia oraz integralności danych dostępnego w systemie teleinformatycznym udostępnionym bezpłatnie przez Zakład Ubezpieczeń Społecznych). |
|  | **OBSŁUGA IZBY PRZYJĘĆ** |
|  | Aplikacja posiada menu górne, które zawiera co najmniej następujące pozycje: |
|  | wizyty (wraz z szybką informacją w postaci liczby informującej o pacjentach czekających na wizytę do realizacji), |
|  | lista konsultacji (wraz z szybką informacją w postaci liczby konsultacji czekających na obsłużenie), |
|  | lista zadań (lista wizyt posiadających braki w ewidencji danych tj. rozpoznanie, procedura medyczna, opis wizyty, procedura rozliczeniowa wraz z szybką informację w postaci liczby takich wizyt), |
|  | lista dokumentów EDM (wraz z szybką informacją w postaci liczby dokumentów oczekających na podpisanie). |
|  | Pozycje w menu górnym reprezentują podstawowe konteksty pracy lekarza: |
|  | Wizyty - podczas pracy z pacjentami lekarz może oglądać i ewidencjonować dokumentację medyczną pacjenta, |
|  | Konsultacje - lekarz ma podgląd dokumentacji w celu wykonania konsultacji lekarskiej, |
|  | Dokumenty EDM - lekarz ma podgląd powstającej elektronicznej dokumentacji medycznej. |
|  | Zadania - podgląd podstawowych zadań do wykonania przez lekarza wygenerowanych na podstawie konfiguracji systemu: |
|  | \* Uzupełnienie braków w ewidencji - brak opisu wizyty, rozpoznania, procedury medycznej lub procedury rozliczeniowej. |
|  | Po wyborze z menu górnego odpowiedniego kontekstu, aplikacja prezentuje listę danych w ramach kontekstu z możliwością przełączania między trybami: pełna lista (prezentowana na całej szerokości ekranu), skrócona lista z obszarem roboczym (lista prezentowana jest tylko z lewej strony ekranu), tylko obszar roboczy. |
|  | Z obszarów roboczych możliwe jest przejście do ekranów szczegółowych umożliwiających podgląd i ewidencję danych dziedzinowych. |
|  | Pulpit wykorzystuje tzw. pływający przycisk (ang. floatingbutton). Przycisk ten zapewnia szybki dostęp do akcji w systemie. Razem z menu górnym umożliwia szybką i łatwą nawigację pomiędzy podstawowymi kontekstami pracy lekarza oraz ewidencją danych dziedzinowych w ekranach szczegółowych. |
|  | Ustawienia użytkownika obejmują personalizację aplikacji w zakresie obszaru roboczego (szczegóły w wymaganiach dotyczących obszaru roboczego) oraz możliwość importu certyfikatu ZUS służącego do podpisywania elektronicznej dokumentacji medycznej (certyfikat ZUS - podpisywanie z wykorzystaniem sposobu potwierdzania pochodzenia oraz integralności danych dostępnego w systemie teleinformatycznym udostępnionym bezpłatnie przez Zakład Ubezpieczeń Społecznych). |
|  | Możliwość przełączenia (przechwytywania) sesji na innym stanowisku roboczym - użytkownik systemu zmieniający miejsce pracy może na dowolnym komputerze kontynuować wcześniej utworzoną sesję na innym komputerze zachowując ciągłość pracy. |
|  | WYMAGANIA DOTYCZĄCE KONTEKSTU WIZYTY |
|  | Aplikacja zapewnia pełny widok listy pacjentów, prezentuje dane w zakresie co najmniej: |
|  | nazwisko, |
|  | imię, |
|  | PESEL, |
|  | data wizyty, |
|  | data wizyty do, |
|  | lekarz przyjmujący, |
|  | poradnia, |
|  | specjalne statusy pacjenta, |
|  | decyzja. |
|  | Aplikacja prezentuje skrócony widok listy pacjentów prezentuje dane w zakresie co najmniej: |
|  | imię, |
|  | nazwisko, |
|  | PESEL, |
|  | specjalne statusy pacjenta. |
|  | Moduł umożliwia wyszukiwanie pacjentów na listach pacjentów minimum według następujących filtrów: |
|  | imię, |
|  | nazwisko, |
|  | PESEL, |
|  | nr wizyty, |
|  | nr kartoteki, |
|  | lekarz przyjmujący, |
|  | data wizyty (zakres od-do), |
|  | data urodzenia pacjenta (zakres od-do), |
|  | decyzja. |
|  | Moduł posiada możliwość sortowania pacjentów na liście minimum według następujących kryteriów: |
|  | nr wizyty, |
|  | nr kartoteki, |
|  | nazwisko i imię pacjenta, |
|  | lekarz przyjmujący, |
|  | data wizyty, |
|  | data urodzenia. |
|  | Moduł umożliwia grupowanie pacjentów na liście minimum według następujących kryteriów: |
|  | według data wizyty, |
|  | według lekarza przyjmującego, |
|  | według decyzji, |
|  | Moduł podczas wszystkich operacji na pacjencie prezentuje tzw. belkę z elementarnymi danymi pacjenta obejmującymi co najmniej: |
|  | imię i nazwisko, |
|  | PESEL, |
|  | płeć, |
|  | wiek, |
|  | status weryfikacji eWUŚ, |
|  | grupa krwi, |
|  | rozpoznanie zasadnicze, |
|  | specjalny status pacjenta, |
|  | alergie pacjenta, |
|  | Chowana lista pacjentów może być ukrywana i ujawniana poprzez najechanie na lewą stronę ekranu. |
|  | Dane w obszarze roboczym prezentowane są w oparciu o dane źródłowe pochodzące z HIS, w zależności od wdrożonych zakresów funkcjonalnych HIS. Przy założeniu, że dany zakres funkcjonalny HIS stanowi przedmiot projektu system umożliwia odpowiednio: |
|  | udostępnianie danych zleconych badań diagnostycznych i ich wyników (Pracownia Diagnostyczna), |
|  | udostępnianie danych zleconych badań laboratoryjnych i ich wyników (Laboratorium), |
|  | udostępnianie danych zleconych badań bakteriologicznych i danych o ich wykonaniu (Bakteriologia), |
|  | udostępnianie danych zleconych badań histopatologicznych i danych o ich wykonaniu (Histopatologia), |
|  | Określenie Specjalnych Statusów Pacjenta (SSP) np. pacjent VIP, pacjent z zakażeniem szpitalnym. Statusy nadawane przez użytkownika systemu. |
|  | Możliwe specjalne statusy pacjenta nadawane przez użytkowników systemu konfigurowane przez administratora systemu. |
|  | Możliwość przypisania wielu SSP dla pacjenta. |
|  | Nadanie statusu SSP może powodować przesłanie poprzez wewnętrzny system komunikacyjny zdefiniowanej wiadomości do określonego użytkownika ZSI. |
|  | SSP prezentowane są na karcie pacjenta oraz podczas zbiorczego widoku list pacjentów w pulpicie ambulatoryjnym. |
|  | System umożliwia filtrowanie danych wyświetlanych w dziedzinowych blokach danych na podstawie zakresów: |
|  | tylko bieżąca wizyta |
|  | wszystkie świadczenia |
|  | System umożliwia filtrowania danych na podstawie zakresów w co najmniej poniższych dziedzinowych blokach danych: |
|  | skierowania na badania diagnostyczne, |
|  | wyniki badań diagnostycznych, |
|  | skierowania na badania laboratoryjne, |
|  | wyniki badań laboratoryjnych, |
|  | skierowania na badania histopatologiczne, |
|  | wyniki badań histopatologicznych, |
|  | skierowania na badania bakteriologiczne, |
|  | wyniki badań bakteriologicznych, |
|  | konsultacje lekarskie, |
|  | rozpoznania, |
|  | dokumenty EDM, |
|  | zrealizowane procedury medyczne, |
|  | eRecepta, |
|  | eSkierowania, |
|  | zaświadczenia, |
|  | Szczególnym rodzajem bloku danych jest widok, który prezentuje historię leczenia danego pacjenta w pojedynczym oknie na osi czasu w układzie chronologicznym, w postaci rozwijanego drzewa wszystkich zdarzeń medycznych. |
|  | Widok historii leczenia umożliwia filtrowanie według wybranego przez użytkownika: |
|  | rodzaju zdarzeń medycznych (np. skierowania, wyniki, obserwacje), |
|  | czasu wystąpienia zdarzenia, |
|  | Wybór bloku dziedzinowego (lub zdarzenia medycznego z osi czasu) powoduje wywołanie odpowiedniego widoku prezentującego dane szczegółowe poszczególnych obszarów merytorycznych. |
|  | WYMAGANIA DOTYCZĄCE EKRANÓW SZCZEGÓŁOWYCH |
|  | Ekrany szczegółowe są uruchamiane poziomu obszaru roboczego lub poprzez tzw. pływający przycisk (ang. floatingbutton). Poza prezentacją danych szczegółowych dotyczących wybranego dziedzinowego bloku danych, ekrany szczegółowe umożliwiają także ewidencję danych (funkcja ta zależna jest od uprawnień użytkownika i dziedzinowego bloku danych). |
|  | System umożliwia ewidencję danych co najmniej w ekranach szczegółowych: |
|  | szczegóły wizyty, |
|  | karta pacjenta (minimum w zakresie adresu oraz danych o zawodzie i zatrudnieniu), |
|  | skierowania na badania diagnostyczne, |
|  | skierowania na badania laboratoryjne, |
|  | skierowania na badania histopatologiczne, |
|  | skierowania na badania bakteriologiczne, |
|  | konsultacje lekarskie, |
|  | rozpoznania, |
|  | eRecepta, |
|  | eSkierowania, |
|  | zaświadczenia, |
|  | W ekranach szczegółowych aplikacja umożliwia podzielenie ekranu w celu jednoczesnego wprowadzania danych i wyświetlaniem danych z innej dziedziny (w zakresach dostępnych ekranów szczegółowych). Przykładowym oczekiwanym efektem są np.: |
|  | system umożliwia jednoczesne wprowadzanie danych dotyczących wizyty oraz wystawiania skierowania laboratoryjnego, |
|  | system umożliwia jednoczesne wprowadzenie danych dotyczących wizyty i wystawiania eRecepty. |
|  | WYMAGANIA DOTYCZĄCE PŁYWAJĄCEGO PRZYCISKU |
|  | Użytkownik ma możliwość z każdego miejsca pracy w systemie łatwego przejścia do akcji dostępnych w systemie poprzez kliknięcie pływającego przycisku (ang. floatingbutton). |
|  | Na dostępne akcje składają się: |
|  | przejścia do ekranów szczegółowych (co najmniej do eRecepty, eSkierowania), |
|  | Dostępne akcje wyświetlane po kliknięciu pływającego przycisku są podzielone na trzy zbiory: |
|  | wszystkie dostępne akcje, |
|  | najczęściej wykorzystywane przez użytkownika akcje, |
|  | akcje powiązane z bieżącym ekranem. |
|  | W ramach listy najczęściej używanych akcji, wyświetlanej poprzez kliknięcie na pływający przycisk, użytkownik ma możliwość wyszukania interesującej go akcji po jej nazwie. |
|  | WYMAGANIA DOTYCZĄCE KOMUNIKATORA |
|  | Użytkownik ma dostęp do powiadomień generowanych przez wewnętrzny system komunikacji. |
|  | Obsługa powiadomień nie blokuje bieżącej pracy użytkownika za wyjątkiem powiadomień wymuszających taką blokadę. |
|  | System informuje użytkownika o liczbie nieprzeczytanych powiadomień. |
|  | Z poziomu pulpitu ambulatoryjnego system umożliwia obsługę powiadomień: |
|  | systemowych (np. informacja o pojawieniu się wyniku do zleconego badania, informacja o konieczności udzielenia konsultacji), |
|  | przysłanych przez administratora (np. informacja o aktualizacji sytemu HIS), |
|  | przysłanych przez innych użytkowników (np. w postaci wewnętrznego komunikatora). |
|  | WYMAGANIA DOTYCZĄCE KONTEKSTU DOKUMENTÓW |
|  | Po wyborze z menu górnego pozycji Dokumenty EDM, aplikacja prezentuje wykaz dokumentów EDM z możliwością przełączania między trybami: pełna lista dokumentów (prezentowana na całej szerokości ekranu), skrócona lista dokumentów (prezentowana jest tylko z lewej strony ekranu). |
|  | Moduł umożliwia wyszukiwanie dokumentów EDM po nazwie. |
|  | Możliwość ograniczania listy dokumentów według zakresów: |
|  | wszystkie dokumenty użytkownika w jednostce, |
|  | wszystkie dokumenty w jednostce, |
|  | wszystkie dokumenty użytkownika, |
|  | Moduł umożliwia filtrowanie dokumentów. Dostępne filtry: |
|  | podpisany, |
|  | do podpisu, |
|  | aktualne, |
|  | Dla każdego dokumentu EDM moduł prezentuje: |
|  | dane o autorze dokumentu, |
|  | czy dokument jest podpisany, |
|  | dane pracownika, który podpisał dokument, |
|  | cel podpisu, |
|  | datę podpisu, |
|  | podgląd dokumentu. |
|  | Aplikacja umożliwia wydruk dokumentu EDM. |
|  | ROZBUDOWANE WYMAGANIA DOTYCZĄCE EKRANÓW SZCZEGÓŁOWYCH W ZINTEGROWANYM PULPICIE LEKARSKIM: |
|  | **Szczegóły wizyty** |
|  | Moduł umożliwia ewidencje danych dotyczących wizyty w zakresie opisu wizyty, rozpoznań, procedur medycznych oraz procedur rozliczeniowych. |
|  | Moduł umożliwia obsługę odmowy do izby przyjęć. |
|  | Moduł umożliwia automatyczne wygenerowanie dokumentu Karty odmowy podczas kończenia wizyty w izbie przyjęć. |
|  | Moduł umożliwia podgląd eSkierowania na podstawie którego przyjmowany jest pacjent. |
|  | Moduł umożliwia kopiowanie rozpoznań z dowolnej wizyty w poradni. |
|  | Moduł umożliwia kopiowanie procedur z dowolnej wizyty w poradni. |
|  | Moduł umożliwia przypisania zaległej procedury medycznej z wykonania badań diagnostycznych dla aktualnej wizyty. |
|  | Moduł umożliwia wykorzystywanie szablonów podpowiedzi dla opisów wizyt. |
|  | Moduł umożliwia wykorzystywanie szablonów wizyty, które pozwalają po wyborze szablonu wstawienie rozpoznania, procedur medycznych, opisu wizyty. |
|  | Moduł umożliwia ewidencjonowanie leków i alergii pacjenta. |
|  | Moduł umożliwia dodawanie zestawów procedur medycznych np. procedura porada, w której skład wchodzi kilka procedur ICD-9. |
|  | Moduł umożliwia ewidencje danych na szczegółach wizyty oraz podgląd historii choroby pacjenta na jednym ekranie. |
|  | Moduł umożliwia podgląd karty pacjenta. |
|  | Moduł umożliwia edycję karty pacjenta w zakresie danych adresowych pacjenta. |
|  | **Konsultacje lekarskie** |
|  | Użytkownik posiada możliwość przeglądania konsultacji lekarskich wybranego pacjenta. |
|  | Na liście konsultacji system prezentuje dla każdej konsultacji jej status oraz pilność. |
|  | Moduł umożliwia wysłanie prośby o konsultację do danej jednostki z wskazaniem lekarza konsultującego lub bez wskazania lekarza. |
|  | Możliwość oznaczenia konsultacji jako pilnej. |
|  | Moduł umożliwia przyjęcie konsultacji do opisu. |
|  | Rozpoznania |
|  | Użytkownik systemu posiada możliwość przeglądania rozpoznań wybranego pacjenta w postaci listy: |
|  | z aktualnego pobytu, |
|  | z poprzednich pobytów. |
|  | Użytkownik ma możliwość dodawania informacji dotyczących: |
|  | rozpoznań pacjenta, |
|  | karty zgłoszenia choroby zakaźnej, |
|  | karty psychiatrycznej. |
|  | rozpoznań dodatkowych VY i \*\*. |
|  | Możliwość ewidencji rozpoznań pacjenta. |
|  | Możliwość kopiowania rozpoznań z poprzednich świadczeń pacjenta (pobyty, wizyty). |
|  | Poza kodem i opisem wg ICD-10 użytkownik systemu może dodać własny opis rozpoznania jako uszczegółowienie rozpoznania. |
|  | Zrealizowane procedury medyczne |
|  | Możliwość filtrowania listy procedur medycznych według minimum: |
|  | dat realizacji procedur, |
|  | pokaż wszystkie, |
|  | pokaż procedury ICD-9 PL. |
|  | Możliwość wyszukiwania na liście procedur według symbolu czy nazwy procedury. |
|  | **Skierowania na badania** |
|  | Moduł prezentuje listę zleconych badań wraz z informacją o statusie skierowania w postaci osi statusów (materiał do pobrania, aktualne, zrealizowane) i jego pilności. |
|  | Dla każdego skierowania system prezentuje dane szczegółowe. |
|  | Użytkownik ma możliwość powtórzenia danego skierowania lub skopiowania badań z poprzedniego skierowania. |
|  | W ramach skierowania laboratoryjnego i diagnostycznego moduł umożliwia przetwarzanie danych dotyczących rozpoznań i informacji dodatkowych. |
|  | W ramach skierowania laboratoryjnego możliwość zlecenia cyklicznego (wystawienie jednego skierowania powoduje wystawienie N skierowań w określonym interwale czasu np. 5 skierowań z tymi samymi badanami co 24 godziny). |
|  | **Wyniki zleconych badań** |
|  | Moduł prezentuje listę wyników do zleconych badań. |
|  | Dla każdego wyniku badań system prezentuje dane szczegółowe wyniku. |
|  | Możliwość wykonania analizy retrospektywnej dla konkretnych badań w ramach wyników laboratoryjnych. |
|  | Możliwość generacji wykresu w ramach analizy retrospektywnej w ramach wyników laboratoryjnych. |
|  | Możliwość wyszukiwania wyników badań laboratoryjnych po nazwie badania lub grupy badań np. Morfologia. |
|  | **eRecepta** |
|  | Moduł prezentuje listę wystawionych recept zarówno elektronicznych jak i papierowych. |
|  | Moduł umożliwia dodanie nowej eRecepty a w przypadku niepowodzenia w komunikacji z systemem centralnym, również w wersji papierowej. |
|  | Możliwość wydruku informacji o wystawionej eRecepcie dla pacjenta. |
|  | **eSkierowania** |
|  | Moduł prezentuje listę wystawionych skierowań, zarówno elektronicznych jak i papierowych. |
|  | Moduł umożliwia dodanie nowego skierowania elektronicznego a w przypadku niepowodzenia w komunikacji z systemem centralnym, również w wersji papierowej. |
|  | Możliwość wydrukowania informacji o wystawionym eSkierowaniu dla pacjenta. |
|  | Możliwość podglądu aktualnego statusu eSkierowania po stronie platformy P1 - możliwość podglądu czy eSkierowanie zostało zrealizowane przez pacjenta. |
|  | **Dokumenty EDM** |
|  | Moduł prezentuje listę dokumentów EDM wystawionych dla pacjenta. |
|  | Moduł pozwala na wydruk dokumentu EDM. |
|  | Moduł umożliwia podpisanie dokumentu EDM za pomocą certyfikatu ZUS (wykorzystaniem sposobu potwierdzania pochodzenia oraz integralności danych dostępnego w systemie teleinformatycznym udostępnionym bezpłatnie przez Zakład Ubezpieczeń Społecznych). |

Pulpit Pielęgniarski

|  |  |
| --- | --- |
| **LP.** | **WYMAGANIA PODSTAWOWE** |
| 1. | Pulpit umożliwia personelowi pielęgniarskiemu szybki i w pełni konfigurowalny dostęp do najważniejszych elementów pobytu szpitalnego oraz dokumentacji medycznej wielu pacjentów odwzorowując metodykę pracy użytkownika. |
|  | Aplikacja posiada menu górne, które zawiera co najmniej następujące pozycje: |
| 2. | harmonogram, |
| 3. | pobyty (wraz z szybką informacją w postaci liczby informującej o pacjentach czekających na przyjęcie), |
| 4. | raport, |
| 5. | zadania, |
|  | Pozycje w menu górnym reprezentują podstawowe konteksty pracy: |
| 6. | Harmonogram - wykaz materiałów do pobrania w ramach skierowań laboratoryjnych oraz mikrobiologicznych, informacja o zaplanowanym badaniu w ramach skierowania diagnostyki obrazowej, zlecone leki do podania pacjentom - wszystkie informacje w ramach danej zmiany pielęgniarskie. Ponadto informacja o zaplanowanym zabiegu chirurgicznym, informacja o zamówieniu na krew. |
| 7. | Pobyty - podczas pracy z pacjentami personel pielęgniarski może oglądać i ewidencjonować dokumentację medyczną pacjenta |
| 8. | Raport - podsumowanie ostatnich 24godzin dla wszystkich pacjentów oddziału w zakresie obserwacji pielęgniarskich oraz wyników badań laboratoryjnych, diagnostyki obrazowej. |
| 9. | Po wyborze z menu górnego odpowiedniego kontekstu, aplikacja prezentuje listę danych w ramach kontekstu z możliwością przełączania między trybami: pełna lista (prezentowana na całej szerokości ekranu), skrócona lista z obszarem roboczym (lista prezentowana jest tylko z lewej strony ekranu), tylko obszar roboczy. |
| 10. | Obszary robocze prezentują dane zorganizowane w dziedzinowe bloki danych. |
| 11. | Z obszarów roboczych możliwe jest przejście do ekranów szczegółowych umożliwiających podgląd i ewidencję danych dziedzinowych. |
| 12. | Pulpit wykorzystuje tzw. pływający przycisk (ang. floatingbutton). Przycisk ten zapewnia szybki dostęp do akcji w systemie. Razem z menu górnym umożliwia szybką i łatwą nawigację pomiędzy podstawowymi kontekstami pracy personelu pielęgniarskiego oraz ewidencją danych dziedzinowych w ekranach szczegółowych. |
| 13. | Ustawienia użytkownika obejmują personalizację aplikacji w zakresie obszaru roboczego (szczegóły w wymaganiach dotyczących obszaru roboczego) oraz możliwość importu certyfikatu ZUS służącego do podpisywania elektronicznej dokumentacji medycznej (certyfikat ZUS - podpisywanie z wykorzystaniem sposobu potwierdzania pochodzenia oraz integralności danych dostępnego w systemie teleinformatycznym udostępnionym bezpłatnie przez Zakład Ubezpieczeń Społecznych). |
| 14. | Możliwość przełączenia (przechwytywania) sesji na innym stanowisku roboczym - użytkownik systemu zmieniający miejsce pracy może na dowolnym komputerze kontynuować wcześniej utworzoną sesję na innym komputerze zachowując ciągłość pracy. |
|  | **WYMAGANIA DOTYCZĄCE KONTEKSTU POBYTÓW** |
| 15. | Po wyborze z menu górnego pozycji pobyty, aplikacja prezentuje wykaz pacjentów na oddziale z możliwością przełączania między trybami: pełna lista pacjentów (prezentowana na całej szerokości ekranu), skrócona lista pacjentów (prezentowana jest tylko z lewej strony ekranu), chowana lista pacjentów (prezentowana z lewej strony, chowająca się po wybraniu pacjenta). |
|  | Aplikacja zapewnia pełny widok listy pacjentów, prezentuje dane w zakresie co najmniej: |
| 16. | nr księgi głównej, |
| 17. | nr księgi oddziałowej, |
| 18. | nazwisko, |
| 19. | imię, |
| 20. | PESEL, |
| 21. | data przyjęcia, |
| 22. | data wypisania, |
| 23. | lekarz prowadzący, |
| 24. | oddział, |
| 25. | specjalne statusy pacjenta, |
| 26. | łóżko, |
| 27. | sala. |
|  | Aplikacja prezentuje skrócony widok listy pacjentów prezentuje dane w zakresie co najmniej: |
| 28. | imię, |
| 29. | data przyjęcia, |
| 30. | nazwisko, |
| 31. | PESEL, |
| 32. | specjalne statusy pacjenta. |
|  | Moduł umożliwia wyszukiwanie pacjentów na listach pacjentów minimum według następujących filtrów: |
| 33. | imię, |
| 34. | nazwisko, |
| 35. | PESEL, |
| 36. | nr księgi głównej, |
| 37. | nr księgi oddziałowej, |
| 38. | lekarz prowadzący, |
| 39. | specjalne statusy pacjenta, |
| 40. | data przyjęcia na oddział (zakres od-do), |
| 41. | data urodzenia pacjenta (zakres od-do). |
|  | Moduł posiada możliwość sortowania pacjentów na liście minimum według następujących kryteriów: |
| 42. | nr księgi oddziałowej, |
| 43. | nr księgi głównej, |
| 44. | nazwisko i imię pacjenta, |
| 45. | lekarz prowadzący, |
| 46. | sala, |
| 47. | łóżko, |
| 48. | data wypisania, |
| 49. | data przyjęcia. |
|  | Moduł umożliwia grupowanie pacjentów na liście minimum według następujących kryteriów: |
| 50. | według Sali, |
| 51. | według lekarza prowadzącego, |
| 52. | według daty przyjęcia, |
| 53. | według daty wypisania, |
| 54. | według rozpoznania zasadniczego. |
|  | Moduł podczas wszystkich operacji na pacjencie prezentuje tzw. belkę z elementarnymi danymi pacjenta obejmującymi co najmniej: |
| 55. | imię i nazwisko, |
| 56. | PESEL, |
| 57. | płeć, |
| 58. | wiek, |
| 59. | sala / łóżko, |
| 60. | status weryfikacji eWUŚ, |
| 61. | grupa krwi, |
| 62. | rozpoznanie zasadnicze, |
| 63. | specjalny status pacjenta, |
| 64. | alergie pacjenta, |
| 65. | szczepienie COVID. |
| 66. | Chowana lista pacjentów może być ukrywana i ujawniana poprzez najechanie na lewą stronę ekranu. |
| 67. | Po wyborze pacjenta na liście pacjentów system prezentuje dane i dokumentację medyczną wytypowanego pacjenta w formie obszaru roboczego, tj. panelu prezentującego zbiorczo wiele zakładek i bloków zawierających dane i dokumentację pacjenta. |
| 68. | W przypadku zmiany pacjenta na skróconej liście pacjentów system automatycznie zaktualizuje dane prezentowane w obszarze roboczym i zaprezentuje je w kontekście wybranego pacjenta. |
| 69. | Pacjenci przyjęci w ciągu ostatnich 24h powinni być wyróżnieni na liście pacjentów odpowiednim znakiem graficznym. |
| 70. | Pacjenci przyjęciu w ciągu ostatnich 24h w trybie pilnym powinni być wyróżnieni na liście pacjentów odpowiednim znakiem graficznym. |
|  | Dane w obszarze roboczym prezentowane są w oparciu o dane źródłowe pochodzące z HIS, w zależności od wdrożonych zakresów funkcjonalnych HIS. Przy założeniu, że dany zakres funkcjonalny HIS stanowi przedmiot projektu system umożliwia odpowiednio: |
| 71. | podgląd zużytych leków i materiałów (Apteczka), |
| 72. | podgląd zleceń lekarskich w zakresie leków i procedur (Ordynacja Lekarska), |
| 73. | udostępnianie danych zleconych badań diagnostycznych i ich wyników (Pracownia Diagnostyczna), |
| 74. | udostępnianie danych zleconych badań laboratoryjnych i ich wyników (Laboratorium), |
| 75. | udostępnianie danych zleconych badań bakteriologicznych i danych o ich wykonaniu (Bakteriologia), |
| 76. | udostępnianie danych zleconych badań histopatologicznych i danych o ich wykonaniu (Histopatologia), |
| 77. | podgląd danych uzupełnianych przez pielęgniarki (Dokumentacja medyczna pielęgniarska), |
| 78. | dostęp do danych dotyczących zabiegów operacyjnych (Blok operacyjny). |
| 79. | Określenie Specjalnych Statusów Pacjenta (SSP) np. pacjent COVID, pacjent z zakażeniem szpitalnym. Statusy nadawane przez użytkownika systemu. |
| 80. | Możliwe specjalne statusy pacjenta nadawane przez użytkowników systemu konfigurowane przez administratora systemu. |
| 81. | Możliwość przypisania wielu SSP dla pacjenta. |
| 82. | SSP prezentowane są na karcie pacjenta oraz podczas zbiorczego widoku list pacjentów w pulpicie lekarskim. |
|  | **WYMAGAGANIA DOTYCZĄCE KONTEKSTU HARMONOGRAMU** |
|  | Możliwość wyświetlenia zaplanowanych zleceń na określone godziny z podziałem na: |
| 83. | leki, |
| 84. | wlewy, |
| 85. | leczenie żywieniowe, |
| 86. | procedury, |
| 87. | diagnostyka obrazowa, |
| 88. | pobranie materiału, |
| 89. | zabiegi, |
| 90. | wszystkie zlecenia powyższe na jednym ekranie. |
| 91. | Możliwość wyświetlenia zleceń już zrealizowanych |
|  | Możliwość wyświetlenia informacji dodatkowych uwzględniających: |
| 92. | specjalny status pacjenta, |
| 93. | zamówienia na krew. |
| 94. | Poszczególne zlecenia przedstawione są za pomocą ikonek na osi czasu danej zmiany pielęgniarskiej. |
| 95. | Zlecenia zlecone w przeciągu ostatniej godziny są wyróżnione graficznie na harmonogramie |
| 96. | Możliwość podglądu poprzednich i kolejnych zmian pielęgniarskich |
| 97. | Możliwość filtrowania zleceń po salach |
| 98. | Możliwość grupowania zleceń po salach |
| 99. | Możliwość podglądu szczegółów zlecenia leku, przyjęcia zlecenia oraz jego realizacji. |
| 100. | Możliwość grupowego przyjęcia zlecenia oraz realizacji zlecenia podania leku |
| 101. | Możliwość podglądu szczegółów zlecenia wlewu, przyjęcia zlecenia oraz jego realizacji. |
| 102. | Możliwość grupowego przyjęcia zlecenia wlewów oraz jego realizacji |
| 103. | Możliwość wyświetlenia szczegółów skierowania diagnostycznego w zakresie nazwy badania |
| 104. | Możliwość wysyłania wszystkich materiałów wchodzących w skład skierowania do laboratorium po pobraniu materiału. |
| 105. | Możliwość wysłania wybranych materiałów wchodzących w skład skierowania do laboratorium po pobraniu materiału. |
| 106. | Możliwość wydrukowania kodu kreskowego na probówkę z materiałem |
| 107. | Możliwość dopisania uwag do poszczególnych materiałów w ramach skierowania |
| 108. | Możliwość zbiorczego zaznaczenia materiałów do wysłania do laboratorium |
| 109. | Możliwość zbiorczego wydruku kodów kreskowych do probówek bez wysyłania materiału. |
| 110. | Możliwość zbiorczego wysłania materiałów wraz z wydrukiem kodów kreskowych. |
| 111. | Możliwość uzupełnienia karty indywidualnej opieki pielęgniarskiej dla danego pacjenta. |
| 112. | Możliwość uzupełnienia karty gorączkowej. |
|  | **ROZBUDOWANE WYMAGANIA DOTYCZĄCE EKRANÓW SZCZEGÓŁOWYCH W ZINTEGROWANYM PULPICIE PIELĘGNIARSKIM:** |
|  | **Karta indywidualnej opieki pielęgniarskiej:** |
| 113. | Możliwość ewidencji obserwacji pielęgniarskich, |
| 114. | Możliwość ewidencji czynności pielęgniarskich. |
| 115. | Możliwość ewidencji procesu pielęgnowania z podziałem na problem jaki wystąpił u pacjenta, plan rozwiązania problemu oraz oceny realizacji planu. |
| 116. | Możliwość podglądu wpisów na osi czasu. |
| 117. | Możliwość ewidencji kategorii pielęgnacyjnej. |
| 118. | Możliwość automatycznego kopiowania kategorii po wejściu do ewidencji karty indywidualnej opieki pielęgniarskiej w przypadku gdy pacjent miał wcześniej przypisaną kategorię. |
| 119. | Możliwość kopiowania wpisów z poprzednich zmian pielęgniarskich. |
| 120. | Możliwość dodawania podpowiedzi dla obserwacji pielęgniarskich. |
| 121. | Możliwość korzystania z rozszerzonego słownika podpowiedzi dla procesu pielęgnowania tzn. dla poszczególnych problemów pielęgniarskich dedykowane podpowiedzi związane z planem opieki. |
|  | **Karta gorączkowa (karta pomiarowa):** |
| 122. | Możliwość ewidencji pomiarów temperatury |
| 123. | Możliwość ewidencji masy, wzrostu, ciśnienia, tętna, saturacji, skali bólu |
| 124. | Możliwość wyświetlania informacji czy dana wartość pomiaru jest większa/mniejsza względem poprzedniej ewidencji pomiaru |
| 125. | Możliwość graficznej reprezentacji przekroczenia normy dla danego pomiaru |
| 126. | Możliwość kopiowania poprzednich pomiarów. |
| 127. | Możliwość generacji wykresu za zadany okres czasu. |
| 128. | Możliwość filtrowania pomiarów po typie pomiaru np. temperatura, ciśnienie. |
|  | **Karta gospodarki wodnej (bilans wodny):** |
| 129. | Możliwość ewidencji ilości płynów podanych i wydalonych w ramach pełnych godzin. |
| 130. | Możliwość ewidencji ilości płynów podanych i wydalonych z podziałem na typ/sposób podania/wydalenia płynu. |
| 131. | Możliwość ewidencji uwag w ramach płynów podanych i wydalonych. |
| 132. | Możliwość automatycznego wyliczenia bilansu zmianowego. |
| 133. | Możliwość automatycznego wyliczenia bilansu dobowego. |
| 134. | Możliwość generacji wykresu z zadanego okresu czasu. |
|  | **Raport pielęgniarski:** |
|  | Możliwość wyświetlenia statystyki ruchu chorych w ramach danej zmiany pielęgniarskiej w zakresie ilości pacjentów: |
| 135. | na oddziale, |
| 136. | przyjęci do szpitala, |
| 137. | przyjęci z innego oddziału, |
| 138. | wypisani, |
| 139. | zmarli. |
| 140. | Możliwość ewidencji wpisów dotyczących pacjentów w ramach danej zmiany pielęgniarskiej. |
| 141. | Możliwość ewidencji uwag ogólnych niezwiązanych z pacjentami. |
| 142. | Możliwość podglądu raportów pielęgniarskich z poszczególnych zmian pielęgniarskich. |
| 143. | Możliwość wydrukowania raportu pielęgniarskiego. |
|  | **Zalecenia pielęgniarskie:** |
| 144. | Możliwość ewidencji zaleceń pielęgniarskich z podziałem na zalecenia pielęgnacyjne, dietetyczne oraz inne wskazania. |
| 145. | Możliwość dodawania podpowiedzi dla poszczególnych zaleceń. |
| 146. | Możliwość korzystania z zestawów zaleceń - gotowych szablonów podpowiedzi w zakresie zaleceń pielęgnacyjnych, dietetycznych oraz innych wskazań. |
| 147. | Możliwość wydrukowania zaleceń pielęgniarskich dla pacjenta. |
|  | **Podgląd dokumentacji pielęgniarskiej:** |
| 148. | Moduł prezentuje w formie osi czasu listę wykonanych czynności pielęgniarskich oraz innych wpisów dokumentacji pielęgniarskiej. |
| 149. | Moduł prezentuje listę dostępnych formularzy dot. dokumentacji pielęgniarskiej. |
|  | **Użytkownik systemu ma możliwość przeglądania dokumentacji pielęgniarskiej w minimum w poniższym zakresie, jeżeli dane występują w HIS:** |
| 150. | karty parametrów życiowych, |
| 151. | realizacji opieki, |
| 152. | karty indywidualnej opieki, |
| 153. | karty gorączkowej, |
| 154. | profilaktyki odleżyn, |
| 155. | pielęgnacji odleżyn, |
| 156. | gospodarki wodnej, |
| 157. | ewidencji wkłuć. |
| 158. | Istnieje możliwość prezentacja na poziomie osi czasu. |

Pulpit Rejestracyjny

|  |  |
| --- | --- |
| **Lp.** | **Opis funkcjonalności** |
|  | Możliwość tworzenia szablonu usługi z wykorzystaniem zasobów oraz atrybutów w tym:   * jednostka organizacyjna, * personel medyczny, * aparat medyczny, * badanie diagnostyczne, * płatnik, * procedura medyczna, * czas pracy, * czas trwania usługi (min), * limit przyjęć, * procedura rozliczeniowa, * program leczenia, * rodzaj wizyty. |
|  | Definiowanie okresu obowiązywania szablonu usług. |
|  | Podczas tworzenia nowego szablonu jest możliwość skopiowania szablonu z istniejącego szablonu. |
|  | Możliwość definiowania harmonogramu usług dla jednostki organizacyjnej. |
|  | Możliwość tworzenia harmonogramu usług na podstawie szablonu usług. |
|  | Tworzenie planu tygodnia pracy dla wskazanej usługi określając:   * dzień tygodnia, * zakres czasu, * czas trwania świadczenia w minutach, * liczbę stanowisk, * limit dzienny. |
|  | Możliwość rozpisania harmonogramu usługi we wskazanych datach. |
|  | Możliwość wyszukania terminu usługi na podstawie:   * danej usługi, * kodu eSkierowania. |
|  | Prezentacja wolnych terminów w postaci listy dostępnych terminów. |
|  | Prezentacja wolnych terminów w postaci widoku kalendarza z dostępnym widokiem tygodniowym i dla poszczególnych dni. |
|  | Możliwość wyboru wolnego terminu na liście terminów. |
|  | Możliwość wyboru wolnego terminu na kalendarzu. |
|  | Po wyborze terminu planowanej usługi możliwość wyszukania pacjenta. |
|  | Możliwość wyszukania pacjenta po numerze PESEL lub nazwisku lub imieniu oraz po danych z eSkierowania. |
|  | Przed wyborem pacjenta z listy jest możliwość podglądu danych z kartoteki pacjenta. |
|  | Możliwość dodania nowej kartoteki pacjenta podczas rezerwacji terminu. |
|  | Możliwość planowania wizyt pacjentów na termin w rozpisanych harmonogramie. |
|  | Rezerwacja wizyty w poradni według wcześniej zdefiniowanego planu. |
|  | Tworzenie nowej rezerwacji w poradni. |
|  | Możliwość planowania pacjentów poza limitem. |
|  | Definiowanie oraz obsługa zastępstw poszczególnych lekarzy. |
|  | Możliwość dodawania blokad i notatek na kalendarzu. |
|  | Możliwość dodawania nowej kartoteki pacjenta. |
|  | Możliwość ewidencji szczegółowych danych dotyczących skierowania pacjenta na wizytę do poradni. |
|  | Możliwość zapisania pacjenta na usługę na podstawie eSkierowania. |
|  | Możliwość zaewidencjonowania skierowania z jednostek kierujących wewnętrznych oraz zewnętrznych. |
|  | Zapisywanie pacjentów na wizytę do poradni wraz z wpisem do harmonogramu przyjęć. |
|  | System umożliwia Elektroniczną Weryfikację Uprawnień Świadczeniobiorców. |
|  | Przyjęcie pacjenta z rozróżnieniem płatnika za konkretną usługę:   * NFZ, * pacjent opłaca samodzielnie, * kontrahent komercyjny. |
|  | Możliwość wprowadzenia informacji o trybie przyjęcia podczas rezerwacji usługi. |
|  | Możliwość przełożenia wizyty na wolny termin w harmonogramie. |
|  | System podpowiada pierwszy wolny termin podczas wyszukiwania terminu. |
|  | Możliwość ewidencji szczegółowych danych podczas rezerwacji wizyty:   * dane dotyczące skierowania, * rozpoznanie ze skierowania, * program leczenia, * kod świadczenia, * uwagi do wizyty. |
|  | Możliwość przyjęcia pacjenta na podstawie karty diagnostyki i leczenia onkologicznego (DiLO) z możliwością dodania numeru karty DiLO. |

Pulpit Bloku operacyjnego

|  |  |
| --- | --- |
| **LP.** | **WYMAGANIA PODSTAWOWE** |
|  | Moduł możliwa personelowi medycznemu dostęp do najważniejszych elementów związanych ze zlecaniem i realizacją zabiegów operacyjnych oraz dokumentacji medycznej wielu pacjentów odwzorowując metodykę pracy użytkownika. |
|  | Możliwość definicji ustawień domyślnych dla wybranego bloku / saliw obszarach: |
|  | Domyślny kontekst pracy, |
|  | Domyślne typy zdarzeń dla historii choroby, |
|  | Domyślny zakres czasowy dla historii chorób. |
|  | Aplikacja posiada menu górne, które zawiera co najmniej następujące pozycje: |
|  | Zabiegi, |
|  | Dokumenty - Lista dokumentów EDM z możliwością wyświetlenia ilości dokumentów do podpisania. |
|  | Zadania - podgląd podstawowych zadań do wykonania przez lekarza wygenerowanych na podstawie konfiguracji systemu: |
|  | Uzupełnienie Okołooperacyjnej Karty Kontrolnej dla zabiegów z datą przeszłą, |
|  | Uzupełnienie wszystkich wymaganych elementów realizacji zabiegu i jego zakończenie (wykonanie) dla zabiegów z datą przeszłą. |
|  | Moduł wykorzystuje tzw. pływający przycisk (ang. floatingbutton), który słóży do szybkiego wywoływania akcji w systemie. |
|  | Moduł umożliwia użytkownikom pracę w 2 wariantach w zależności od wybranej jednostki organizacyjnej: |
|  | Możliwość zagregowania danych z wszystkich sal operacyjnych w ramach jednego bloku. |
|  | Możliwość podglądu danych dotyczących zabiegów w wybranej sali operacyjnej. |
|  | Możliwość prezentacji wykazu pacjentów na bloku / sali z możliwością przełączania się między trybami: duża lista, mała lista. |
|  | **WYMAGANIA DOTYCZĄCE KONTEKSTU ZABIEGÓW MAŁEJ LISTY** |
|  | Prezentacja danych aktualnie wybranego pacjenta i pobytu w zakresie: |
|  | nr w wykazie głównym (księdze), |
|  | nr w wykazie oddziałowym (księdze), |
|  | nazwisko, |
|  | imię, |
|  | PESEL, |
|  | płeć, |
|  | wiek, |
|  | dane adresowe, |
|  | sala, |
|  | łóżko, |
|  | aktualny status weryfikacji eWUŚ, |
|  | rozpoznanie zasadnicze ICD10, |
|  | grupa krwi, |
|  | specjalne statusy pacjenta, |
|  | alergie, |
|  | data przyjęcia, |
|  | doba i godzina pobytu |
|  | lekarz prowadzący, |
|  | Prezentacja skróconego widoku listy zabiegów z danymi: |
|  | nazwisko i imię pacjenta |
|  | PESEL lub data rodzenia (jeśli pacjent nie posiada numeru PESEL). |
|  | symbol i nazwa procedury zaplanowanej- dla zabiegów w statusie innym niż wykonany, |
|  | symbol i nazwa procedury wykonanej- dla zabiegów w statusie wykonany, |
|  | data zabiegu planowana-dla zabiegów w statusie innym niż wykonany, |
|  | data zabiegu faktyczna - dla zabiegów w statusie wykonany, |
|  | status zabiegu, |
|  | informacja o trybie leczenia, |
|  | informacja o istnieniu opisu przedoperacyjnego. |
|  | Moduł umożliwia wyszukiwanie zabiegów na liście minimum według następujących filtrów: |
|  | Nazwisko, imię, PESEL, |
|  | Zabiegi: |
|  | Dzisiaj - prezentujący wszystkie zabiegi z planowaną bądź faktyczną datą realizacji zabiegu równą dacie aktualnej, |
|  | Zaplanowane - prezentujący wszystkie zabiegi które zostały zaplanowane i niezrealizowane, |
|  | Wszystkie - wyświetla wszystkie zabiegi. |
|  | Tylko moi pacjenci - prezentuje zabiegi, gdzie zalogowany personeljest wskazany jako lekarz kierujący, prowadzący lub jako członek zespołu operacyjnego, |
|  | nr w wykazie bloku, |
|  | nr w wykazie oddziału, |
|  | planowana data zabiegu od, |
|  | planowana data zabiegu do, |
|  | faktyczna data zabiegu od, |
|  | faktyczna data zabiegu do, |
|  | sala operacyjna, |
|  | tryb zabiegu, |
|  | operator, |
|  | anestezjolog, |
|  | Moduł umożliwia sortowanie zabiegów na liście minimum według następujących kryteriów: |
|  | nr w wykazie bloku, |
|  | nr w wykazie oddziału, |
|  | nazwisko i imię pacjenta, |
|  | sala operacyjna, |
|  | planowana data zabiegu, |
|  | faktyczna data zabiegu. |
|  | Moduł umożliwia grupowanie zabiegów na liście minimum według następujących kryteriów: |
|  | sala operacyjna, |
|  | planowana data zabiegu, |
|  | faktyczna data zabiegu, |
|  | lekarz kierujący. |
|  | System prezentuje historię leczenia pacjenta w układzie chronologicznym, w postacji rozwijanego drzewa. |
|  | Możliwość filtrowania danych ze względu na: |
|  | rodzaj zdarzeń medycznych (np. zabiegi, wyniki laboratoryjne, diagnostyczne, obserwacje) |
|  | czas wystąpienia zdarzenia. |
|  | Możliwość przejścia do szczegółów zlecenia i realizacji zabiegów: |
|  | dla statusówedytowany, wysłany możliwość otwarcia karty zabiegu chirurgicznego na zakładce Planowanie |
|  | dla statusów przyjęty, wykonany możliwość otwarcia karty zabiegu chirurgicznego na zakładce Realizacja |
|  | **WYMAGANIA DOTYCZĄCE KONTEKSTU ZABIEGÓW DUŻEJ LISTY** |
|  | Możliwość wyszukiwania zabiegów na liście według następujących filtrów: |
|  | Nazwisko, imię, PESEL, |
|  | Zabiegi: |
|  | Dzisiaj - prezentujący wszystkie zabiegi z planowaną bądź faktyczną datą realizacji zabiegu równą dacie aktualnej, |
|  | Zaplanowane - prezentujący wszystkie zabiegi które zostały zaplanowane i niezrealizowane, |
|  | Wszystkie - wyświetla wszystkie zabiegi. |
|  | Tylko moi pacjenci - prezentuje zabiegi, gdzie zalogowany personeljest wskazany jako lekarz kierujący, prowadzący lub jako członek zespołu operacyjnego, |
|  | planowana data zabiegu od-do, |
|  | faktyczna data zabiegu od-do, |
|  | sala operacyjna, |
|  | status zabiegu, |
|  | tryb zabiegu, |
|  | kod icd10, |
|  | operator, |
|  | anestezjolog, |
|  | asysta, |
|  | procedura. |
|  | Pulpit prezentuje listę zabiegów w postaci tabeli z danymi: |
|  | nr w wykazie bloku, |
|  | nazwisko, imię, PESEL, |
|  | data planowana, |
|  | procedura główna, |
|  | kod icd10, |
|  | sala operacyjna, |
|  | status zabiegu, |
|  | tryb zabiegu, |
|  | operator, |
|  | opis przedoperacyjny. |
|  | Dla kolumn wyświetlających ograniczoną ilość danych istnieje możliwość zaprezentowania szczegółowych informacji. |
|  | Możliwość sortowania po wybranych kolumnach z listą zabiegów. |
|  | System umożliwia przejście do szczegółów zlecenia i realizacji zabiegu, w zależności od statusu: |
|  | otwiera kartę zabiegu chirurgicznego na zakładce Planowanie (dla statusów: edytowany, wysłany), |
|  | otwiera kartę zabiegu chirurgicznego na zakładce na zakładce Realizacja (dla statusów: przyjęty, wykonany). |
|  | Moduł umożliwia wydruk co najmniej następujących raportów: |
|  | Księga/wykazbloku operacyjnego, |
|  | Plan zabiegów. |
|  | Możliwość dodania zlecenia nowego zabiegu dla aktualnych pobytów. |
|  | formularz nowego zabiegu wyświetla listę aktualnych, pogrupowanych (wg jednostki) pobytów pacjentów w jednostkach typu oddział, SOR oraz IP do których użytkownik ma dostęp, |
|  | Możliwość sprawdzenia czy istnieje niezrealizowane zlecenie zabiegu dla wskazanego pobytu: |
|  | W przypadku gdy w systemie istnieje niezrealizowane zlecenie system otwiera kartę nowego zlecenia zabiegu chirurgicznego. |
|  | Możliwość wykorzystania czytników kodów kreskowych. |
|  | Możliwość sprawdzenie czy w systemie istnieje zabieg o statusie innym niż Wykonany |
|  | Możliwość wyświetlenia komunikatu o nieznalezieniu zabiegów dla danego pobytu. System umożliwia utworzenie nowego zlecenia. |
|  | Możliwość wyświetlenia karty z danym pobytem i zabiegiem. System umożliwia przekazanie pacjenta między miejscami / pomieszczeniami w zakresie: |
|  | miejsca przekazania (np.. sala operacyjna, blok, śluza przedoperacyjna, sala wybudzeń), |
|  | daty i godziny przekazania, |
|  | nazwiska, imienia i numeru pracownika przekazującego pacjenta, |
|  | nazwiska, imienia i numeru pracownika odbierającego pacjenta, |
|  | prezentacji w formie tabeli całej historii przepływu pacjenta w ramach wybranego zabiegu |
|  | **ROZBUDOWANE WYMAGANIA DOTYCZĄCE EKRANÓW SZCZEGÓŁOWYCH W ZINTEGROWANYM MODULE BLOKU OPERACYJNEGO** |
|  | **Zabiegi chirurgiczne:** |
|  | Moduł prezentuje listę zleconych oraz wykonanych zabiegów chirurgicznych. |
|  | Możliwość ewidencji danych przy zleceniu: |
|  | planowane procedury, |
|  | zespół operacyjny z możliwością wskazania pracownika oraz funkcji jaką będzie on pełnił przy danym zabiegu, |
|  | planowana data i godzina zabiegu, |
|  | planowana sala operacyjna, |
|  | nr zabiegu, |
|  | lekarz kierujący, |
|  | lekarz kwalifikujący, |
|  | rozpoznanie przedoperacyjne, |
|  | rodzaj (tryb) leczenia, |
|  | zgoda na leczenie, |
|  | opis przedoperacyjny - z możliwością wykorzystania szablonów podpowiedzi |
|  | Istnieje możliwość zmiany członka zespołu przypisanego do danej roli bez konieczności usuwania i dodawania wpisu. |
|  | Istnieje możliwość szybkiego przypisania zalogowanego użytkownika do funkcji pełnionej przy zabiegu bez konieczności otwierania i przeszukiwania całej listy (np. przyciskiem). Pracownik może zostać przypisany do danej funkcji tylko jeśli może ją pełnić. |
|  | Istnieje możliwość zlecenia reoperacji w oparciu o poprzednio wykonany zabieg. |
|  | Istnieje możliwość zlecenia zabiegu grupowego na podstawie wcześniej utworzonego zlecenia zabiegu. |
|  | Moduł umożliwia ewidencję co najmniej następujących danych przy realizacji zabiegu: |
|  | czas trwania znieczulenia - automatycznie aktualizowany przy dodawaniu i modyfikacji czasów związanych z poszczególnymi rodzajami znieczuleń, |
|  | czas trwania zabiegu, |
|  | całkowity czas na bloku - automatycznie aktualizowany przy dodawaniu i modyfikacji czasów związanych z przepływem pacjenta pomiędzy salami/miejscami w trakcie trwania zabiegu, |
|  | zgoda na leczenie, |
|  | nr w wykazie bloku - nadawany ręcznie lub automatycznie zgodnie z konfiguracją, |
|  | nr w wykazie oddziału - nadawany ręcznie lub automatycznie zgodnie z konfiguracją, |
|  | rodzaj znieczulenia, |
|  | opis znieczulenia - ręcznie lub z wykorzystaniem szablonów, |
|  | czas trwania poszczególnych rodzajów znieczulenia - ewidencja czasów znieczuleń powinna aktualizować "czas trwania znieczulenia" |
|  | system może dopisywać automatycznie procedury anestezjologiczne powiązane z wybranym rodzajem znieczulenia, |
|  | rodzaj operacji, |
|  | rodzaj zabiegu operacyjnego, |
|  | dawka naświetlania, |
|  | czas naświetlania, |
|  | opis zabiegu- ręcznie lub z wykorzystaniem szablonów, |
|  | rozpoznanie pooperacyjne, |
|  | zrealizowane procedury wraz z określeniem ich rodzaju (Główna, dodatkowa, anestezjologiczna), symbolu, nazwy, realizatora oraz czasu trwania, |
|  | członkowie zespołu operacyjnego wraz z określeniem ich funkcji, pracownika oraz czasu obecności przy zabiegu, |
|  | zużycie środków (leków i materiałów) zużytych na pacjenta w trakcie zabiegu, |
|  | Możliwość ewidencji powikłań / skutków ubocznych w zakresie: |
|  | typ (chirurgicznie/anestezjologiczne), |
|  | opis, |
|  | data i godzina wystąpienia. |
|  | Możliwość ewidencjonowania przepływu pacjenta w zakresie: |
|  | miejsce przekazania, |
|  | data i godzina przekazania, |
|  | osoba przyjmująca, |
|  | osoba przekazująca, |
|  | historia przepływu w ramach bieżącego zabiegu. |
|  | Możliwość jednoczesnego uzupełniania różnych danych na karcie realizacji zabiegu przez kilku użytkowników. |
|  | System posiada mechanizm walidacji uniemożliwiający wykonanie zabiegu bez uzupełnienia wszystkich, obligatoryjnych danych. |
|  | Istnieje możliwość zmiany członka zespołu przypisanego do danej roli bez konieczności usuwania i dodawania wpisu. |
|  | Istnieje możliwość zmiany członka zespołu przypisanego do danej procedury bez konieczności usuwania i dodawania wpisu. |
|  | Istnieje mechanizm szybkiego przypisania czasu trwania procedury na podstawie jednego z trzech wprowadzonych czasów: Czasu zabiegu, Czasu na bloku bądź Czasu znieczulenia. |
|  | Istnieje mechanizm szybkiego przypisania czasu trwania znieczulenia na podstawie jednego z trzech wprowadzonych czasów: Czasu zabiegu, Czasu na bloku bądź Czasu znieczulenia. |
|  | Istnieje mechanizm szybkiego przypisania czasu obecności przy zabiegu wybranego pracownika na podstawie jednego z trzech wprowadzonych czasów: Czasu zabiegu, Czasu na bloku bądź Czasu znieczulenia. |
|  | Istnieje możliwość uzupełnienia Okołooperacyjnej Karty Kontrolnej. |
|  | Istnieje możliwość szybkiego wywołania karty historia leczenia (np. dedykowanym przyciskiem). |
|  | Istnieje możliwość szybkiego wywołania karty umożliwiającej przechwycenie zdjęć lub wideo z podłączonego urządzenia (np. dedykowanym przyciskiem). |

Pulpit Ordynacji leków

|  |  |
| --- | --- |
| **LP.** | **WYMAGANIA DOTYCZĄCE ZLECEŃ LEKARSKICH** |
| 1. | Możliwość filtrowania wg rodzaju zlecenia. |
| 2. | Możliwość sortowania zleceń wg opisu zlecenia, daty planowanej realizacji oraz daty wystawienia. |
| 3. | Możliwość prezentacji odpowiednich statusów realizacji zlecenia za pomocą znaków graficznych lub kolorów. |
| 4. | Możliwość wybory leków z receptariusza oddziałowego. |
| 5. | Możliwość zlecania leków recepturowych zdefiniowanych w module Apteka. |
| 6. | Możliwość zlecania leków spoza receptariusza. |
| 7. | Możliwość zawężenia listy leków do stanów magazynowych jednostki, apteki. |
| 8. | Możliwość weryfikacji, czy dany lek jest dostępny na stanach magazynowych w innych jednostkach. |
| 9. | Możliwość zlecania leków na poziomie nazwy handlowej dostępnej w receptariuszu. |
| 10. | Możliwość zlecania leków po nazwie handlowej lub poprzez wyszukanie nazwy międzynarodowej. |
| 11. | Możliwość zlecania w trybie zwykłym,do decyzji lekarza. |
| 12. | Możliwość zlecenia podania doraźnego, premedykacji zabiegowej. |
| 13. | Możliwość przeglądania wszystkich zleceń lekarskich pacjenta z możliwością wybrania zakresu aktualnej hospitalizacji, aktualnego pobytu/wizyty. |
| 14. | Możliwość określenia daty i godziny realizacji zlecenia. |
| 15. | Możliwość wyznaczenia terminu podania zlecenia na podstawie interwału i predefiniowanego schematu. |
| 16. | Możliwość ewidencjonowania dodatkowych środków w ramach jednego zlecenia lekowego. |
| 17. | Możliwość podglądu szczegółów zlecenia. |
| 18. | Możliwość przedłużania, odstawianie oraz anulowanie zleceń. |
| 19. | Możliwość przywrócenia odstawionych zleceń. |
| 20. | Możliwość zlecania "pakietów leków", czyli predefiniowanych grup leków składowanych pod jedną nazwą np. przedoperacyjny. |
| 21. | Możliwość oznaczenia zlecenia leków pacjenta. |
| 22. | Możliwość ewidencji uwag do zlecenia. |
| 23. | Możliwość podglądu interakcji między lekami (przy wykupionej licencjiBLOZ interakcje) |
| 24. | Możliwość kopiowania zbiorczego zleceń z poprzednich pobytów/wizyt. |
| 25. | Możliwość kopiowaniazleceń ze wskazanego dnia |
| 26. | Możliwość grupowego przedłużania zleceń. |
| 27. | Możliwość grupowego anulowania zleceń. |
| 28. | Możliwość wysłania żądania anulowania zlecenia o statusieprzyjęte |
| 29. | Możliwość wydrukowaniaIndywidualnej karty zleceń lekarskich z określonego przedziału czasowego. |
| 30. | Możliwość zlecenia podania gazów medycznych; |
| 31. | Możliwość zlecenia wlewów, wlewów ciągłych. |
| 32. | Możliwość definiowania zmian przepływu dla wlewów. |
| 33. | Możliwość zlecania środków dodatkowych również w trakcie trwania wlewu ciągłego. |
| 34. | Możliwość zlecenia leków wydawanych pacjentowi do domu przez Aptekę Szpitalną wraz z mechanizmem automatycznego zużycia środków na pacjenta. |
| 35. | Możliwość zlecenia leków wydawanych pacjentowi do domu przez jednostkę realizująca świadczenie. |
| 36. | Możliwość prezentacji zleceń w ujęciu: dzień, 4 dni, 7 dni; |
| 37. | Możliwość weryfikacji alergenów podczas ordynacji leków. |
| 38. | Możliwość prezentacji leków wedługpredefiniowanych grup analitycznych w module Apteka. |
| 39. | Możliwość prezentacji zleceń tylko aktualnych, które są zaplanowane od dziś w przyszłość. |
| 40. | Możliwość wyboru wariantu programu lekowego na podstawie EAN-13 oraz zakontraktowanej dla danej jednostki umowy. |
| 41. | Prezentacji zleceń na osi czasu. |
| 42. | Możliwość dla określonej grupy analitycznej leków np.: antybiotyki, ordynowania zlecenia tylko pod warunkiem wskazania wyniku badania mikrobiologicznego. |
|  | **WYMAGANIA DOTYCZĄCE REALZIACJI ZLECEŃ LEKARSKICH** |
| 1. | Możliwość zbiorczego przyjmowania zleceń przez personel pielęgniarski. |
| 2. | Możliwość wyświetlenia zleceń lekowych z określonego zakresu czasu - dyżuru, dla konkretnego pacjenta i dla konkretnej sali, na której leżą pacjenci. |
| 3. | Moduł umożliwia ewidencjonowanie uwag dotyczących realizacji zlecenia. |
| 4. | Moduł umożliwia zamknięcie zlecenia lekowego bez jego realizacji. W tej sytuacji powód niemożliwości realizacji zlecenia musi być bezwzględnie określony, wyjątkiem jest status 'żądanie anulowania' zaewidencjonowany przez lekarza. |
| 5. | Możliwość prezentacji zleceń z podziałem na :leki,wlewy i gazy medyczne, leczenie żywieniowe, procedury. |
| 6. | Możliwość pojedynczejrealizacji zleceń wraz z zużyciem leku. |
| 7. | Prezentacja zleceń na osi czasu. |
| 8. | Możliwość prezentacji odpowiednich statusów realizacji zlecenia za pomocą znaków graficznych lub kolorów. |
| 9. | System prezentuje zlecenia do realizacji o statusach:nowe, przyjęte, w trakcie wlewu, żądanie anulowania. |
| 10. | Możliwość identyfikacji pacjenta po imieniu, nazwisku i peselu. |
| 11. | Prezentacja uwag lekarskich podczas przyjmowania i realizacji zlecenia. |
| 12. | Możliwość ewidencji żużycia środków podczas realizacji zlecenia. |

Wyniki i opisy badań histopatologicznych

|  |  |
| --- | --- |
| **Lp.** | **Opis funkcjonalności** |
|  | Możliwość podłączenia do centralnej platformy eZdrowie( P1) w zakresie zapisu dokumentu wyniku histopatologicznego. |
|  | Możliwość wygenerowania dokumentu wyniku histopatologiczne zgodnego z HL7 CDA. |
|  | Możliwość podpisania dokumentu wyniku histopatologicznego z wykorzystaniem sposobu potwierdzania pochodzenia oraz integralności danych dostępnego w systemie teleinformatycznym udostępnionym bezpłatnie przez Zakład Ubezpieczeń Społecznych tzw. certyfikat ZUS. |
|  | Możliwość wysłania dokumentu wyniku histopatologicznego do Centralnej Bazy Histopatologicznej. |
|  | Możliwość anulowania dokumentu wyniku histopatologicznego w Centralnej Bazie Histopatologicznej. |
|  | Możliwość wydruku dokumentu wyniku histopatologicznego. |

Wyniki i opisy badań cytologicznych

|  |  |
| --- | --- |
| **Lp.** | **Opis funkcjonalności** |
|  | Możliwość podłączenia do centralnej platformy eZdrowie( P1) w zakresie wysłania dokumentu wyniku cytologicznego. |
|  | Możliwość wygenerowania dokumentu wyniku cytologicznego zgodnego z HL7 CDA. |
|  | Możliwość podpisania dokumentu wyniku cytologicznego z wykorzystaniem sposobu potwierdzania pochodzenia oraz integralności danych dostępnego w systemie teleinformatycznym udostępnionym bezpłatnie przez Zakład Ubezpieczeń Społecznych tzw. certyfikat ZUS. |
|  | Możliwość wysłania dokumentu wyniku cytologicznego do Centralnej Bazy Histopatologicznej. |
|  | Możliwość wysłania anulowania dokumentu wyniku cytologicznego w Centralnej Bazie Histopatologicznej. |
|  | Możliwość standardowego wydruku dokumentu wyniku cytologicznego. |

Karta diagnostyki i leczenia onkologicznego - e-DILO

|  |  |
| --- | --- |
| **Lp.** | **Opis funkcjonalności** |
|  | Możliwość ewidencji danych związanych z elektroniczną kartą diagnostyki i leczenia onkologicznego (e-DILO) w modułach źródłowych. |
|  | Możliwość wysłania danych związanych z e-DILO na platformę P1. |
|  | Możliwość odczytu danych związanych z e-DILO z platformy P1. |

Plan leczenia onkologicznego

|  |  |
| --- | --- |
| **Lp.** | **Opis funkcjonalności** |
|  | Możliwość ewidencji danych związanych z planem leczenia onkologicznego. |
|  | Możliwość wysłania danych związanych z planem leczenia onkologicznego na platformę P1. |
|  | Możliwość odczytu danych związanych z e-KOK z platformy P1. |

PatientSummary (karta zdrowia pacjenta)

|  |  |
| --- | --- |
| **Lp.** | **Opis funkcjonalności** |
|  | Możliwość podłączenia do centralnej platformy eZdrowie( P1) w zakresie pobierania dokumentu PatientSummary. |
|  | Możliwość pobrania dokumentu PatientSummary w formacie PDF. |
|  | Możliwość wydruku dokumentu PatientSummary. |
|  | Możliwość podglądu dokumentu PatientSummary bezpośrednio z systemu HIS. |
|  | Ostateczny zakres dokumentu możliwy do pobrania określa CeZ. |

Karta opieki kardiologicznej (e-KOK)

|  |  |
| --- | --- |
| **Lp.** | **Opis funkcjonalności** |
|  | Możliwość ewidencji danych związanych z kartą opieki kardiologicznego (e-KOK). |
|  | Możliwość wysłania danych związanych z e-KOK na platformę P1. |
|  | Możliwość odczytu danych związanych z e-KOK z platformy P1. |

RZM API

|  |  |
| --- | --- |
| **Lp.** | **Opis funkcjonalności** |
|  | Możliwość przyjęcia z systemu zewnętrznego dokumentu wyniku laboratoryjnego w formacie HL7CDA wraz z zapisaniem tych dokumentów w repozytorium EDM. |
|  | Możliwość przyjęcia z systemu zewnętrznego dokumentu wyniku diagnostycznego w formacie HL7CDA wraz z zapisaniem tych dokumentów w repozytorium EDM. |
|  | Możliwość przyjęcia wyłącznie wyników wysyłanych w ramach działającej integracji HL7, w której przesyłane są dokumenty XML oraz PDFpodpisane podpisem elektronicznym. W skład dokumentów nie wchodzą wyniki histopatologiczne, które mają indywidualną integrację w ramach platformy P1. |
|  | Możliwość wygenerowania indeksu dokumentu wyniku otrzymanego w ramach punktu pierwszego. |
|  | Możliwość zapisania indeksu dokumentu elektronicznego w ramach platformy P1. |
|  | Możliwość podglądu dokumentu wstawionego z użyciem RZM EXT API w systemie HIS i możliwy do podglądu w ramach kontekstu danego świadczenia pacjenta. |

EDM Gateway

|  |  |
| --- | --- |
| **Lp.** | **Opis funkcjonalności** |
|  | Możliwość dodania dokumentu elektronicznego zgodnego z HL7 CDA dla danego pacjenta za pomocą dedykowanego API. |
|  | Możliwość eksportu dokumentów elektronicznych danego pacjenta za zadany okres czasu za pomocą dedykowanego API. |
|  | Możliwość pobrania listy dokumentów EDM do pobrania. |
|  | Możliwość pobrania konkretnych dokumentów EDM na podstawie listy dokumentów do pobrania. |
|  | Import oraz eksport dokumentów odbywa się z wykorzystaniem profilu IHE XDS.b (Cross-Enterprise DocumentSharing) |
|  | Dokument EDM dodany za pomocą API widoczny w systemie HIS w kontekście danego pacjenta. |

Wieloskładnikowe uwierzytelnianie (MFA)

|  |  |
| --- | --- |
| **Lp.** | **Opis funkcjonalności** |
|  | System umożliwia wykorzystanie protokołu OpenID Connect. |
|  | System umożliwia wieloskładnikowe uwierzytelnianie (MFA) z użyciem jednorazowych haseł OTP. |
|  | System umożliwia generowanie jednorazowych haseł z wykorzystaniem mobilnych aplikacji (np. Google Authenticator, Microsoft Authenticator). |
|  | System umożliwia wymuszenie skonfigurowania wieloskładnikowego uwierzytelniania dla użytkownika przy pierwszej próbie zalogowania |
|  | System umożliwia skonfigurowanie kodów zapasowych do odzyskiwania dostępu. |
|  | System umożliwia pozyskanie informacji o kontach użytkowników bezpośrednio z bazy danych HIS Eskulap. |
|  | System umożliwia integrację kont z LDAP / Active Directory. |
|  | System umożliwia jednokrotne uwierzytelnianie (SSO) pomiędzy wersjami systemu HIS Eskulap. |
|  | System umożliwia audyt zdarzeń wieloskładnikowego uwierzytelniania. |
|  | System umożliwia blokowanie dostępu po określonej liczbie nieudanych prób skorzystania z OTP. |

1. Zakres przedmiotowy Etap IV – Dostawa i instalacja Infrastruktury IT
2. Przedmiotem etapu jest dostawa i instalacja Infrastruktury IT u Zamawiającego.

Poniżej wyspecyfikowano minimalne parametry Infrastruktury IT, które należy dostarczyć w ramach realizacji Etapu. W przypadku, gdy nie określono, że parametr określa maksymalną wartość jest to jego wartość minimalna.

1. Wymagania ogólne:

* Całość dostarczanego sprzętu musi pochodzić z autoryzowanego kanału sprzedaży producenta.
* Całość dostarczanego rozwiązania, tzn. każde z dostarczonych urządzeń, musi być nowe, wcześniej nieużywane, rok produkcji nie starszy niż 2025.
* Całość dostarczanego rozwiązania, tzn. każde z dostarczonych urządzeń, w którym nie wskazano warunków gwarancji, musi być objęte gwarancją w okresie minimum 36 miesięcy
* Urządzenia i ich komponenty muszą być oznakowane przez producentów w taki sposób, aby możliwa była identyfikacja zarówno produktu, producenta, jak i daty produkcji danego elementu.
* Do każdego urządzenia musi być dostarczony komplet standardowej dokumentacji dla użytkownika w formie papierowej lub elektronicznej w języku polskim lub angielskim.
* Do każdego urządzenia musi być dostarczony niezbędny sprzęt eksploatacyjny (przewody zasilające, przewody sygnałowe itp.) niezbędny do uruchomienia danego urządzenia w budowanym rozwiązaniu w miejscu dostawy wskazanym przez Zamawiającego. Sprzęt, o którym mowa powyżej jest integralną częścią oferty i przechodzi na własność Zamawiającego.
* Wszystkie urządzenia muszą posiadać oznakowanie CE.
* Wszystkie dostarczane urządzenia na dzień złożenia oferty nie mogą być w fazie end-of-life (EOL)
* Wszystkie urządzenia muszą współpracować z siecią energetyczną o parametrach: 230 V ± 10%, 50 Hz.
* Wymagane jest, aby Infrastruktura IT była gotowym produktem posiadającym nazwę handlową i złożonym z zamkniętej, ściśle zdefiniowanej listy komponentów posiadających odpowiednie numery katalogowe.
* Dostarczane oprogramowanie musi zostać dostarczone w najnowszej stabilnej wersji, która uzyskała certyfikację producenta dostarczanego sprzętu (jeśli podlega certyfikacji).

1. Wykonawca w ramach etapu IV zobowiązany jest do wykonania co najmniej następujących usług związanych z montażem i konfiguracją dostarczanej Infrastruktury IT:
2. Wykonanie Projektu Technicznego dostarczanej Infrastruktury sprzętowej, który będzie składał się co najmniej z następujących elementów:
   * Dokładna specyfikacja techniczna wraz z numerami katalogowymi poszczególnych elementów,
   * Nazwy oraz szczegółowej adresacja poszczególnych elementów,
   * Planowana konfiguracja środowiska wraz z połączeniami, konfiguracją poszczególnych elementów w tym logiczną konfiguracją miejsca,
   * Wymagane działania ze strony Zamawiającego w celu poprawnego montażu i konfiguracji,
   * Harmonogram prac.

Projekt techniczny musi zostać wykonany po wcześniejszej analizie środowiska wykonanej przez Wykonawcę oraz musi zostać zaakceptowany przez Zamawiającego.

1. Instalacja oraz konfiguracji oprogramowania.
2. Testy rozwiązania.
3. Instruktaż dla administratorów demonstrujący sposób zarządzania środowiskiem.
4. Dostarczenie dokumentacji powykonawczej infrastruktury sprzętowej, która będzie składała się co najmniej z następujących elementów:
   * Specyfikacja techniczna wraz z numerami katalogowymi poszczególnych elementów oraz numerami seryjnymi poszczególnych elementów,
   * Końcowe nazwy oraz szczegółowa adresacja poszczególnych elementów,
   * Konfiguracja środowiska wraz z połączeniami, konfiguracją poszczególnych elementów w tym logiczną konfiguracją miejsc
   * Komplety poświadczeń do całej infrastruktury – wymagana zmiana haseł domyślnych – dostarczone jako osobny załącznik w postaci zaszyfrowanego pliku kdbx,
   * Dokumentacja techniczna w formie elektronicznej do każdego elementu w języku polskim lub angielskim
   * Szczegóły dotyczące instalacji i uruchomienia infrastruktury sprzętowej, w zakresie modernizacji infrastruktury szpitala, zostaną ustalone pomiędzy Stronami w trakcie Analizy Przedwdrożeniowej.
   * Zamawiający zapewni odpowiedni zapas mocy oraz odpowiednie warunki środowiskowe w komorach serwerowni.
   * Po zakończonym montażu Wykonawca przekaże Zamawiającemu wszystkie hasła dostępowe do kont „super użytkowników”.
6. Opis parametrów minimalnych dostarczanej infrastruktury:
   * + 1. Stacje robocze 200 szt.

|  |  |
| --- | --- |
| **Parametr** | **Minimalne wymagania** |
| Przekątna ekranu | min 23.8'' |
| Rozdzielczość | min 1920 x 1080 (FHD 1080) |
| Ekran dotykowy | Nie |
| Typ matrycy | min TFT IPS |
| Powierzchnia matrycy | min Matowa |
| Rodzina procesora | Procesor min. 6-cio rdzeniowy o taktowaniu bazowym nie niższym niż 2 Ghz |
| Liczba rdzeni | min 6 |
| Liczba wątków | min 10 |
| Zainstalowana pamięć RAM | 16 GB |
| Maks. wielkość pamięci | 64 GB |
| Rodzaj pamięci | DDR5 |
| Częstotliwość szyny pamięci | Min 4800 MHz |
| Typ dysku | SSD |
| Pojemność SSD | 512 GB |
| Model karty graficznej | zintegrowany |
| Porty wideo | 1 x HDMI |
| Interfejs sieciowy | 1 x 10/100/1000 Mbit/s |
| Wi-Fi 802.11a/b/g/n/ac |
| Bluetooth |
| Napęd optyczny | Brak |
| Czytnik kart pamięci | Nie |
| Porty USB | 2 x USB 2.0 Type-A |
| 2 x USB 3.2 Type-A Gen 1 |
| 1 x USB 3.2 Type-C Gen 1 |
| Pozostałe porty we/wy | 1 x Audio (Combo) |
| 1 x RJ-45 |
| Obudowa | All-In-One |
| System operacyjny | min. Windows 11 Pro lub równoważny |
| Akcesoria w zestawie | Mysz kablowa |
| Klawiatura kablowa |

* + - 1. Macierz 1 szt.

|  |  |  |
| --- | --- | --- |
| Lp | Cecha | Opis Wymagań |
|  | Obudowa | Obudowa do montażu w szafie rack 19” za pomocą dostarczonych dedykowanych elementów. Oferowana macierz nie może przekroczyć rozmiaru 4U. Obudowa musi umożliwiać instalację min 24 dysków. |
|  | Zasilanie | Oferowane urządzenie musi być przystosowane do zasilania z sieci AC oraz wyposażone w kable zasilające PDU. Macierz musi być wyposażona w zdublowany, redundantny system zasilania, umożliwiający prawidłową, nieprzerwaną pracę urządzenia w przypadku awarii dowolnego pojedynczego źródła zasilania. |
|  | Redundancja | Macierz nie może posiadać pojedynczego punktu awarii (SPOF), który powodowałby brak dostępu do danych. Wszystkie krytyczne komponenty takie jak kontrolery dyskowe, pamięć, zasilacze i wentylatory muszą być zaprojektowane nadmiarowo. |
|  | Kontrolerydyskowe | Macierz wyposażona w minimum 2 kontrolery pracujące w trybie active-active. Akceptowalna architektura to symmetricactive-active, to znaczy pracę kontrolerów w trybie zapewniającym dostęp do wolumenów logicznych (LUN) utworzonych w macierzy, z wykorzystaniem wszystkich dostępnych ścieżek (path) i portów kontrolerów bez wymuszania preferowanej ścieżki dostępu oraz z zapewnieniem automatycznego równoważenia obciążenia (loadbalancing) pomiędzy kontrolerami. Kontrolery nie mogą być połączone ze sobą zewnętrznym okablowaniem. Muszą wykorzystywać wewnętrzną magistralę gwarantującą najkrótsze opóźnienia. Kontrolery nie mogą pracować w trybie active-passive. |
|  | Wydajność | Macierz w oferowanej konfiguracji w teście wydajnościowym osiągnie min. 100 000 IOPS przy następujących parametrach:  - Zapełnienie macierzy – min. 80% fizycznej pojemności,  - Protokół: FC,  - Porty: 32G,  - Read 80% - blok 8k,  - Write 20% - blok 8k,  - 100% Random  - Read Hit Ratio – max 10%  - Write Hit Ratio – max 10%  - Latency – max 1ms  - RAID 6  - Deduplikacja i kompresja – włączone (dedupratio=2, compratio=2)  Zamawiający ma prawo przeprowadzić test po dostawie macierzy aby sprawdzić czy dostarczone rozwiązanie osiąga deklarowane parametry wydajnościowe. Wydajność średnia nie mniejsza niż 100 000 IOPS uzyskiwana przez co najmniej 180 min testu. Środowisko testowe – serwery wirtualne.Ewentualny test zostanie przeprowadzony ogólnodostępnym narzędziem Vdbench. Wykonawca ma możliwość określenia jedynie wartości parametrów określonych w specyfikacji. Wszystkie inne parametry nie określone w zapytaniu muszą przyjąć wartości domyślne. |
|  | Wymagana przestrzeń | Fizyczna przestrzeń dyskowa zbudowana tylko i wyłącznie za pomocą dysków SSD SAS lub SSD NVMe. Przestrzeń użytkowa po zbudowaniu RAID 6 z min. 1 dyskiem hot-spare lub przestrzenią hot-spare równą pojemności min. 1 dysku musi wynosić min 95 TiB. Ze względów wydajnościowych oraz niezawodnościowych rozmiar pojedynczego dysku nie może być większy niż 8 TB, co przełoży się na większą liczbę dysków. Wymagana pojemność RAW min 130 TB. Wymagana pojemność użytkowa rozumiana jest jako pojemność dostępna po konfiguracji RAID i odliczeniu rezerwy na dyski/przestrzeń *spare* i dostępna dla hostów bez uwzględnienia jakichkolwiek mechanizmów kompresji, czy deduplikacji.  Dyski muszą być wyposażone w podwójne interfejsy.Niedopuszczalne są dyski SSD zbudowane w oparciu o chipset QLC ze względu na skróconą żywotność oraz wydłużone czasy odpowiedzi. |
|  | Zabezpieczenia dyskami SPARE | Możliwość definiowania przez administratora dysków SPARE lub odpowiedniej zapasowej przestrzeni dyskowej. |
|  | Możliwości rozbudowy macierzy | Wymagana możliwość rozbudowy oferowanej macierzy do co najmniej 500 TB przestrzeni użytecznej lub efektywnej, bez wymiany kontrolerów macierzowych oraz bez rozbudowy o dodatkowe kontrolery, tylko poprzez dodawanie półek i dysków SSD SAS lub SSD NVMe. Macierzniemożeobsługiwaćdysków HDD. |
|  | Pamięć Cache | Co najmniej 128GB pamięci cache na całą macierz (dwa kontrolery). Zamawiający niedopuszcza możliwości zastosowania dysków SSD/NVMe lub kart pamięci FLASH jako rozszerzenia pamięci cache.Pamięć cache musi być zabezpieczona przed utratą danych w przypadku awarii zasilania poprzez funkcję zapisu zawartości pamięci cache na nieulotną pamięć. |
|  | Porty front-end | Razem kontrolery muszą udostępnić minimum 4 porty 10G Eth oraz 8 portów 32G FC. Wszystkie moduły muszą posiadać wkładki optyczne SFP+.  Wymagana możliwość rozbudowy o kolejne 8 portów 32G FC tylko poprzez instalację kart sieciowych w oferowanej obudowie macierzy.  Karty sieciowe muszą być hot-swap, tzn umożliwiać wymianę bez konieczności wyjmowania kontrolera ani zatrzymywania dostępu do danych pozostałymi kartami i portami w danym kontrolerze (nie dotyczy wbudowanych portów).  Macierz musi posiadać wbudowane min 4 porty SAS 12Gb/s do podłączenia półek dyskowych SAS lub inne dedykowane do półek dyskowych NVMe. |
|  | Obsługiwane protokoły | Wymagane wsparcie dla FC, iSCSI. |
|  | Obsługiwane typy zabezpieczenia RAID | Kontrolery wyposażone w funkcjonalność konfiguracji poziomu RAID 6 lub równoważnego tolerującego jednoczesną awarię 2 dysków bez utraty danych. |
|  | Zabezpieczenie SPARE | W celu zapewnienia odpowiedniej ochrony danych oraz redukcji czasu odbudowy wymagana jest obsługa rozproszonej przestrzeni spare pomiędzy dyskami. Wymagana możliwość definiowania przez administratora odpowiedniej zapasowej przestrzeni dyskowej. Niedopuszczalne są klasyczne realizacje ochrony danych oparte o grupy dysków RAID, gdzie wymagane jest stosowanie dedykowanych dysków parzystości tzw. paritydrives oraz dedykowanych dysków zapasowych tzw. hot sparedrives. |
|  | Prezentacja dysków logicznych o pojemności większej niż zajmowana przestrzeń dyskowa (ang. Thin Provisioning) | Wymagana funkcjonalność tworzenia i prezentacji dysków logicznych (LUN) o pojemności większej niż zajmowana fizyczna przestrzeń dyskowych (ang. ThinProvisioning). Wymagana funkcjonalność zwrotu skasowanej przestrzeni dyskowej do puli zasobów wspólnych (ang. Space Reclamation). Macierz musi wspierać nie mniej niż 2000 LUNów. Wymagana możliwość tworzenia grup wolumenów. Max liczba LUNów w grupie wolumenów nie może być mniejsza niż 100.  Wymagane dostarczenie w/w funkcjonalności na zainstalowaną przestrzeń dyskową. |
|  | Zarządzanie | Zarządzanie macierzą (wszystkimi kontrolerami) z poziomu pojedynczego interfejsu graficznego. Wymagane jest stałe monitorowanie stanu macierzy w tym monitorowanie wydajności obiektów takich jak:  - cała macierz  - kontrolery  - porty front-end  - porty logiczne  - dyski  - LUNy  - hosty  Pod kątem parametrów takich jak:  - operacje wejścia/wyjścia IOPS  - przepustowość (KB/s lub MB/s)  - czas odpowiedzi (latency)  - zużycie CPU (w % dla kontrolerów)  - trafienia w cache (dla kontrolerów)  Wymagana możliwość monitorowania stanu żywotności dysków SSD SAS. Wymagana możliwość dostępu do historycznych danych wydajnościowych z poziomu GUI macierzy do co najmniej 3 lat wstecz lub jako równoważne dostarczenie fizycznego serwera z oprogramowaniem umożliwiającym zbieranie i przeglądanie danych historycznych.  Wymagana możliwość konfigurowania zasobów macierzy.  Wymagana możliwość tworzenia polityk logowania.  Wymagane wsparcie multi-factorauthentication do logowania się do macierzy.  Wymagany min 1 port 1G Eth per kontroler dedykowany do zarządzania macierzą. |
|  | Kopiewewnątrzmacierzy | Tworzenie na żądanie tzw. migawkowej kopii danych (ang. snapshot) w ramach macierzy do wykorzystania w celu np. wykonywania kopii zapasowych. Snapshoty muszą być wykonywanie w technologii ROW (Redirect On Write). Macierz musi obsługiwać min 2000 snapshotów.  Wymagane wsparcie dla snapshotów kaskadowych.  Musi być możliwość utworzenia harmonogramu snapshotów których nie można modyfikować ani usunąć bez odpowiednich uprawnień celem przywrócenia danych w przypadku ataku ransomware. Funkcjonalność musi umożliwiać określenie okresu ochrony snapshotów.  Tworzenie na żądanie kopii danych typu klon w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Funkcjonalność ta musi umożliwiać synchronizację danych z wolumenu źródłowego na docelowy oraz resynchronizację danych z wolumenu docelowego na źródłowy. |
|  | Replikacjadanych | Możliwość zdalnej replikacji danych typu on-line (bez przerywania prezentacji wolumenów dyskowych) do macierzy tej samej rodziny w trybie asynchronicznym oraz synchronicznym przy wykorzystaniu portów FC. Funkcjonalność ta nie może wpływać na obciążenie serwerów podłączonych do macierzy. |
|  | Deduplikacja i kompresja | Macierz musi wspierać funkcjonalności deduplikacji i kompresji danych. |
|  | Klaster macierzowy | Wsparcie dla technologii klastrowania macierzy dyskowych (ang. Storage Metro Cluster). Macierz musi dostarczać funkcjonalność klastra klasy "wysokiej dostępności" tj. zapewnienia wysokiej dostępności zasobów dyskowych macierzy dla podłączonych platform oprogramowania i sprzętowych z wykorzystaniem synchronicznej replikacji danych po protokole FC pomiędzy 2 macierzami. Pod użytym pojęciem "wysoka dostępność zasobów dyskowych" należy rozumieć zapewnienie bezprzerwowego działania środowiska (aplikacja/system operacyjny/serwer) podłączonego do macierzy (macierz preferowana) w przypadku wystąpienia awarii logicznego połączenia z tą macierzą bądź awarii samej macierzy powodujących dla danego środowiska brak dostępu do zasobów macierzy preferowanej. Funkcjonalność klastra "wysokiej dostępności" pozwala na automatyczne przełączanie obsługi środowisk produkcyjnych z macierzy preferowanej na niepreferowaną w przypadku awarii macierzy preferowanej (tzw. automatedfailover). Wymagany jest również automatyczny failover z macierzy niepreferowanej na preferowaną. Dopuszczalne jest zastosowanie tzw arbitra (serwer quorum). |
|  | Priorytety zadań | Macierz musi posiadać możliwość zapewnienia ciągłości biznesu na oczekiwanym poziomie usług (QoS) poprzez definicję polityk QoS w oparciu o maksymalne progi wydajności IOPS i MB/s. Musi istnieć możliwość określenia polityk QoS na poziomie wolumenów. Dostarczenietejfunkcjonalności jest wymaganenatymetapiepostępowania. |
|  | Licencje | Wymagane jest dostarczenie licencji wieczystych na wszystkie opisane wyżej funkcjonalności. |
|  | Integralność danych | Macierz musi oferować wsparcie dla zachowania integralności danych na całej ścieżce transferu (ang. End-to-End) zgodnego ze standardem/specyfikacją T10 PI. |
|  | Wspierane systemy operacyjne | Wsparcie, dla co najmniej Microsoft Server Windows 2016/2019/2022, VMware 6.x/7.x/8.x, Linux RedHat 7.x/8.x/9.x, CentOS 7.x/8.x |
|  | Certyfikaty | Wymagane jest aby dostarczony system został wyprodukowany przez producenta sprzętu posiadającego: • Certyfikat ISO 9001 dla producenta sprzętu obejmujący proces projektowania i produkcji • Certyfikat ISO 14001 dla producenta sprzętu  • Certyfikat ISO 50001 dla producenta sprzętu • Certyfikat ISO 27001 dla producenta sprzętu |
|  | Serwisowalność | Wymagane uaktualnianie firmware-u kontrolerów macierzy bez przerywania dostępu do danych.  Macierz przystosowana do napraw w miejscu zainstalowania oraz wymiany elementów bez konieczności jej wyłączania.  Macierz musi umożliwiać zdalne zarządzanie.  Urządzenie musibyć fabrycznienowe, wyprodukowanenie wcześniejniż 6 miesięcy przed datądostarczenia doZamawiającego ipochodzić zautoryzowanego kanału dystrybucji producenta w Polsce, a także musi być objęte serwisem producenta lub autoryzowanego partnera serwisowego na terenie RP.  Producent oferowanego urządzenia musi posiadać portal internetowy, gdzie po wpisaniu numeru seryjnego urządzenia można zweryfikować warunki serwisu gwarancyjnego i czas na jaki został udzielony.  Wymagana gwarancja na 3 lata w trybie 9x5 NBD. Uszkodzone dyski pozostają własnością Zamawiającego. |

* + - 1. Serwer Wirtualizacji 2 szt.

Serwer musi spełniać następujące minimalne warunki techniczne i funkcjonalne:

1. obudowa do montażu w szafie typu rack;
2. zasilanie redundantne, przynajmniej 2 zasilacze typu HotPlug;
3. płyta główna z możliwością zainstalowania minimum dwóch procesorów;
4. bazowy zegar procesora minimum 3,65 GHz;
5. zainstalowany 1 procesor minimum 16 - rdzeniowy klasy x86 dedykowany do pracy w serwerach, zaprojektowane do pracy w układach wieloprocesorowych;
6. pamięć minimum 768 GB DDDR5 ECC DIMM, rozszerzalna, z zabezpieczeniem typu: ECC.
7. dyski minimum 2x 460 GB umożliwiające skonfigurowanie RAID 1 ;
8. interfejsy minimum: 1x 1GbE ,4x 10GB sfp+ SR, 2x32GB FC (należy dostarczyć wkładki)
9. z przodu obudowy min: 1x USB 3.0.
10. z tyłu obudowy: 2x USB 3.0, 1x DB-15
11. Zarządzanie:
12. Zintegrowany z płytą główną serwera, niezależny od systemu operacyjnego, sprzętowy kontroler zdalnego zarządzania
13. Monitoring statusu i zdrowia systemu
14. Logowanie zdarzeń
15. Umożliwiający Update systemowego firmware
16. Umożliwiający zdalną konfigurację serwera
17. Monitoring i możliwość ograniczenia poboru prądu
18. Zdalnewłączanie/wyłączanie/restart
19. Przekierowanie konsoli szeregowej przez IPMI
20. Możliwość przejęcia zdalnego ekranu 1920x1200, 60 Hz,16 bpp
21. Zdalny dostęp do serwera
22. Możliwość zdalnej instalacji systemu operacyjnego
23. Alerty Syslog
24. Przekierowanie konsoli szeregowej przez SSH
25. Wyświetlanie danych aktualnych I historycznych dla użycia energii I temperatury serwera
26. Możliwość mapowania obrazów ISO z lokalnego dysku operatora
27. Możliwość mapowania obrazów ISO przez min HTTPS
28. Możliwość jednoczesnej pracy do 6 użytkowników przez wirtualną konsolę
29. Wspierane protokoły/interfejsy: IPMI v2.0, SNMP v3, DCMI v1.5, REST API
30. Możliwość przewidywania awarii dla procesorów, pamięci, dysków wewnętrznych, wentylatorów, zasilaczy, kontrolerów RAID
31. Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA.
32. Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w Unii Europejskiej;
33. Serwerowy System operacyjny + licencje:
34. 2 szt Licencji systemu operacyjnego na 16 rdzeni (per licencję)umożliwiających licencjonowane uruchomienie nielimitowanej ilości systemów operacyjnych OSE w najnowszej wersji zgodnych z posiadanym środowiskiem Active Directory.
35. 100 licencji dostępowych na urządzenie, umożliwiających zarządzanie urządzeniami z poziomu serwera AD za pośrednictwemusługi Active Directory.
36. System Wirtualizacji

Dostawa komercyjnego systemu do wirtualizacji, zgodnym z dostarczanymi rozwiązaniami sprzętowymi oraz systemem backupu.

* 1. Rozwiązanie musi zapewnić możliwość obsługi wielu instancji systemów operacyjnych na jednym serwerze fizycznym i powinno się charakteryzować maksymalnym możliwym stopniem konsolidacji sprzętowej.
  2. Pojedynczy klaster może się składać z min.2 fizycznych hostów
  3. Oprogramowanie do wirtualizacji musi zapewnić możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi
  4. Oprogramowanie do wirtualizacji powinno zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych (tzw. snapshot).
  5. Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy serwerami fizycznymi
  6. System musi posiadać funkcjonalność wirtualnego przełącznika (virtualswitch) umożliwiającego tworzenie sieci wirtualnej w obszarze hosta i pozwalającego połączyć maszyny wirtualne   
     w obszarze jednego hosta, a także na zewnątrz sieci fizycznej
     + 1. Serwer Bazodanowy 1 szt.

Serwer musi spełniać następujące minimalne warunki techniczne i funkcjonalne:

1. obudowa do montażu w szafie typu rack;
2. zasilanie redundantne, przynajmniej 2 zasilacze typu HotPlug;
3. płyta główna z możliwością zainstalowania minimum dwóch procesorów;
4. bazowy zegar procesora minimum3,5 GHz;
5. zainstalowany 1 procesor minimum 16 - rdzeniowy klasy x86 dedykowany do pracy w serwerach, zaprojektowane do pracy w układach wieloprocesorowych;
6. pamięć minimum 256 GB DDR5 ECC DIMM, rozszerzalna, z zabezpieczeniem typu: ECC.
7. dyski minimum 2x 480 GB w Raid1 , 2x min 3,2TB SSD NVME w RAID 1 oraz 4x dysk 2,4TB 10K skonfigurowane w raid 5;
8. Kontroler Raid z min 2GB Cache
9. interfejsy minimum: 4x 10GB sfp+ SR ( nalezy dostarczyć wkładki)
10. z przodu obudowy: min 1x USB 3.0
11. z tyłu obudowy: min 2x USB 3.0, 1x DB-15
12. Zarządzanie:
13. Zintegrowany z płytą główną serwera, niezależny od systemu operacyjnego, sprzętowy kontroler zdalnego zarządzania
14. Monitoring statusu i zdrowia systemu
15. Logowanie zdarzeń
16. Umożliwiający Update systemowego firmware
17. Umożliwiający zdalną konfigurację serwera
18. Monitoring i możliwość ograniczenia poboru prądu
19. Zdalne włączanie/wyłączanie/restart
20. Przekierowanie konsoli szeregowej przez IPMI
21. Możliwość przejęcia zdalnego ekranu 1920x1200, 60 Hz,16 bpp
22. Zdalny dostęp do serwera
23. Możliwość zdalnej instalacji systemu operacyjnego
24. Alerty Syslog
25. Przekierowanie konsoli szeregowej przez SSH
26. Wyświetlanie danych aktualnych I historycznych dla użycia energii I temperatury serwera
27. Możliwość mapowania obrazów ISO z lokalnego dysku operatora
28. Możliwość mapowania obrazów ISO przez min HTTPS
29. Możliwość jednoczesnej pracy do 6 użytkowników przez wirtualną konsolę
30. Wspierane protokoły/interfejsy: IPMI v2.0, SNMP v3, DCMI v1.5, REST API
31. Możliwość przewidywania awarii dla procesorów, pamięci, dysków wewnętrznych, wentylatorów, zasilaczy, kontrolerów RAID
32. Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA.
33. Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w Unii Europejskiej;
    * + 1. Tablet do zbierania zgód 20 szt.

|  |  |
| --- | --- |
| Parametr | Minimalne wymagania |
| Technologia pracy | Rezonans elektromagnetyczny (EMR) |
| Typ podpisu elektronicznego | Odręczny podpis elektroniczny (biometryczny) |
| Wymagane podłączenie do komputera | Tak |
| Zabezpieczenia | Slot zabezpieczenia Kensington® Lock |
| Rozmiar ekranu (mierzony po przekątnej) | 10.1 cala (25,65 cm) |
| Rozdzielczość ekranu | 1920 x 1080 pikseli (Full HD) |
| Technologia wyświetlania | AHVA (powierzchnia z trawionego szkła redukująca odblaski) |
| Głębia koloru | 8 bitów (16,7 milionów kolorów) |
| Proporcje / jasność matrycy | 16:9 / 200 cd/m2 (typ) |
| Wielodotyk (obsługa dotykiem) | Nie |
| Regulacja podstawy | 15° (rozkładana podstawa) |
| Wymiary aktywnego obszaru roboczego dla pióra | 223,2 x 125,6 mm (8.79 x 4.94 in) |
| Podłączenie do komputera | Przewodowo - USB-A |
| Typ pióra | Bezbateryjne, Bezprzewodowe, Czułe na nacisk (1024 poziomów nacisku) |
| Szybkość odczytu pozycji pióra | 200 pps |
| Rozdzielczość odczytu pozycji pióra | 100 linii na 1 mm (2540 linii na 1 cal) |
| Rozpoznawanie / zakres pochylenia pióra | ± 60° / 60 poziomów |
| Przechowywanie pióra | Zintegrowana przegroda na piórko, stojak na piórko |
| Ułatwienia dostępu | 4 programowalne przyciski |
| Zgodność z systemami operacyjnymi MAC/PC | Mac OSX 10.11 lub nowszy, Windows 7 lub nowszy. Dla każdego systemu wymagana instalacja sterownika |
| Szyfrowanie danych | AES 256 / RSA 2048 |
| Kompatybilność z oprogramowaniem do podpisu elektronicznego | SDK/API dostępne dla programistów  eSign, Wacomsign pro PDF; C++, .NET i Java |
| Sterowniki | Wymagany sterownik tabletu i sterownik wideo DisplayLink, SDK/API dostępne dla programistów |
| Wymiary zewnętrzne urządzenia | 283 x 210 x 11 mm |
| System mocowania | VESA mount (75 x 75 mm) |

* + - 1. Tablet 15 szt.

|  | **Opis parametrów wymaganych** | |
| --- | --- | --- |
|  | System operacyjny | Android 16 |
|  | Procesor | Octa-core min1,8 GHz |
|  | Pamięć RAM | 6 GB |
|  | Pamięć Flash | 128 GB |
|  | Wymiary (mm) | Max 170x260x8, mm |
|  | Waga | Max550g |
|  | Wyświetlacz | Podświetlany ekran TFT11-calowy (1920x1200) |
|  | Panel dotykowy | pojemnościowy ekran dotykowy |
|  | Interfejsy | USB typu C |
|  | Typ Baterii | Min. 7000 mAh |
|  | Czujniki | Akcelerometr,  Żyroskop,  Kompas,  Czujnik światła,  Czujnik Halla |
|  | Łączność | Wi-Fi (802.11a/b/g/n/ac)  Wi-Fi Direct  Bluetooth 5.3  5G  GPS |
|  | Gniazdo rozszerzeń | 1 gniazdo na kartę micro SD ,  Nano-SIM, eSIM |
|  | Aparat fotograficzny | Tylny aparat 8 MP z autofokusem, Lampa błyskowa LED o wysokiej jasności, przedni aparat 5 MP |
|  | Ochrona | Etui ochronne wykonane z TPU i poliwęglanu, ekran zabezpieczony szybką wbudowaną w etui.  Uchwyt na dłoń |
|  | Integracja | Integracja z systemem dziedzinowym HIS Eskulap w zakresie obsługi ruchu chorych |

1. Zakres przedmiotowy Etap V – świadczenia przez Wykonawcę na rzecz Zamawiającego Usług Gwarancji i Opieki Serwisowej w zakresie eksploatacji rozbudowywanego i modernizowanego Systemu HIS, wdrożonego przez Wykonawcę u Zamawiającego – 36 miesięcy od daty wykonania przedmiotu zamówienia tj. podpisania Protokołu Odbioru Końcowego
2. Wykonawca w ramach realizacji Przedmiotu Zamówienia przez 36 miesiące od wykonania przedmiotu zamówienia tj. podpisania Protokołu Odbioru Końcowego będzie świadczył na rzecz Zamawiającego Usługi Opieki serwisowej i aktualizacji w zakresie eksploatacji dostarczanego w ramach realizacji zadania Systemu HIS.
3. ZASADY ŚWIADCZENIA USŁUG DOSTĘPU DO NOWYCH WERSJI ORAZ USŁUG SERWISOWYCH DLA OPROGRAMOWANIA APLIKACYJNEGO

[ZASADY OGÓLNE]

1. Usługi Serwisowe są świadczone w odniesieniu do dostarczanego w ramach realizacji zadania w etapie II Systemu HIS zgodnie z postanowieniami rozdziału: Warunki brzegowe realizacji usług.

[UŻYTKOWNICY]

1. Wraz z podpisaniem Umowy ZAMAWIAJĄCY otrzymuje dane identyfikacyjne (login, hasło) umożliwiające Użytkownikom ZAMAWIAJĄCEGO uwierzytelnienie w systemie „Help Desk” zwanym dalej „HD” udostępnionym przez WYKONAWCĘ.
2. W zależności od woli ZAMAWIAJĄCEGO poszczególnym Użytkownikom zostaną przyznane prawa do ewidencji lub/i edycji Zgłoszeń Serwisowych.
3. Użytkownicy są zobligowani do ochrony danych identyfikacyjnych przed dostępem osób trzecich. Użytkownicy przyjmują także do wiadomości, że wszystkie operacje wykonywane w serwisie HD są rejestrowane.
4. Użytkownicy systemu HD posiadają możliwość dokonywania zmian swoich danych kontaktowych oraz podstawowych danych podmiotowych ZAMAWIAJĄCEGO. System HD będzie komunikował się z Użytkownikami wyłącznie w oparciu o informacje zamieszczone w HD.

Powinnością Użytkowników jest bieżące śledzenie informacji pojawiających się w systemie HD.

1. Powinnością Administratora jest zapoznanie się z postanowieniami Umowy, jak również przeszkolenie w zakresie jej zakresu oraz treści pozostałych Użytkowników.
2. Użytkownicy dołożą wszelkich starań, żeby dane osobowe nie były zamieszczane w Zgłoszeniach Serwisowych. Jeżeli jest to niezbędne do obsłużenia Zgłoszenia Serwisowego Użytkownicy zamieszczą informacje oraz dane wyłącznie w postaci zanonimizowanej lub zaszyfrowanej, jak również oznaczą Zgłoszenia Serwisowego zawierające takie dane w sposób określony w HD.

[EWIDENCJA I OBSŁUGA ZGŁOSZEŃ]

1. Ewidencja i uzupełnianie Zgłoszenia Serwisowego przez ZAMAWIAJĄCEGO jest realizowane wyłącznie w systemie HD. Obsługa przez Serwis Zgłoszenia Serwisowego w zależności od usługi jest realizowana w systemie HD lub z wykorzystaniem innych mediów bądź wizyt osobistych, przy czym każdorazowo w HD ewidencjonowany jest status zgłoszenia.
2. Użytkownik może zaewidencjonować w systemie HD następujące typy Zgłoszeń Serwisowych:
   * Błąd Aplikacji
   * Awaria
   * Usterka programistyczna
   * Konsultacja
   * Zamówienie indywidualne: Nowa funkcjonalność/Usługa odpłatna
   * Zapytanie handlowe
3. Zamawiający dopuszcza, by w systemie HD zgłoszenia uzyskiwały inne typy niż ww. odpowiadające rodzajowo powyższym Zgłoszeniom serwisowym.
4. Ewidencja Zgłoszenia Serwisowego odbywa się poprzez wprowadzenie przez Użytkownika do systemu HD wszystkich niezbędnych dla danego Zgłoszenia Serwisowego informacji w szczególności określenia obszaru/Modułu Oprogramowania Aplikacyjnego, którego Zgłoszenie Serwisowe dotyczy.

Po zaewidencjonowaniu przez Użytkownika Zgłoszenia Serwisowego system HD nadaje mu status „oczekujące” oraz unikalny numer.

1. Każde Zgłoszenie Serwisowe obejmować może wyłącznie jedno zagadnienie. W przypadku, gdy Zgłoszenie Serwisowe obejmuje kilka zagadnień WYKONAWCA może takie Zgłoszenie Serwisowe odrzucić lub wydzielić zagadnienia do odrębnych Zgłoszeń Serwisowych.
2. Jeżeli do Zgłoszenia Serwisowego pozostającego w toku Użytkownik wprowadzi nowe zagadnienie WYKONAWCA może je przenieść do odrębnego Zgłoszenia Serwisowego lub odrzucić realizację. Jeżeli nowe zagadnienie zostaje przeniesione do wyodrębnionego Zgłoszenia Serwisowego Termin realizacji usług określony w Warunkach brzegowych realizacji usług wszczyna swój bieg od początku.
3. Po wstępnej weryfikacji kompletności oraz formy Zgłoszenia Serwisowego, nie później niż w Czasie reakcji określonym w Warunkach brzegowych realizacji usług w systemie HD zostaje Zgłoszeniu Serwisowemu nadany status „zarejestrowane”. Alternatywnie, jeżeli weryfikacja wykaże, że Zgłoszenie Serwisowe nie spełnia wymogów Umowy lub dotyczy wątku stanowiącego przedmiot innego Zgłoszenia Serwisowego, zostaje mu nadany status odpowiednio „odrzucone” lub „duplikat”.
4. Dalsza obsługa Zgłoszenia Serwisowego przebiega na zasadach określonych w procedurach realizacji przewidzianych dla poszczególnych usług. W zależności od typu Zgłoszenia Serwisowego, fazy obsługi Zgłoszenia Serwisowego oraz jego zawartości, Zgłoszenie Serwisowe przyjmie jeden z następujących statusów:
   * nowe,
   * zarejestrowane,
   * u klienta,
   * aktywne,
   * odrzucone,
   * zrealizowane,
   * zamknięte.
5. Zamawiający dopuszcza, by w systemie HD zgłoszenia uzyskiwały inne statusy niż ww. odpowiadające aktualnemu etapowi realizacji Zgłoszenia.
6. Zamówienia indywidualne: Nowa funkcjonalność/Usługa Odpłatna – nie są objęte żadnym reżimem proceduralnym, w szczególności finansowym czy czasowym z wyłączeniem uzgodnień poczynionych w samej treści Zgłoszenia Serwisowego.
7. Szczególnym typem Zgłoszenia Serwisowego jest zapytanie handlowe. Jego ewidencja w HD służy jedynie celom informacyjnym o charakterze handlowym, natomiast obsługa nie jest objęta żadnym reżimem proceduralnym, w szczególności finansowym czy czasowym.
8. W każdym momencie Użytkownik może Zgłoszenie Serwisowe anulować, co spowoduje, że Zgłoszenie Serwisowe od momentu anulowania nie będzie przez Serwis dalej obsługiwane.
9. Po realizacji przez WYKONAWCĘ Zgłoszenia Serwisowego i wykonaniu przez WYKONAWCĘ testu poprawnego działania Oprogramowania Aplikacyjnego, zaakceptowanego przez Zamawiającego, Zgłoszenie Serwisowe traktowane jest jako zakończone.
10. Zgłoszenie Serwisowe jest ostatecznie zamykane, jeżeli upłynęło 7 dni od terminu przejścia Zgłoszenia w status zrealizowane, a Zamawiający nie wniósł w tym czasie zastrzeżeń do wyniku realizacji Zgłoszenia Serwisowego.

[USŁUGI SERWISOWE]

1. UsługarealizowanabędzieprzezWYKONAWCĘpoprzez:
   * wizytyserwisowewsiedzibieZAMAWIAJĄCEGO,
   * połączeniaZdalnego Dostępu.
2. Wizyty serwisowe realizowane będą przez Wykonawcę w zależności od potrzeb ZAMAWIAJĄCEGO.
3. Zgłoszenie wizyty serwisowej przez ZAMAWIAJĄCEGO nastąpi z 7 dniowym wyprzedzeniem. Każde Zgłoszenie zawierać będzie szczegółowo zakres prac do wykonania przez WYKONAWCĘ- zapotrzebowanie na wizytę konsultanta będzie zakładać pobyt konsultanta nie krótszy niż 5 godzin w siedzibie ZAMAWIAJĄCEGO.
4. W sytuacjach szczególnych i uzasadnionych termin wizyty serwisowej może zostać zmieniony za zgodą ZAMAWIAJĄCEGO, jednakże różnica dni w terminie wizyty nie może przekraczać 5 dni liczonych od wcześniej ustalonego terminu.
5. PołączeniazdalnerealizowanebędąprzezWykonawcęwgodzinachpracyZAMAWIAJĄCEGO,powcześniejszym uzgodnieniu terminu, godziny połączenia i rodzaju prac do wykonania z osobami upoważnionymi przez ZAMAWIAJĄCEGO. Terminy realizacji usług zdalnych będą obowiązywały wówczas, kiedy ZAMAWIAJĄCY udostępni połączenie zdalne. W przypadku braku takiego dostępu terminy realizacji usług mogą się przedłużać i tym samym mogą być niedochowane co nie będzie miało odzwierciedlenia w konsekwencjach dochowania terminów realizacji określonych dla WYKONAWCY
6. Rozliczenie czasu trwania usługi wykonanej poprzez połączenie zdalne WYKONAWCA winien przesłać ZAMAWIAJĄCEMU w narzędziu HD do akceptacji. Usługa może zostać rozliczona w limicie godzin przeznaczonych na Usługi serwisowe wyłącznie po pozytywnym wykonaniu prac (osiągnięciu zamierzonego przez Zamawiającego celu i efektu) i zaakceptowaniu rozliczenia czasu trwania usługi.
7. KażdorazowewykonaniewsiedzibieZAMAWIAJĄCEGOprzezSerwisWYKONAWCYzgłoszonychpraczakończone zostanie zarejestrowaniem przez ZAMAWIAJĄCEGO lub WYKONAWCĘ w HD tych prac, zawierających w szczególnościzakreswykonanychpraciliczbęprzepracowanychprzezSerwisWYKONAWCYgodzin,aprotokół będzie generowany automatycznie na podstawie zgłoszeń o statusie „zamknięte” z narzędzia HelpDesk, który to nie wymaga podpisu ze strony ZAMAWIAJĄCEGO i WYKONAWCY.
8. Usługi serwisowe wykorzystane będą przez ZAMAWIAJĄCEGO do określonego limitu godzinowego.
9. Każdorazowy dojazd do siedziby ZAMAWIAJĄCEGO stanowi równowartość 2 godzin usług serwisowych i umniejsza o tą ilość pakiet godzin serwisowych.

[DOSTĘP DO AKTUALIZACJI]**– dotyczy całego systemu HIS**

1. WYKONAWCA zapewni dostęp do aktualizacji za pomocą FTP z indywidualnie przydzielonym kontem Użytkownika - czas dostępu 24h/dobę w dni robocze, wolne i święta,
2. Każdy zestaw/paczka musi posiadać dokumentację opisującą wprowadzane zmiany w zakresie technicznym, funkcjonalnym i wynikającym ze zmian w prawie,
3. WYKONAWCA zapewni gwarancje zgodności zgromadzonych w systemie danych historycznych, pod kątem technicznym, funkcjonalnym i wynikającym ze zmian w prawie,
4. WYKONAWCA zapewni gwarancję zachowania pełnej sprawności systemów oraz poprawności i stabilności w zakresie przechowywania danych po wprowadzonych aktualizacjach
5. W przypadku stwierdzenia wystąpienia wad i błędów w Systemie po wprowadzeniu aktualizacji WYKONAWCA zobowiązany jest do nieodpłatnego usunięcia przyczyn oraz skutków wad i błędów w terminie do 7 Dni Roboczych od momentu otrzymania zgłoszenia o tym fakcie lub innym ustalonym i po akceptacji obu stron,
6. W przypadku wystąpienia Awarii uniemożliwiającej korzystanie z Systemu po wprowadzeniu aktualizacji wykonawca zobowiązany jest do nieodpłatnego usunięcia przyczyn i skutków Awarii w terminie do 24 godzin od momentu otrzymania zgłoszenia o tym fakcie,
7. Dostęp do nowych wersji zapewnia:

* utrzymanie Systemu w wersji polskojęzycznej z pełną dokumentacją w języku polskim pozwalającą na samodzielną naukę obsługi każdego modułu;
* zabezpieczenia przed nieautoryzowanym dostępem;
* monitorowanie wszystkich zdarzeń związanych z eksploatacją Systemu, przechowując informacje o Użytkowniku obsługującym zdarzenie;
* stabilność w zakresie funkcjonalno-technicznym konfigurowalnych indywidualnie elementów Systemu po przeprowadzeniu aktualizacji.
* gwarancje zgodności z aktualnym stanem prawnym oraz wytycznymi organizacyjno-technologicznymi wymaganych dla systemów medycznych.

1. WARUNKI BRZEGOWE REALIZACJI USŁUG SERWISOWYCH

|  |  |  |  |
| --- | --- | --- | --- |
| Lp. lp. | Nazwa | Terminy realizacji usług | Uwagi |
| 1. | Godziny pracy Serwisu | 8:00-16:00 | W dni robocze, tj. od poniedziałku do piątku z wyłączeniem dni wolnych od pracy w rozumieniu art. 1 oraz art. 1a ustawy z dnia 18 stycznia 1951 r. o dniach wolnych od pracy (tekst jedn.: Dz. U. z 2020 r. poz. 1920). Dni robocze stosuje się także w odniesieniu do wszystkich terminów przewidzianych w Załączniku na automatyczne czynności HD oraz do terminów zastrzeżonych dla Zamawiającego. |
| 2. | Czas reakcji Serwisu | 8h | Czas liczony w Godzinach pracy serwisu od momentu zaewidencjonowania Zgłoszenia Serwisowego do momentu przyjęcia zgłoszenia tj. nadania mu statusu „zarejestrowane”. |
| 3. | Czas usunięcia Błędu Aplikacji | 10 dni | 1. Czas liczony w godzinach lub dniach roboczych od upłynięcia Czasu reakcji w Godzinach pracy Serwisu.   Od Czasu obsługi zgłoszenia odlicza się okres, w którym WYKONAWCA oczekuje na uzupełnienie Zgłoszenia przez Zamawiającego lub udostępnienie zdalnego dostępu (jeżeli dotyczy).   1. W odniesieniu do Aplikacji, których Wykonawca nie jest Producentem przewidziane czasy realizacji usług mogą ulec dwukrotnemu wydłużeniu, o czym Zamawiającyzostaje powiadomiony w Zgłoszeniu. 2. Wykonawca gwarantuje udostępnianie co najmniej 4 zbiorczych pakietów aktualizacji zawierających Rozwinięcia wybranych Aplikacji rocznie, publikowanych nie rzadziej niż jedna na kwartał. Jeżeli Zgłoszenie zaklasyfikowane jako Usterka Programistyczna zostanie zaewidencjonowane w HD w terminie krótszym niż 20 dni przed planowanym terminem publikacji aktualizacji zbiorczej, Uaktualnienie zostanie uwzględnione najpóźniej w kolejnej aktualizacji zbiorczej. |
| 4. | Czas usunięcia Awarii | 48h |
| 5. | Czas usunięcia Usterki Programistycznej | Następna aktualizacja zbiorcza |
| 6. | Czas obsługi Konsultacji | 10 dni |
| 7. | Termin przystąpienia Serwisu do realizacji usług zleconych | Niegwarantowany | 1. Dotyczy usług wynikających z zamówień indywidualnych. |
| 8. | Termin udostępnienia Rozwinięć wynikających z nowelizacji aktów prawnych | Najpóźniej w dniu wejścia aktu w życie | 1. W przypadkach szczególnych, jeżeli termin ukazania się aktów prawnych inicjujących Rozwinięcia będzie krótszy niż 14 dni od daty ich wejścia w życie lub wraz z regulacjami nie zostaną opublikowane niezbędne materiały towarzyszące, takie jak: wytyczne, specyfikacje, interfejsy, protokoły, środowiska testowe, słowniki lub inne dane niezbędne do implementacji zmian specyfikacji funkcjonalnej w Rozwinięciach, Serwis określi w systemie HD termin dostarczenia i wprowadzenia Rozwinięcia zgodny z możliwościami realizacji, nie dłuższy jednak niż 21 dni roboczych od daty ukazania się ustaw i przepisów wykonawczych, zarządzeń NFZ lub udostępnienia brakujących materiałów towarzyszących. 2. Rozwinięcia będą wprowadzane w Aplikacjach w ramach usługi pod warunkiem, że procesy stanowiące przedmiot zmian legislacyjnych przed ich opublikowaniem występowały w specyfikacji funkcjonalnej Oprogramowania Aplikacyjnego zakupionego przez Zamawiającego a organy administracji publicznej nie udostępniły innego narzędzia bądź systemu umożliwiającego Zamawiającemu wykonanie obowiązku wynikającego z aktu prawnego. |

1. WYKAZ OBLIGATORYJNYCH USŁUG SERWISOWYCH

|  |  |  |
| --- | --- | --- |
| Lp. | Nazwa Usługi | Przedmiot Usługi |
|  | Serwis Aplikacji  [SA] | Gotowość WYKONAWCY do usuwania Błędów Oprogramowania Aplikacyjnego w posiadanym przez ZAMAWIAJĄCEGO zakresie funkcjonalnym w szczególności poprzez udostępnianie Uaktualnień Oprogramowania. |
|  | Konserwacja [KS] | Usługa realizowana przez WYKONAWCĘ bezpośrednio lub pośrednio, jeżeli WYKONAWCA nie jest jednocześnie Producentem Aplikacji. Subskrypcja usługi zapewnia dostosowanie specyfikacji funkcjonalnej Oprogramowania Aplikacyjnego posiadanego przez ZAMAWIAJĄCEGO do zmian legislacyjnych. W ramach usługi Producent gwarantuje:   * udostępnienie portalu HD umożliwiającego ewidencję Zgłoszeń Serwisowych, * prowadzeniu stałego audytu w zakresie zgodności funkcji Oprogramowania Aplikacyjnego z powszechnie obowiązującymi przepisami prawa polskiego o randze co najmniej rozporządzenia, w rozumieniu art. 87 ust.1 Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. i wprowadzanie do Aplikacji zmian stanowiących konsekwencję wejścia w życie tychże w postaci Rozwinięć. * prowadzeniu stałego audytu w zakresie zgodności funkcji Oprogramowania Aplikacyjnego z obowiązującymi ZAMAWIAJĄCEGO zarządzeniami Prezesa Narodowego Funduszu Zdrowia i wprowadzanie do Aplikacji zmian stanowiących konsekwencję wejścia w życie tychże. |
|  | Ewaluacja [EW] | Usługa realizowana przez WYKONAWCĘ bezpośrednio lub pośrednio, jeżeli WYKONAWCA nie jest jednocześnie Producentem Aplikacji. Subskrypcja usługi zapewnia poprawę jakości i rozszerzenie specyfikacji funkcjonalnej Oprogramowania Aplikacyjnego posiadanego przez ZAMAWIAJĄCEGO w zakresie jakim Producent Oprogramowania dokonuje Ewaluacji. W ramach usługi WYKONAWCA gwarantuje:   * wprowadzanie do Aplikacji nowych funkcji oraz usprawnień funkcji już w nich istniejących, stanowiących wynik inwencji twórczej Producenta, * wprowadzanie do Aplikacji nowych funkcji oraz usprawnień funkcji już w nich istniejących wnioskowanych przez Użytkowników. * Rozwinięcia wprowadzane w Aplikacjach w wyniku inwencji twórczej Producenta rozpowszechniane w ramach Licencji są udostępniane odpłatnie i uwzględnione w opłacie zryczałtowanej wnoszonej za subskrypcję usługi. |

1. DIGITALIZACJA DOKUMENTACJI MEDYCZNEJ ISTOTNEJ Z PUNKTU WIDZENIA LECZENIA I PROFILAKTYKI
2. Termin realizacji zadania

Wykonawca zobowiązuje się wykonać przedmiot Umowy od dnia podpisania umowy w terminach poszczególnych Etapów, które wynoszą:

Etap I – Dostawa licencji Aplikacji Digitalizacja Dokumentacji Medycznejoraz HL7- do 30 dni kalendarzowych od daty podpisania Umowy

Etap II - Wdrożenie Aplikacji: Digitalizacja Dokumentacji Medyczneji HL7 oraz Dostawa skanera– do 30.04.2026r

Etap III – świadczenie przez Wykonawcę na rzecz Zamawiającego Usług Gwarancji i Opieki Serwisowej w zakresie Aplikacji: Digitalizacja Dokumentacji Medycznej – 36 miesięcy od daty podpisania Protokołu Odbioru Końcowego.

UWAGA: Całość zadania musi zostać zrealizowana nie później niż do 30.04.2026r

1. Zakres przedmiotowy Etapu I - Dostawa Licencji
2. Wykaz Licencji objętych przedmiotem Umowy:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Lp. | Nazwa modułu | Ilość | Rodzaj licencji | Okres |
|  | Digitalizacja Dokumentacji Medycznej | 1 | SRW | bezterminowa |
|  | HL7CDA | 1 | SYS | bezterminowa |

1. Warunki licencji:
2. Zamawiający oczekuje udzielenia licencji Serwerowej (SRW) dla Aplikacji- Zamawiający jest uprawniony do korzystania z danego modułu oprogramowania na maksymalnie takiej liczbie serwerów, na jaką została udzielona przez nieograniczoną liczbę użytkowników na nieograniczonej liczbie komputerów lub terminali. Licencja reglamentuje także systemy operacyjne serwera do liczby tożsamej z ilością serwerów, na które została udzielona,
3. Licencja nie może wprowadzać ograniczenia na tzw. „nazwanych użytkowników”
4. Licencją objęte zostaną również wszelkie poprawki i aktualizacje Aplikacji pojawiające się w trakcie obowiązywania przedmiotowej Umowy a także w trakcie następnych umów serwisowych.
5. Wykonawca zobowiązany jest udzielić licencji na Aplikacje, jej rozwinięcia i uaktualnienia oraz towarzyszącą dokumentację na czas nieoznaczony.
6. Zakres przedmiotowy Etapu II - Wdrożenie Aplikacji
7. Usługi Wdrożeniowe
8. Wdrożenie należy rozumieć jako szereg uporządkowanych i zorganizowanych działań mających na celu wykonanie Przedmiotu Zamówienia.
9. Wykonawca umożliwi Zamawiającemu udział we wszystkich pracach realizowanych przez Wykonawcę w ramach realizacji Przedmiotu Zamówienia (m.in. w czasie dostaw, instalacji, konfiguracji i pozostałych elementach wdrożenia).
10. Wykonawca zobowiązany jest przeprowadzić dostawy i usługi będące Przedmiotem Zamówienia w dokładnych terminach i godzinach uzgodnionych z Zamawiającym.
11. Wdrożenie będą realizowane w ramach powołanych do tego celu struktur organizacyjnych po stronie Wykonawcy i Zamawiającego.
12. Wykonawca zorganizuje prace tak, aby w maksymalnym stopniu nie zakłócać ciągłości funkcjonowania prac u Zamawiającego. 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.
13. Wykonawca musi uwzględnić, że wszystkie prace wykonywane będą w użytkowanych obiektach przy dużym ruchu pracowników i chorych, tzn. organizacja prac powinna przede wszystkim zapewniać bezpieczeństwo przebywających w oddziałach pracowników i chorych oraz zachowanie ciszy nocnej w godzinach właściwych dla Zamawiającego.
14. Po zakończeniu prac instalacyjnych Aplikacja musi zostać skonfigurowana i wdrożona w sposób kompleksowy tak, aby oferowała wszystkie funkcjonalności zgodnie z Dokumentacjąw zakresie opisanych w OPZ wymagań funkcjonalnych.
15. Aplikacja musi zostać zainstalowana przez Wykonawcę w środowiskach informatycznych Zamawiającego. Aplikacja musi zostać zainstalowana i skonfigurowana w sposób kompleksowy.
16. Wymagania funkcjonalne Aplikacji: Digitalizacja Dokumentacji Medycznej

|  |  |
| --- | --- |
| Lp. | Digitalizacja Dokumentacji Medycznej – WYMAGANIA MINIMALNE |
| 1. | Możliwość wygenerowania zaległych kart informacyjnych za lata 2023-2025 przy założeniu zaewidencjonowanych wcześniej danych w systemie. |
| 2. | Możliwość zaindeksowania zaległych kart informacyjnych za lata 2023-2025 przy założeniu wygenerowanych wcześniej kart w systemie. |

1. Dostawa skanera 1 szt.

|  |  |
| --- | --- |
| **Parametr** | **Charakterystyka** |
| **Typ** | Skaner biurkowy z podajnikiem dokumentów |
| **Skanowanie** | Skanowanie dwustronne |
| **Prędkość skanowania A4** | min. 40 stron /min |
| **Podajnik ADF** | Skaner musi posiadać podajnik ADF na min. 80 arkuszy |
| **Wyświetlacz** | Skaner musi posiadać kolorowy ekran dotykowy |
| **Interfejsy** | 1 x USB3.0, 1 x Ethernet (10Base-T/100Base-TX), 1 x Wi-Fi 802.11b/g/n (2.4GHz) |
| **Głębia kolorów** | 48-bitowa wewnętrzna i 24- bitowa zewnętrzna |
| **Skala szarości** | 256 odcieni (8 bitów) |
| **Obsługiwane formaty**  **plików** | PDF (jednostronicowe, wielostronicowe, PDF/A-1b, zabezpieczony, podpisany), |
| JPEG, TIFF (jednostronicowe, wielostronicowe) |
| **Rodzaje nośników** | Papier standardowy, cienki, gruby, grubszy, makulaturowy, wizytówki, karty plastikowe |
| **Zarządzanie** | Skaner musi mieć możliwość po wpisaniu w przeglądarce internetowej adresu IP lub nazwy węzła urządzenia oraz podając zaszyfrowane hasło dostęp do zainstalowanego w urządzeniu oprogramowania do zarządzania urządzeniem. |

1. Zakres przedmiotowy Etap III- świadczenie przez Wykonawcę na rzecz Zamawiającego Usług Gwarancji i Opieki Serwisowej w zakresie Aplikacji: Digitalizacja Dokumentacji Medycznej i HL7– 36 miesięcy od daty wykonania przedmiotu zamówienia tj. podpisania Protokołu Odbioru Końcowego.
2. Wykonawca w ramach realizacji Przedmiotu Zamówienia przez 36 miesiące od zakończenia realizacji przedmiotu zamówienia tj. podpisania Protokołu Odbioru Końcowego będzie świadczył na rzecz Zamawiającego Usługi Opieki serwisowej i aktualizacji w zakresie eksploatacji dostarczanej w ramach realizacji zadania Aplikacji.
3. ZASADY ŚWIADCZENIA USŁUG DOSTĘPU DO NOWYCH WERSJI ORAZ USŁUG SERWISOWYCH DLA APLIIKACJI

[ZASADY OGÓLNE]

1. Usługi Serwisowe są świadczone w odniesieniu do dostarczanej w ramach realizacji zadania Aplikacji: Digitalizacja Dokumentacji Medycznej zgodnie z postanowieniami rozdziału: Warunki brzegowe realizacji usług.

[UŻYTKOWNICY]

1. Wraz z podpisaniem Umowy ZAMAWIAJĄCY otrzymuje dane identyfikacyjne (login, hasło) umożliwiające Użytkownikom ZAMAWIAJĄCEGO uwierzytelnienie w systemie „Help Desk” zwanym dalej „HD” udostępnionym przez WYKONAWCĘ.
2. W zależności od woli ZAMAWIAJĄCEGO poszczególnym Użytkownikom zostaną przyznane prawa do ewidencji lub/i edycji Zgłoszeń Serwisowych.
3. Użytkownicy są zobligowani do ochrony danych identyfikacyjnych przed dostępem osób trzecich. Użytkownicy przyjmują także do wiadomości, że wszystkie operacje wykonywane w serwisie HD są rejestrowane.
4. Użytkownicy systemu HD posiadają możliwość dokonywania zmian swoich danych kontaktowych oraz podstawowych danych podmiotowych ZAMAWIAJĄCEGO. System HD będzie komunikował się z Użytkownikami wyłącznie w oparciu o informacje zamieszczone w HD.

Powinnością Użytkowników jest bieżące śledzenie informacji pojawiających się w systemie HD.

1. Powinnością Administratora jest zapoznanie się z postanowieniami Umowy, jak również przeszkolenie w zakresie jej zakresu oraz treści pozostałych Użytkowników.
2. Użytkownicy dołożą wszelkich starań, żeby dane osobowe nie były zamieszczane w Zgłoszeniach Serwisowych. Jeżeli jest to niezbędne do obsłużenia Zgłoszenia Serwisowego Użytkownicy zamieszczą informacje oraz dane wyłącznie w postaci zanonimizowanej lub zaszyfrowanej, jak również oznaczą Zgłoszenia Serwisowego zawierające takie dane w sposób określony w HD.

[EWIDENCJA I OBSŁUGA ZGŁOSZEŃ]

1. Ewidencja i uzupełnianie Zgłoszenia Serwisowego przez ZAMAWIAJĄCEGO jest realizowane wyłącznie w systemie HD. Obsługa przez Serwis Zgłoszenia Serwisowego w zależności od usługi jest realizowana w systemie HD lub z wykorzystaniem innych mediów bądź wizyt osobistych, przy czym każdorazowo w HD ewidencjonowany jest status zgłoszenia.
2. Użytkownik może zaewidencjonować w systemie HD następujące typy Zgłoszeń Serwisowych:
   * Błąd Aplikacji
   * Awaria
   * Usterka programistyczna
   * Konsultacja
   * Zamówienie indywidualne: Nowa funkcjonalność/Usługa odpłatna
   * Zapytanie handlowe
3. Zamawiający dopuszcza, by w systemie HD zgłoszenia uzyskiwały inne typy niż ww. odpowiadające rodzajowo powyższym Zgłoszeniom serwisowym.
4. Ewidencja Zgłoszenia Serwisowego odbywa się poprzez wprowadzenie przez Użytkownika do systemu HD wszystkich niezbędnych dla danego Zgłoszenia Serwisowego informacji.

Po zaewidencjonowaniu przez Użytkownika Zgłoszenia Serwisowego system HD nadaje mu status „oczekujące” oraz unikalny numer.

1. Każde Zgłoszenie Serwisowe obejmować może wyłącznie jedno zagadnienie. W przypadku, gdy Zgłoszenie Serwisowe obejmuje kilka zagadnień WYKONAWCA może takie Zgłoszenie Serwisowe odrzucić lub wydzielić zagadnienia do odrębnych Zgłoszeń Serwisowych.
2. Jeżeli do Zgłoszenia Serwisowego pozostającego w toku Użytkownik wprowadzi nowe zagadnienie WYKONAWCA może je przenieść do odrębnego Zgłoszenia Serwisowego lub odrzucić realizację. Jeżeli nowe zagadnienie zostaje przeniesione do wyodrębnionego Zgłoszenia Serwisowego Termin realizacji usług określony w Warunkach brzegowych realizacji usług wszczyna swój bieg od początku.
3. Po wstępnej weryfikacji kompletności oraz formy Zgłoszenia Serwisowego, nie później niż w Czasie reakcji określonym w Warunkach brzegowych realizacji usług w systemie HD zostaje Zgłoszeniu Serwisowemu nadany status „zarejestrowane”. Alternatywnie, jeżeli weryfikacja wykaże, że Zgłoszenie Serwisowe nie spełnia wymogów Umowy lub dotyczy wątku stanowiącego przedmiot innego Zgłoszenia Serwisowego, zostaje mu nadany status odpowiednio „odrzucone” lub „duplikat”.
4. Dalsza obsługa Zgłoszenia Serwisowego przebiega na zasadach określonych w procedurach realizacji przewidzianych dla poszczególnych usług. W zależności od typu Zgłoszenia Serwisowego, fazy obsługi Zgłoszenia Serwisowego oraz jego zawartości, Zgłoszenie Serwisowe przyjmie jeden z następujących statusów:
   * nowe,
   * zarejestrowane,
   * u klienta,
   * aktywne,
   * odrzucone,
   * zrealizowane,
   * zamknięte.
5. Zamawiający dopuszcza, by w systemie HD zgłoszenia uzyskiwały inne statusy niż ww. odpowiadające aktualnemu etapowi realizacji Zgłoszenia.
6. Zamówienia indywidualne: Nowa funkcjonalność/Usługa Odpłatna – nie są objęte żadnym reżimem proceduralnym, w szczególności finansowym czy czasowym z wyłączeniem uzgodnień poczynionych w samej treści Zgłoszenia Serwisowego.
7. Szczególnym typem Zgłoszenia Serwisowego jest zapytanie handlowe. Jego ewidencja w HD służy jedynie celom informacyjnym o charakterze handlowym, natomiast obsługa nie jest objęta żadnym reżimem proceduralnym, w szczególności finansowym czy czasowym.
8. W każdym momencie Użytkownik może Zgłoszenie Serwisowe anulować, co spowoduje, że Zgłoszenie Serwisowe od momentu anulowania nie będzie przez Serwis dalej obsługiwane.
9. Po realizacji przez WYKONAWCĘ Zgłoszenia Serwisowego i wykonaniu przez WYKONAWCĘ testu poprawnego działania Aplikacji, zaakceptowanego przez Zamawiającego, Zgłoszenie Serwisowe traktowane jest jako zakończone.
10. Zgłoszenie Serwisowe jest ostatecznie zamykane, jeżeli upłynęło 7 dni od terminu przejścia Zgłoszenia w status zrealizowane, a Zamawiający nie wniósł w tym czasie zastrzeżeń do wyniku realizacji Zgłoszenia Serwisowego.

[USŁUGI SERWISOWE]

1. UsługarealizowanabędzieprzezWYKONAWCĘpoprzez:
   * wizytyserwisowewsiedzibieZAMAWIAJĄCEGO,
   * połączeniaZdalnego Dostępu.
2. Wizyty serwisowe realizowane będą przez Wykonawcę w zależności od potrzeb ZAMAWIAJĄCEGO.
3. Zgłoszenie wizyty serwisowej przez ZAMAWIAJĄCEGO nastąpi z 7 dniowym wyprzedzeniem. Każde Zgłoszenie zawierać będzie szczegółowo zakres prac do wykonania przez WYKONAWCĘ- zapotrzebowanie na wizytę konsultanta będzie zakładać pobyt konsultanta nie krótszy niż 5 godzin w siedzibie ZAMAWIAJĄCEGO.
4. W sytuacjach szczególnych i uzasadnionych termin wizyty serwisowej może zostać zmieniony za zgodą ZAMAWIAJĄCEGO, jednakże różnica dni w terminie wizyty nie może przekraczać 5 dni liczonych od wcześniej ustalonego terminu.
5. PołączeniazdalnerealizowanebędąprzezWykonawcęwgodzinachpracyZAMAWIAJĄCEGO,powcześniejszym uzgodnieniu terminu, godziny połączenia i rodzaju prac do wykonania z osobami upoważnionymi przez ZAMAWIAJĄCEGO. Terminy realizacji usług zdalnych będą obowiązywały wówczas, kiedy ZAMAWIAJĄCY udostępni połączenie zdalne. W przypadku braku takiego dostępu terminy realizacji usług mogą się przedłużać i tym samym mogą być niedochowane co nie będzie miało odzwierciedlenia w konsekwencjach dochowania terminów realizacji określonych dla WYKONAWCY
6. Rozliczenie czasu trwania usługi wykonanej poprzez połączenie zdalne WYKONAWCA winien przesłać ZAMAWIAJĄCEMU w narzędziu HD do akceptacji. Usługa może zostać rozliczona w limicie godzin przeznaczonych na Usługi serwisowe tylko i wyłącznie po pozytywnym wykonaniu prac (osiągnięciu zamierzonego przez Zamawiającego celu i efektu) i zaakceptowaniu rozliczenia czasu trwania usługi.
7. KażdorazowewykonaniewsiedzibieZAMAWIAJĄCEGOprzezSerwisWYKONAWCYzgłoszonychpraczakończone zostanie zarejestrowaniem przez ZAMAWIAJĄCEGO lub WYKONAWCĘ w HD tych prac, zawierających w szczególnościzakreswykonanychpraciliczbęprzepracowanychprzezSerwisWYKONAWCYgodzin,aprotokół będzie generowany automatycznie na podstawie zgłoszeń o statusie „zamknięte” z narzędzia HelpDesk, który to nie wymaga podpisu ze strony ZAMAWIAJĄCEGO i WYKONAWCY.
8. Usługi serwisowe wykorzystane będą przez ZAMAWIAJĄCEGO do określonego limitu godzinowego.
9. Każdorazowy dojazd do siedziby ZAMAWIAJĄCEGO stanowi równowartość 2 godzin usług serwisowych i umniejsza o tą ilość pakiet godzin serwisowych.

[DOSTĘP DO AKTUALIZACJI]

1. WYKONAWCA zapewni dostęp do aktualizacji za pomocą FTP z indywidualnie przydzielonym kontem Użytkownika - czas dostępu 24h/dobę w dni robocze, wolne i święta,
2. Każdy zestaw/paczka musi posiadać dokumentację opisującą wprowadzane zmiany w zakresie technicznym, funkcjonalnym i wynikającym ze zmian w prawie,
3. WYKONAWCA zapewni gwarancje zgodności zgromadzonych w systemie danych historycznych, pod kątem technicznym, funkcjonalnym i wynikającym ze zmian w prawie,
4. WYKONAWCA zapewni gwarancję zachowania pełnej sprawności systemów oraz poprawności i stabilności w zakresie przechowywania danych po wprowadzonych aktualizacjach
5. W przypadku stwierdzenia wystąpienia wad i błędów w Aplikacji po wprowadzeniu aktualizacji WYKONAWCA zobowiązany jest do nieodpłatnego usunięcia przyczyn oraz skutków wad i błędów w terminie do 7 Dni Roboczych od momentu otrzymania zgłoszenia o tym fakcie lub innym ustalonym i po akceptacji obu stron,
6. W przypadku wystąpienia Awarii uniemożliwiającej korzystanie z Aplikacji po wprowadzeniu aktualizacji wykonawca zobowiązany jest do nieodpłatnego usunięcia przyczyn i skutków Awarii w terminie do 24 godzin od momentu otrzymania zgłoszenia o tym fakcie,
7. Dostęp do nowych wersji zapewnia:

* utrzymanie Systemu w wersji polskojęzycznej z pełną dokumentacją w języku polskim pozwalającą na samodzielną naukę obsługi każdego modułu;
* zabezpieczenia przed nieautoryzowanym dostępem;
* monitorowanie wszystkich zdarzeń związanych z eksploatacją Aplikacji, przechowując informacje o Użytkowniku obsługującym zdarzenie;

1. WARUNKI BRZEGOWE REALIZACJI USŁUG SERWISOWYCH

|  |  |  |  |
| --- | --- | --- | --- |
| Lp. lp. | Nazwa | Terminy realizacji usług | Uwagi |
| 1. | Godziny pracy Serwisu | 8:00-16:00 | W dni robocze, tj. od poniedziałku do piątku z wyłączeniem dni wolnych od pracy w rozumieniu art. 1 oraz art. 1a ustawy z dnia 18 stycznia 1951 r. o dniach wolnych od pracy (tekst jedn.: Dz. U. z 2020 r. poz. 1920). Dni robocze stosuje się także w odniesieniu do wszystkich terminów przewidzianych w Załączniku na automatyczne czynności HD oraz do terminów zastrzeżonych dla ZAMAWIAJĄCEGO. |
| 2. | Czas reakcji Serwisu | 8h | Czas liczony w Godzinach pracy serwisu od momentu zaewidencjonowania Zgłoszenia Serwisowego do momentu przyjęcia zgłoszenia tj. nadania mu statusu „zarejestrowane”. |
| 3. | Czas usunięcia Błędu Aplikacji | 10 dni | 1. Czas liczony w godzinach lub dniach roboczych od upłynięcia Czasu reakcji w Godzinach pracy Serwisu.   Od Czasu obsługi zgłoszenia odlicza się okres, w którym WYKONAWCA oczekuje na uzupełnienie Zgłoszenia przez ZAMAWIAJĄCEGO lub udostępnienie zdalnego dostępu (jeżeli dotyczy).   1. W odniesieniu do Aplikacji, których WYKONAWCA nie jest Producentem przewidziane czasy realizacji usług mogą ulec dwukrotnemu wydłużeniu, o czym ZAMAWIAJĄCY zostaje powiadomiony w Zgłoszeniu. 2. WYKONAWCA gwarantuje udostępnianie co najmniej 4 zbiorczych pakietów aktualizacji zawierających Rozwinięcia wybranych Aplikacji rocznie, publikowanych nie rzadziej niż jedna na kwartał. Jeżeli Zgłoszenie zaklasyfikowane jako Usterka Programistyczna zostanie zaewidencjonowane w HD w terminie krótszym niż 20 dni przed planowanym terminem publikacji aktualizacji zbiorczej, Uaktualnienie zostanie uwzględnione najpóźniej w kolejnej aktualizacji zbiorczej. |
| 4. | Czas usunięcia Awarii | 48h |
| 5. | Czas usunięcia Usterki Programistycznej | Następna aktualizacja zbiorcza |
| 6. | Czas obsługi Konsultacji | 10 dni |
| 7. | Termin przystąpienia Serwisu do realizacji usług zleconych | Niegwarantowany | 1. Dotyczy usług wynikających z zamówień indywidualnych. |

1. WYKAZ OBLIGATORYJNYCH USŁUG SERWISOWYCH

|  |  |  |
| --- | --- | --- |
| Lp. | Nazwa Usługi | Przedmiot Usługi |
|  | Serwis Aplikacji  [SA] | Gotowość WYKONAWCY do usuwania Błędów Aplikacji w posiadanym przez ZAMAWIAJĄCEGO zakresie funkcjonalnym w szczególności poprzez udostępnianie Uaktualnień Aplikacji. |
|  | Konserwacja [KS] | Usługa realizowana przez WYKONAWCĘ bezpośrednio lub pośrednio, jeżeli WYKONAWCA nie jest jednocześnie Producentem Aplikacji. Subskrypcja usługi zapewnia dostosowanie specyfikacji funkcjonalnej Aplikacji posiadanej przez ZAMAWIAJĄCEGO do zmian legislacyjnych. W ramach usługi Producent gwarantuje:   * udostępnienie portalu HD umożliwiającego ewidencję Zgłoszeń Serwisowych, * prowadzeniu stałego audytu w zakresie zgodności funkcji Aplikacji z powszechnie obowiązującymi przepisami prawa polskiego o randze co najmniej rozporządzenia, w rozumieniu art. 87 ust.1 Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. i wprowadzanie do Aplikacji zmian stanowiących konsekwencję wejścia w życie tychże w postaci Rozwinięć. * prowadzeniu stałego audytu w zakresie zgodności funkcji Aplikacji z obowiązującymi ZAMAWIAJĄCEGO zarządzeniami Prezesa Narodowego Funduszu Zdrowia i wprowadzanie do Aplikacji zmian stanowiących konsekwencję wejścia w życie tychże. |
|  | Ewaluacja [EW] | Usługa realizowana przez WYKONAWCĘ bezpośrednio lub pośrednio, jeżeli WYKONAWCA nie jest jednocześnie Producentem Aplikacji. Subskrypcja usługi zapewnia poprawę jakości i rozszerzenie specyfikacji funkcjonalnej Aplikacji posiadanej przez ZAMAWIAJĄCEGO w zakresie jakim Producent Aplikacji dokonuje Ewaluacji. W ramach usługi WYKONAWCA gwarantuje:   * wprowadzanie do Aplikacji nowych funkcji oraz usprawnień funkcji już w nich istniejących, stanowiących wynik inwencji twórczej Producenta, * wprowadzanie do Aplikacji nowych funkcji oraz usprawnień funkcji już w nich istniejących wnioskowanych przez Użytkowników. * Rozwinięcia wprowadzane w Aplikacjach w wyniku inwencji twórczej Producenta rozpowszechniane w ramach Licencji są udostępniane odpłatnie i uwzględnione w opłacie zryczałtowanej wnoszonej za subskrypcję usługi. |

1. DZIAŁANIA ZWIĘKSZAJĄCE POZIOM CYBERBEZPIECZEŃSTWA SZPITALA
2. Termin realizacji zadania

Wykonawca zobowiązuje się wykonać przedmiot Umowy od dnia podpisania umowy w terminach poszczególnych Etapów, które wynoszą:

Etap I – Dostawa i instalacja Infrastruktury IT oraz szkolenia z cyberbezpieczeństwa – do 15.05.2026r

Etap II – uruchomienie przez Wykonawcę na rzecz Zamawiającego usługi SOC – do 30 dni od daty podpisania umowy

Etap III – świadczenia przez Wykonawcę na rzecz ZamawiającegoUsług Gwarancji w zakresie dostarczanej Infrastruktury IT– 36 miesięcy od daty podpisania Protokołu Odbioru Końcowego

UWAGA: Całość zadania musi zostać zrealizowana nie później niż do 15.05.2026r

1. Zakres przedmiotowy Etapu I - Dostawa i instalacja Infrastruktury IT
2. Przedmiotem etapu jest dostawa i instalacja infrastruktury ICT u Zamawiającego.

Poniżej wyspecyfikowano minimalne parametry infrastruktury ICT, które należy dostarczyć w ramach realizacji zadania. W przypadku, gdy nie określono, że parametr określa maksymalną wartość jest to jego wartość minimalna.

1. Organizacja prac związanych z Projektem

W celu efektywnego prowadzenia prac projektowych, w ramach projektu w terminie 7 dni kalendarzowych od dnia podpisania Umowy zostaną powołane odpowiednie struktury projektowe, zarówno po stronie Wykonawcy, jak również po stronie Zamawiającego.

Podstawowe role w ramach powołanej struktury powinny być minimalnie:

* Kierownik Projektu po stronie Wykonawcy odpowiedzialny za całość prac projektowych,
* Kierownik Projektu po stronie Zamawiającego odpowiedzialny za prace wykonywane przez Zamawiającego,

1. Przygotowanie Dokumentacji

W ramach procesu prac Wykonawca opracuje dla Zamawiającego Dokumentację Przedmiotu Zamówienia (zwaną dalej Dokumentacją), która składa się z nw. zakresów:

* Dokumentacja Analizy Przedwdrożeniowej (DAP)
* Dokumentacja Powykonawcza

Dokumentacja powyższa będzie zawierać bazowe zapisy opisujące budowane rozwiązania, procesy oraz sposób organizacji prac, dostaw, instalacji. Na podstawie zapisów w Dokumentacji będą prowadzone i odbierane poszczególne etapy realizowane w ramach Przedmiotu zamówienia. Dokumentacja Analizy Przedwdrożeniowej DAP

DAP powinna określać w poszczególnych obszarach co najmniej:

ZARZĄDCZY

* Harmonogram Realizacji zadania
* plan i sposób komunikacji Stron,
* zarządzenie ryzykiem,
* zarządzanie zmianą.

INFRASTRUKTURA

* analiza parametrów infrastruktury udostępnionej przez Zamawiającego do celów realizacji Przedmiotu Zamówienia,
* przygotowanie planu reinstalacji /rekonfiguracji infrastruktury serwerowej i sieciowej, opis instalacji
* karty katalogowe urządzeń potwierdzające spełnienie wymagań,
* plan dostaw,
* opis instalacji i wdrożenia oprogramowania wdrażanego wraz z Infrastrukturą IT
* opis modernizacji i budowy Infrastruktury serwerowej, sieciowej oraz komputerowej,
* szczegółowy zakres i zawartość pozostałej Dokumentacji.

1. Wymagania ogólne:

* Całość dostarczanego sprzętu i oprogramowania musi pochodzić z autoryzowanego kanału sprzedaży producenta.
* Całość dostarczanego rozwiązania, tzn. każde z dostarczonych urządzeń, musi być nowe, wcześniej nieużywane, rok produkcji nie starszy niż 2025.
* Całość dostarczanego rozwiązania, tzn. każde z dostarczonych urządzeń, w którym nie wskazano warunków gwarancji, musi być objęte gwarancją w okresie minimum 36 miesięcy
* Urządzenia i ich komponenty muszą być oznakowane przez producentów w taki sposób, aby możliwa była identyfikacja zarówno produktu, producenta, jak i daty produkcji danego elementu.
* Do każdego urządzenia musi być dostarczony komplet standardowej dokumentacji dla użytkownika w formie papierowej lub elektronicznej w języku polskim lub angielskim.
* Do każdego urządzenia musi być dostarczony niezbędny sprzęt eksploatacyjny (przewody zasilające, przewody sygnałowe itp.) niezbędny do uruchomienia danego urządzenia w budowanym rozwiązaniu w miejscu dostawy wskazanym przez Zamawiającego. Sprzęt, o którym mowa powyżej jest integralną częścią oferty i przechodzi na własność Zamawiającego.
* Wszystkie urządzenia muszą posiadać oznakowanie CE.
* Wszystkie dostarczane urządzenia na dzień złożenia oferty nie mogą być w fazie end-of-life (EOL)
* Wszystkie urządzenia muszą współpracować z siecią energetyczną o parametrach: 230 V ± 10%, 50 Hz.
* Wymagane jest, aby infrastruktura sprzętowa była gotowym produktem posiadającym nazwę handlową i złożonym z zamkniętej, ściśle zdefiniowanej listy komponentów posiadających odpowiednie numery katalogowe.
* Dostarczane oprogramowanie musi zostać dostarczone w najnowszej stabilnej wersji, która uzyskała certyfikację producenta dostarczanego sprzętu (jeśli podlega certyfikacji).

1. Wykonawca w ramach etapu I zobowiązany jest do wykonania co najmniej następujących usług związanych z montażem i konfiguracją dostarczanej infrastruktury sprzętowej:
2. Wykonanie Projektu Technicznego dostarczanej Infrastruktury sprzętowej, który będzie składał się co najmniej z następujących elementów:
   * Dokładna specyfikacja techniczna wraz z numerami katalogowymi poszczególnych elementów,
   * Nazwy oraz szczegółowej adresacja poszczególnych elementów,
   * Planowana konfiguracja środowiska wraz z połączeniami, konfiguracją poszczególnych elementów w tym logiczną konfiguracją miejsca,
   * Wymagane działania ze strony Zamawiającego w celu poprawnego montażu i konfiguracji,
   * Harmonogram prac.

Projekt techniczny musi zostać wykonany po wcześniejszej analizie środowiska wykonanej przez Wykonawcę oraz musi zostać zaakceptowany przez Zamawiającego.

1. Instalacja oraz konfiguracji oprogramowania.
2. Testy rozwiązania.
3. Instruktaż dla administratorów demonstrujący sposób zarządzania środowiskiem.
4. Dostarczenie dokumentacji powykonawczej infrastruktury sprzętowej, która będzie składała się co najmniej z następujących elementów:
   * Specyfikacja techniczna wraz z numerami katalogowymi poszczególnych elementów oraz numerami seryjnymi poszczególnych elementów,
   * Końcowe nazwy oraz szczegółowa adresacja poszczególnych elementów,
   * Konfiguracja środowiska wraz z połączeniami, konfiguracją poszczególnych elementów w tym logiczną konfiguracją miejsc
   * Komplety poświadczeń do całej infrastruktury – wymagana zmiana haseł domyślnych – dostarczone jako osobny załącznik w postaci zaszyfrowanego pliku kdbx,
   * Dokumentacja techniczna w formie elektronicznej do każdego elementu w języku polskim lub angielskim
   * Szczegóły dotyczące instalacji i uruchomienia infrastruktury sprzętowej, w zakresie modernizacji infrastruktury szpitala, zostaną ustalone pomiędzy Stronami w trakcie Analizy Przedwdrożeniowej.
   * Zamawiający zapewni odpowiedni zapas mocy oraz odpowiednie warunki środowiskowe w komorach serwerowni.
   * Po zakończonym montażu Wykonawca przekaże Zamawiającemu wszystkie hasła dostępowe do kont „super użytkowników”.
5. Opis parametrów minimalnych dostarczanej Infrastruktury IT

3.3.1. System Backupu 1 szt.

1. Wymagania ogólne
   1. Oprogramowanie musi być produktem przeznaczonym do obsługi środowisk DataCenter. Oferowany produkt musi znajdować się w kwadracie liderów Gartner Magic Quadrant for Data Center Backup and Recovery Solutions oraz na ogólnie dostępnej liście referencyjnej Gartner: https://www.gartner.com/reviews/market/data-center-backup-and-recovery-solutions i spełniać minimalne wymaganie : - minimalna liczba referencji 150, - minimalna ocena z referencji 4,5,
   2. Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 6.x, 7.x i 8.0 oraz Microsoft Hyper-V 2012, 2012R2, 2016, 2019 i 2022. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej
   3. Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux.
2. Całkowite koszty posiadania
   1. Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej
   2. Oprogramowanie musi tworzyć “samowystarczalne” archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków
   3. Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji
   4. Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu.
   5. Oprogramowanie musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć jedną wirtualną pulę pamięci na kopie zapasowe. Wymagane jest wsparcie dla nieograniczonej liczby pamięci masowych to takiej puli.
   6. Oprogramowanie musi pozwalać na tworzenie repozytorium kopii zapasowych bezpośrednio na zasobach Microsoft AzureBlob, Google Cloud Storage, Amazon S3, Wasabi Cloud Storage oraz na innych kompatybilnych z S3 przestrzeniach obiektowych. Dodatkowo, oprogramowanie musi wspierać archiwizowanie tych danych do Microsoft Azure Archive Blob Storage oraz Amazon S3 Glacier.
   7. Oprogramowanie musi wspierać niezmienność kopii zapasowych na potrzeby ochrony przed ransomware poprzez niedopuszczenie do usunięcia lub modyfikacji kopii zapasowej w zadanym okresie czasu.
   8. Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania
   9. Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL, Oracle oraz PostgreSQL (w tym odtwarzanie point-in-time)
   10. Oprogramowanie musi zapewniać możliwość delegacji uprawnień do odtwarzania na portalu
   11. Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API
   12. Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji
   13. Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji
   14. Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania
   15. Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.
   16. Oprogramowanie musi posiadać natywne mechanizmy uwierzytelniania wieloskładnikowego (MFA) w celu dostępu do konsoli administracyjnej
3. Wymagania RPO
   1. Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej
   2. Oprogramowanie musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych.
   3. Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta musi być dostępna na wszystkich wspieranych platformach wirtualizacyjnych z dokładnością do pojedynczego datastoru
   4. Oprogramowanie musi zapewniać tworzenie kopii zapasowych z bezpośrednim wykorzystaniem snapshotów macierzowych. Musi też zapewniać odtwarzanie maszyn wirtualnych z takich snapshotów. Proces wykonania kopii zapasowej nie może wymagać użycia jakichkolwiek hostów tymczasowych. Opisana funkcjonalność powinna działać w środowisku VMware.
   5. Oprogramowanie musi posiadać wsparcie dla VMwarevSAN potwierdzone odpowiednią certyfikacją VMware.
   6. Oprogramowanie musi wspierać kopiowanie backupów oraz zasobów plikowych na taśmy.
   7. Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son)
   8. Oprogramowanie musi wspierać bezpośrednią integrację z urządzeniami deduplikacyjnymi. Minimalnie wsparcie wymagane dla Dell DataDomain, HPE StoreOnce, ExaGrid, Fujitsu CS800, Quantum DXi oraz InfinidatInfiniGuard.
   9. Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016, 2019 lub 2022 z systemem pliku ReFS jako repozytorium backupu. Podobna funkcjonalność musi być zapewniona dla repozytoriów opartych o linuxowy system plików XFS.
   10. Oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN.
   11. Oprogramowanie musi mieć możliwość replikacji asynchronicznej włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMwarevSphere pomiędzy hostami ESXi oraz pomiędzy hostami Hyper-V. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji.
   12. Oprogramowanie musi mieć możliwość replikacji ciągłej, opartej o VMware VAIO, włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMwarevSphere. Dla replikacji ciągłej musi być możliwość zdefiniowania dziennika pozwalającego na odzyskanie danych z dowolnego punku w ramach ustalonego parametru RPO.
   13. Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik
   14. Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replicaseeding)
   15. Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN)
4. Wymagania RTO
   1. Oprogramowanie musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware, Hyper-V oraz Nutanix AHV niezależnie od rodzaju storage’u użytego do przechowywania kopii zapasowych.
   2. Dodatkowo dla środowiska vSphere, Hyper-V i Nutanix AHV powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna)
   3. Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w hypervisor. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie musi realizować taką migrację swoimi mechanizmami
   4. Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSpehre
   5. Oprogramowanie musi pozwalać na uruchomienie zasobów plikowych SMB oraz baz danych MS SQL i Oracle bezpośrednio ze skompresowanego i skompresowanego pliku backupu. Dodatkowo wspierana musi być migracja on-line tak uruchomionych zasobów na środowisko produkcyjne.
   6. Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków
   7. Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft AzureStack, Amazon EC2 oraz Google Cloud Platform.
   8. Oprogramowanie musi umożliwić odtworzenie plików/folderów lub ich uprawnień na maszynę operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików
   9. Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy natywnego API dla platformy VMware i PowerShell Direct dla platformy Hyper-V.
   10. Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, BSD, Solaris, Mac, Novell
   11. Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM oraz Windows Storage Spaces.
   12. Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej.
   13. Oprogramowanie musi wspierać granularne odtwarzanie obiektów Active Directory takich jak konta komputerów, konta użytkowników, dowolnych atrybutów, rekordów DNS zintegrowanych z AD, Microsoft System Objects, certyfikatów CA, elementów AD Sites oraz pozwalać na odtworzenie haseł.
   14. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2013SP1 i nowszych (dowolny obiekt w tym obiekty w folderze "PermanentlyDeleted Objects"). Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego.
   15. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2008 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku point-in-time, całych baz lub pojedynczych tabeli, widoków oraz procedur.
   16. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2013 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku całych witryn, bibliotek oraz pojedynczych dokumentów wraz z historią ich wersji.
   17. Oprogramowanie musi wspierać granularne odtwarzanie baz danych Oracle z opcją odtwarzanie point-in-time wraz z włączonym Oracle DataGuard. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Windows oraz Linux.
   18. Oprogramowanie musi wspierać granularne odtwarzanie baz danych PostgreSQL z opcją odtwarzanie point-in-time. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Linux.
   19. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez Oracle RMAN
   20. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez SAP HANA, SAP Oracle
   21. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez MS SQL VDI
   22. Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN
5. Ograniczenie ryzyka
   1. Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu. Powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna)
   2. Dla VMware’a oprogramowanie musi pozwalać na uruchomienie takiego środowiska dla replik maszyn wirtualnych oraz bezpośrednio ze snapshotów macierzowych stworzonych na wspieranych urządzeniach.
   3. Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem
   4. Oprogramowanie musi umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem jakichkolwiek danych. Integracja musi być zapewniona minimalnie dla Windows Defender, Symantec Protection Engine oraz ESET NOD32.
   5. Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego.
6. Środowiska fizyczne
   1. Rozwiązanie musi wykonywać kopię zapasową systemu Windows oraz Linux wykorzystując agenta znajdującego się wewnątrz systemu operacyjnego
   2. Rozwiązanie musi wspierać systemy operacyjne Windows w wersjach klienckich oraz serwerowych
   3. Rozwiązanie musi wspierać co najmniej następujące dystrybucje systemów Linux: Debian, Ubuntu, RHEL, CentOS, Oracle Linux, SLES, Fedora, openSUSE
   4. Rozwiązanie musi wspierać system operacyjny macOS
   5. Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, MacOS, Unix
   6. Rozwiązanie musi mieć możliwość instalacji oraz zarządzania wykorzystując tryb niezależny (per agent) jak również zcentralizowany (poprzez centralną konsolę zarządzającą)
   7. Rozwiązanie musi wspierać systemy oparte o Microsoft Failover Cluster
   8. Rozwiązanie musi wspierać zabezpieczanie do oraz odzyskiwanie z urządzeń blokowych pozwalając na odzysk całej maszyny (tzw. bare metal recovery) wybranych wolumenów, oraz wybranych plików i folderów
   9. Rozwiązanie musi wspierać backup podłączonych dysków USB
   10. Kopia zapasowa całej maszyny oraz pojedynczych wolumenów musi być wykonywana na poziomie blokowym
   11. Rozwiązanie musi pozwalać na przechowywanie kopii zapasowych na zasobach lokalnych (wewnętrznych) dyskach zabezpieczanej maszyny, Direct Attached Storage (DAS), takich jak zewnętrzne dyski USB, eSATA lub Firewire, Network Attached Storage (NAS) pozwalającym na wystawienie swoich zasobów poprzez SMB (CIFS) lub NFS, bezpośrednio na zasobach obiektowych (w tym chmury)
   12. Rozwiązanie musi wspierać deduplikacje oraz kompresję na źródle. Dane wysyłane na repozytorium muszą być już odpowiednio przetworzone
   13. Rozwiązanie musi wspierać kontrolę pasma sieciowego
   14. Rozwiązanie musi wspierać ograniczenie wykonywania backupów dla konkretnych sieci bezprzewodowych
   15. Rozwiązanie musi wspierać ograniczenia wykonywania backupów dla połączeń VPN
   16. Rozwiązanie musi wspierać śledzenie zmienionych bloków podczas wykonywania kopii zapasowych. Dla systemów Windows technologia śledzenia bloków dla systemów serwerowych musi być certyfikowana przez Microsoft
   17. Rozwiązanie musi wspierać technologię BitLocker
   18. Rozwiązanie musi wspierać uruchamianie z nośnika odtwarzania
   19. Rozwiązanie musi wspierać odzysk pojedynczych elementów aplikacji z jednoprzebiegowej kopii zapasowej dla Microsoft Exchange 2013SP1 i nowszych, Microsoft Active Directory 2008 i nowszych, Microsoft Sharepoint 2013 i nowszych, Microsoft SQL 2008 i nowszych, Oracle 11g i nowszych oraz PostgreSQL 12 i nowszych
   20. Rozwiązanie musi wspierać odzysk do konkretnego punktu w czasie (point-in-time) dla wspieranych systemów bazodanowych
   21. Rozwiązanie musi umożliwiać natychmiastowe publikowanie baz MS SQL i Oracle poprzez bezpośrednie uruchomienie ich z pliku backupu.
   22. Rozwiązanie musi wspierać odzysk obrazów kopii zapasowych bezpośrednio do vSphere, Hyper-V, Nutanix AHV, Microsoft Azure, Microsoft AzureStack, Amazon EC2 oraz Google Cloud Platform
   23. Rozwiązanie musi wspierać szyfrowanie
   24. Rozwiązanie musi wspierać możliwość wykonywania kopii zapasowych stacji klienckich, lokalnie do repozytorium tymczasowego (cache) gdy połączenie sieciowe do głównego repozytorium kopii zapasowych jest niedostępne
   25. Rozwiązanie musi posiadać funkcjonalność automatycznego zmniejszenia szybkości przetwarzania danych, aby nie dopuścić do obniżenia wydajności systemu zabezpieczanego
   26. Rozwiązanie musi posiadać ochronę przed ransomware poprzez automatyczne odmontowanie nośnika po wykonanym backupie stacji klienckiej
   27. Rozwiązanie musi wspierać tworzenie wielu zadań backupowych
   28. Subskrypcja na minimum 36 miesięcy dla minimum 50 maszyn wirtualnych i 1 serwera fizycznego.
7. Wdrożenie i wsparcie techniczne

Usługa obejmuje realizacje:

1. Analizy przedwdrożeniowej środowiska IT Zamawiającego
2. Instalacja systemu
3. Wdrożenie wymaganych polityk backupu
4. Podłączenie posiadanej biblioteki taśmowej
5. Uruchomienie dodatkowego repozytorium - „Cyfrowy bunkier”
6. Codzienna weryfikacja wykonania wszystkich polityk backupu
7. Raportowanie o nieprawidłowościach
8. Gotowość do udzielenia wsparcia technicznego
9. Ryczałt w wymiarze 50 godzin rocznie, na prace serwisowe związane z backupem
10. Co miesięczne odtworzenie kopii systemów: Eskulap na serwerze odtworzeniowym

Wraz z weryfikacją odtworzonych systemów poprzez fizyczne zalogowanie i zrealizowaniescenariuszy testowych

1. Przekazanie raportu z odtworzenia wraz z dowodami działania systemu
2. Przekazanie dokumentacji aktualizującej Politykę bezpieczeństwa w zakresie odtwarzania backupów

Monitoring kopii zapasowych

* Usługa polega na konfiguracji środowiska do monitorowania statusów wykonywanych kopii zapasowych krytycznych zasobów infrastruktury IT, a w szczególności infrastruktury środowiska Eskulap. Ma na celu zapobieganie, poprzez informowanie z odpowiednim wyprzedzeniem administratorów szpitala, o potencjalnych problemach oraz zagrożeniach w wykonaniu kopii zapasowych danych usług oraz serwisów.
* Konfiguracja musi obejmować przygotowanie serwera monitorowania, przygotowanie oraz personalizację szablonów, konfigurację powiadomień oraz podpięcie do monitorowania systemu kopii zapasowych środowiska Eskulap działającego u Zamawiającego.
* Usługa odtworzenia systemu Eskulap z kopii zapasowych na środowisku odtworzeniowym Zamawiającego
* Wykonywana będzie minimum raz na 30 dni, w okresie trwania usługi oraz po przekazaniu niezbędnych dostępów do infrastruktury. Realizowana będzie przy użyciu wdrażanych przez Wykonawcę mechanizmów kopii zapasowych, które są tak skonfigurowane, że umożliwiają odtworzenie danych bezpośrednio na środowisku odtworzeniowym. Zamawiający przekaże wymaganą dokumentację środowiska kopii zapasowych, środowiska odtworzeniowego oraz niezbędne dane dostępowe. Po każdym odtworzeniu Wykonawca musi sporządzić raport, który zawierał będzie informacje o przeprowadzonych pracach a w szczególności z których kopii zostało wykonane odtworzenie, ile czasu trwało odtworzenie oraz które elementy systemów podlegały testowi odtworzenia.
* Po odtworzeniu Wykonawca dokona weryfikacji środowiska i potwierdzi poprawność odtworzenia zgodnie z ustalony scenariuszami testowymi.
* Po odtworzeniu Wykonawca przekaże raport z odtworzenia wraz z dowodami działania systemu - logi

3.3.2. Biblioteka taśmowa 1 szt.

|  |  |
| --- | --- |
| **Parametry techniczne** | |
|  | Obudowa przystosowana do montażu w standardowej szafie rack 19’’. Maksymalna wysokość oferowanego rozwiązania - 3U. |
|  | Biblioteka taśmowa musi być wyposażona w min. 1 napęd taśmowy LTO8 z interfejsem FC min. 8 Gbit/s. |
|  | Biblioteka taśmowa musi mieć możliwość rozbudowy do min. 8 napędów taśmowych. |
|  | Biblioteka musi być wyposażona w nie mniej niż 20 slotów na taśmy i posiadać możliwość rozbudowy do co najmniej 100 slotów na taśmy. |
|  | Biblioteka musi być wyposażona w przynajmniej 3 sloty wejścia/wyjścia, umożliwiający wymianę taśm bez konieczności wyłączania urządzenia. |
|  | Biblioteka musi być wyposażona w czytnik kodów kreskowych. |
|  | Biblioteka musi być wyposażona w komplet magazynków na taśmy, tak by możliwa była pełna obsada biblioteki taśmami LTO. |
|  | Możliwość zdalnego zarządzania biblioteką poprzez interfejs WWW. |
|  | Możliwość monitorowania stanu biblioteki i napędów. |
|  | Biblioteka musi posiadać panel sterowania oraz wyświetlacz informujący o błędach urządzenia, aktywności napędów. |
| **Parametry dodatkowe** | |
|  | Do biblioteki należy dostarczyć:  - niezbędne kable zasilające,  - taśmę LTO 8 – 20 szt.  - taśmę czyszczącą – 1 szt.  - przewód światłowodowy – 1 szt. |
|  | Dostarczone urządzenie musi mieć zainstalowane wszystkie najnowsze zestawy poprawek dotyczących dostarczanego sprzętu. |
|  | Wszystkie oferowane urządzenia muszą być fabrycznie nowe. |
|  | Urządzenia i ich komponenty muszą być oznakowane przez producenta w taki sposób, aby możliwa była identyfikacja zarówno produktu jak i producenta. |
|  | Urządzenia muszą współpracować z siecią energetyczną o parametrach: 230 V ± 10%, 50 Hz. |
|  | Oferowane produkty (urządzenia, sprzęty) w przedmiotowym postępowaniu o udzielenie zamówienia publicznego muszą spełniać wymagania norm CE, tj. muszą spełniać wymogi niezbędne do oznaczenia produktów znakiem CE. |
|  | Urządzanie musi być objęta 36 miesięczną gwarancją |
|  | Serwis gwarancyjny musi obejmować dostęp do poprawek i nowych wersji oprogramowania wbudowanego, które są elementem zamówienia przez cały okres obowiązywania gwarancji. |

3.3.3. Wsparcie Fortigate

Przedłużenie obecnego wsparcia dla FortiGate: FG-100F; S/N: FG100FTK21038713do 2029-05-31

3.3.4. System bezpieczeństwa poczty 1 szt.

Wymagania ogólne

System ochrony poczty musi zapewniać kompleksową ochronę antyspamową, antywirusową oraz antyspyware’ową bez limitu licencyjnego na ilość chronionych kont użytkowników.

Dopuszcza się, aby poszczególne elementy wchodzące w skład systemu ochrony były zrealizowane w postaci osobnych, komercyjnych platform wirtualnych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia w środowisku wirtualnym. W przypadku implementacji programowej dostawca musi zapewnić platformę w postaci odpowiednio zabezpieczonego systememu operacyjnego, na którym będzie instalowane rozwiązanie. Platformy muszą mieć możliwość uruchomienia na co najmniej następujących hypervisorach: VMware ESX/ESXi 5.0/5.1/5.5/6.0/6.5/7.0, Microsoft Hyper-V 2008 R2/2012/2012 R2/2016, CitrixXenServer 6.0+, Open Source Xen 4.1+, KVM, AWS (Amazon Web Services), Microsoft Azure.

Dla zapewnienia wysokiej sprawności i skuteczności działania rozwiązanie musi pracować w oparciu o komercyjne bazy zabezpieczeń.

Dostarczone rozwiązanie musi mieć możliwość pracy w każdym trybów:

1. Tryb Gateway.
2. Tryb transparentny (nie wymaga rekonfiguracji istniejącego systemu poczty elektronicznej).

Parametry fizyczne systemu antyspamowego

1. System musi obsługiwać co najmniej 4 interfejsy sieciowe oraz wspierać powierzchnię dyskową o pojemności co najmniej 2 TB.

Funkcja serwera poczty

W ramach oferowanego systemu musi zostać dostarczony moduł realizujący funkcję serwera poczty umożliwiający zdefiniowanie co najmniej 400 lokalnych skrzynek pocztowych. Moduł serwera poczty musi integrować się z serwerem LDAP obsługując tym samym pełną listę zdefiniowanych tam użytkowników i przypisanych do nich kont pocztowych.

Funkcje serwera poczty

W tym zakresie dostarczony system musi zapewniać:

1. Obsługę serwisów pocztowych: SMTP, POP3, IMAP.
2. Wsparcie szyfrowania komunikacji: SMTP over SSL (w tym zakresie musi wspierać protokoły: SSL, TLS 1.0, TLS 1.1 oraz TLS 1.2).
3. Definiowanie powierzchni dyskowej dedykowanej dla poszczególnych użytkowników.
4. Szyfrowany dostęp do poczty poprzez WebMail – z wykorzystaniem protokołu SSL (w tym zakresie musi wspierać protokoły: SSL, TLS 1.0, TLS 1.1, TLS 1.2 oraz TLS 1.3).
5. Polski interfejs użytkownika przy dostępie przez WebMail.
6. Lokalne konta użytkowników oraz możliwość czerpania kont pocztowych z zewnętrznego serwera LDAP.
7. Uwierzytelnianie użytkowników w oparciu o: bazę lokalną, zewnętrzny LDAP, Radius oraz protokoły: SMTP, POP3, IMAP.

Ogólne funkcje systemu ochrony poczty

Dostarczany system obsługi i ochrony poczty musi zapewniać poniższe funkcje:

1. Wsparcie dla co najmniej 70 domen pocztowych.
2. System musi realizować skanowanie antyspamowe i antywirusowe z wydajnością min. 50 tys. wiadomości/godzinę.
3. Polityki filtrowania poczty tworzone co najmniej w oparciu o: adresy mailowe, nazwy domenowe, adresy IP (w szczególności powinna być możliwość definiowania reguł all-all).
4. Email routing w oparciu o reguły lokalne lub w oparciu o zewnętrzny serwer LDAP.
5. Zarządzanie kolejkami wiadomości (np. reguły opóźniania dostarczenia wiadomości).
6. Możliwość ograniczenia ilości poczty wychodzącej do chronionych domen w oparciu o nie mniej niż: ilość jednoczesnych sesji, maksymalną liczbę wiadomości w ramach sesji, maksymalną liczbę odbiorców w zadanym czasie.
7. Ochrona i analiza zarówno poczty przychodzącej jak i wychodzącej.
8. Szczegółowe, wielowarstwowe polityki wykrywania spamu oraz wirusów.
9. Możliwość tworzenia polityk kontroli Antywirusowej oraz Antyspamowej w oparciu o użytkownika i atrybuty zwracane z zewnętrznego serwera LDAP.
10. Kwarantanna poczty z dziennym podsumowaniem dla użytkownika z możliwością samodzielnego zwalniania bądź usuwania wiadomości z kwarantanny przez użytkownika.
11. Możliwość poddania ponownemu skanowaniu (antywirus, sandbox) wiadomości w momencie uwalniania ich z kwarantanny użytkownika lub administratora.
12. Dostęp do kwarantanny użytkownika możliwy poprzez WebMail.
13. Archiwizacja poczty przychodzącej i wychodzącej w oparciu o polityki.
14. Możliwość przechowywania poczty oraz jej backup realizowany lokalnie na dysku systemu oraz na zewnętrznych zasobach, co najmniej: NFS, iSCSI.
15. Białe i czarne listy adresów mailowych definiowane globalnie oraz dla domen wskazanych przez administratora systemu.
16. Białe i czarne listy adresów mailowych dla poszczególnych użytkowników.
17. Ochrona przed wyciekiem informacji poufnej DLP (Data LeakPreention).
18. Skanowanie załączników zaszyfrowanych. Odszyfrowywanie ich w oparciu o nie mniej niż: słowa zawarte w wiadomości pocztowej, wbudowaną listę haseł, listę haseł zdefiniowaną przez użytkownika.

Kontrola antywirusowa i ochrona przed malware

W tym zakresie dostarczony system ochrony poczty musi zapewniać:

1. Skanowanie antywirusowe wiadomości SMTP.
2. Kwarantannę dla zainfekowanych plików.
3. Skanowanie załączników skompresowanych.
4. Definiowanie komunikatów powiadomień w języku polskim.
5. Blokowanie załączników w oparciu o typ pliku.
6. Możliwość zdefiniowania nie mniej niż 200 polityk kontroli antywirusowej.
7. Moduł kontroli antywirusowej musi mieć możliwość współpracy z dedykowaną, komercyjną platformą (sprzętową lub wirtualną) lub usługą w chmurze typu Sandbox w celu rozpoznawania nieznanych dotąd zagrożeń. Rozwiązanie musi umożliwiać zatrzymanie poczty w dedykowanej kolejce wiadomości do momentu otrzymania werdyktu.
8. Definiowanie różnych akcji dla poszczególnych metod wykrywania wirusów i malware'u. Powinny one obejmować co najmniej: tagowanie wiadomości, dodanie nowego nagłówka, zastąpienie podejrzanej treści lub załącznika, akcje discard lub reject, dostarczenie do innego serwera, powiadomienie administratora.
9. Ochronę typu wirus outbrake.

Kontrola antyspamowa

System musi zapewniać poniższe funkcje i metody filtrowania spamu:

1. Reputacja adresów źródłowych IP oraz domen pocztowych w oparciu o bazy producenta.
2. Filtrowanie poczty w oparciu o sumy kontrolne wiadomości dostarczane przez producenta rozwiązania.
3. Szczegółowa kontrola nagłówka wiadomości.
4. Analiza Heurystyczna.
5. Współpraca z zewnętrznymi serwerami RBL, SURBL.
6. Filtrowanie w oparciu o filtry Bayes’a z możliwością uczenia przez administratora globalnie dla całego systemu lub dla poszczególnych chronionych domen.
7. Możliwością dostrajania filtrów Bayes’a przez poszczególnych użytkowników.
8. Wykrywanie spamu w oparciu o analizę plików graficznych oraz plików PDF.
9. Kontrola w oparciu o Greylisting oraz SPF.
10. Filtrowanie treści wiadomości i załączników.
11. Kwarantanna zarówno użytkowników jak i systemowa z możliwością edycji nagłówka wiadomości.
12. Możliwość zdefiniowania nie mniej niż 200 polityk kontroli antyspamowej.
13. Ochrona typu outbrake.
14. Filtrowanie poczty w oparciu o kategorie URL (co najmniej: malware, hacking).
15. Definiowanie różnych akcji dla poszczególnych metod wykrywania spamu. Powinny one obejmować co najmniej: tagowanie wiadomości, dodanie nowego nagłówka, akcje discard lub reject, dostarczenie do innego serwera, powiadomienie administratora.

Ochrona przed atakami na usługę poczty

System musi zapewniać poniższe funkcje i metody filtrowania:

1. Ochrona przed atakami na adres odbiorcy (m.in. email bombing).
2. Definiowaniemaksymalnej ilości wiadomości pocztowych otrzymywanych w jednostce czasu.
3. Defniowanie maksymalnej liczby jednoczesnych sesji SMTP w jednostce czasu.
4. Kontrola Reverse DNS (ochrona przed Anty-Spoofing).
5. Weryfikacja poprawności adresu e-mail nadawcy.

Funkcje logowania i raportowania

W tym zakresie dostarczony system ochrony poczty musi zapewniać:

1. Logowanie do zewnętrznego serwera SYSLOG.
2. Logowanie zmian konfiguracji oraz krytycznych zdarzeń systemowych np. w przypadku przepełnienia dysku.
3. Logowanie informacji na temat spamu oraz niedozwolonych załączników.
4. Możliwość podglądu logów w czasie rzeczywistym jak również danych historycznych.
5. Możliwość analizy przebiegu sesji SMTP.
6. Powiadamianie administratora systemu w przypadku wykrycia wirusów w przesyłanych wiadomościach pocztowych.
7. Predefiniowane szablony raportów oraz możliwość ich edycji przez administratora systemu.
8. Możliwość generowania raportów zgodnie z harmonogramem lub na żądanie administratora systemu.

Funkcje pracy w trybie wysokiej dostępności (HA)

System ochrony poczty musi zapewniać poniższe funkcje:

1. Konfigurację HA w każdym ztrybów: gateway, transparent.
2. Tryb synchronizacji konfiguracji dla scenariuszy gdy każde z urządzeń występuje pod innym adresem IP.
3. Wykrywanie awarii poszczególnych urządzeń oraz powiadamianie administratora systemu.
4. Monitorowanie stanu pracy klastra.
5. W ramach postępowania wymaganym jest dostarczenie systemu w formie klastra realizującego funkcje podstawowe, gdzie każdy jego element charakteryzuje się parametrami fizycznymi i funkcjonalnymi opisanymi w tym dokumencie.

Aktualizacje sygnatur, dostęp do bazy spamu

W tym zakresie dostarczony system ochrony poczty musi zapewniać:

1. Pracę w oparciu o bazę spamu oraz url uaktualniane w czasie rzeczywistym.
2. Planowanie aktualizacji szczepionek antywirusowych zgodnie z harmonogramem co najmniej raz na godzinę.

Zarządzanie

System ochrony poczty musi zapewniać poniższe funkcje:

1. System musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH.
2. Możliwość modyfikowania wyglądu interfejsu zarządzania oraz interfejsu WebMail z opcją wstawienia własnego logo firmy.
3. Powinna istnieć możliwość zdefiniowania co najmniej 3 lokalnych kont administracyjnych.

Certyfikaty

Dostarczony system powinien posiadać co najmniej dwie z poniższych certyfikacji:

1. VBSpam, VB100 rated, Common Criteria NDPP, FIPS 140-2 Certified.

Serwisy i licencje

System musi być dostarczony w modelu „na własność” tj. niewykupienie odnowienia licencji wsparcia technicznego dla rozwiązania nie spowoduje zablokowania funkcjonowania systemu a jedynie pozbawi możliwości pobierania aktualizacji oprogramowania.

W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producentai serwisów. Powinny one obejmować:

1. Kontrola Antyspam, URL Filtering, kontrola antywirusowa, ochrona typu VirusOutbrake na okres 36 miesięcy.

3.3.5. Switch core 2 szt.

**Porty przełącznika**: minimum 48\*10G (SFP+), minimum 6\*40/100G (QSFP28) z możliwością rozszycia każdego portu na 4x10G lub 4x25G

**Stackowanie:** możliwość połączenia minimum 4 przełączników w stos za pomocą portów SFP+ lub QSFP28 bez dedykowanego okablowania

**Matryca przełączająca**: 2160 Gb/s

**Przepustowość pakietów**: minimum 600 Mp/s (dla pakietów 64Kb)

**Pojemność tablicy MAC**: minimum 32k

**Tablica routingu:** minimum 16k

**Tablica ARP:** minimum 8k

**Pamięć Flash:** minimum 32M SPI + 8G MMC

**Pamięć RAM:** minimum 4GB

**Zasilanie urządzenia**: minimum dwa modularne, zasilacze hot-swap - 230VAC

**Pobór mocy:** maksimum 130W

**Chłodzenieurządzenia:** min. 3 aktywne + 1 redundantny wentylator, modularne

**Certyfikaty bezpieczeństwa**: CE, RoHS

**Ilość wpisów tablicy ACL**: minimum 1k

**Ilość aktywnych IEEE802.1Q VLAN**: minimum 4k

**Funkcje L1, L2:** Port Loopback Detect, LLDP and LLDP-MED, UDLD, 802.3ad LACP, 127 groups, LACP Load Balance, N:1 Port Mirroring, RSPAN, ERSPAN, IEEEE802.1d(STP), IEEEE802.1w(RSTP), IEEEE802.1s(MSTP), Root Guard, BPDU Guard, BPDU Tunnel, ERPS(ITU-T G.8032), 802.1Q, MAC VLAN, VOICE VLAN, Private VLAN, Protocol VLAN, Multicast VLAN, QinQ, Flexible QinQ, GVRP, N:1 VLAN Translation, Broadcast / Multicast / Unicast Storm Control, IGMP v1/v2/v3 Snooping and L2 Query, ND Snooping, MLDv1/v2 Snooping, Port Security, Flow control: HOL, IEEE802.3x, Bandwidth Control

**Ruting L3**: Static Routing, RIPv1/v2, OSPFv2, BGP4, OSPFv3, BGP4+, OSPF Multiple Process, LPM Routing, Policy-based Routing (PBR) for IPv4 and IPv6, VRRP, URPF, ECMP, BFD, IGMP v1/v2/v3, IGMP Proxy, DVMRP, PIM-DM, PIM-SM, PIM-SSM, any cast RP, MSDP, Static Multicast Route, Multicast Receive Control, Illegal Multicast Source Detection, ARP Guard, Local ARP Proxy, Proxy ARP, ARP Binding, Gratuitous ARP, ARP Limit, Anti ARP Cheat, Anti ARP Scan, DNS Client, GRE Tunnel

**IPv6:** 6to4 Tunnel, Configured Tunnel, ISATAP Tunnel, GRE Tunnel, ICMPv6, ND, DNSv6, IPv6 LPM Routing, IPv6 Policy-Based Routing (PBR), IPv6 VRRPv3, IPv6 URPF, IPv6 RA, RIPng, OSPFv3, BGP4+, MLD Snooping, IPv6 multicast VLAN, MLDv1/v2, PIM-SM/DM for IPv6, IPv6 Anycast RP, IPv6 ACL, IPv6 QOS

**Funkcje QoS:** 8 Queues, SP/WDRR/SP+WDRR, Traffic Classification Based on 802.1p CoS, ToS, DiffServ DSCP, ACL, port number, Traffic Shaping, PRI Mark/Remark

**Lista kontrolidostępu:** IP ACL, MAC ACL, IP-MAC ACL, Standard and Expanded ACL Based on source/destination IP or MAC, IP protocol, TCP/UDP port, DSCP, ToS, IP Precedence), VLAN, Tag/Untag, CoS, REDIRECT and accounting-based ACL, Rules can be configured to port, VLAN, Time ranged ACL

**Bezpieczeństwo:** 802.1x AAA, Port, MAC based authentication, Accounting based on time length and traffic, Guest VLAN and Auto VLAN, RADIUS for IPv4 and IPv6, TACACS+ for IPv4 and IPv6, MAB

**DHCPv4/v6:** DHCP Server/Client for IPv4/IPv6, DHCP Relay/Option 82, DHCP Snooping/Option 82

**Traffic Monitor:**sFlow Traffic Analysis

**Zarządzanie**: CLI, WEB, Telnet, SNMPv1/v2c/v3 through IPv4 and IPv6, Syslog and external Syslog server, HTTP SSL, SNMP MIB, SNMP TRAP, FTP/TFTP, SNTP/NTP, RMOM 1,2,3,9, Authentication by radius, SSH v1/v2, Dual firmware images/ Configuration files, 802.3ah OAM, 802.1ag OAM

**Firmware oraz konfiguracja**: oprogramowanie przełącznika (firmware) dostępny bez ograniczeń czasowych, przez cały okres cyklu życiowego urządzenia poprzez Internet, wsparcie techniczne producenta lub dystrybutora bez konieczności wykupu dodatkowych usług, możliwość wgrania kilku plików z obrazem lub konfiguracją systemu, możliwość wgrania oprogramowania oraz konfiguracji poprzez TFTP/FTP,

3.3.6. Switch brzegowy 18 szt.

**Porty przełącznika**: minimum 48x 10/100/1000Base-T RJ45 PoE oraz minimum 4x 1/10GBase-X SFP+

**Port konsolowy:** RJ45 (RS-232)

**Port USB:** minimum 1 port co najmniej w standardzie 2.0

**Szybkość przełączania:** minimum176Gb/s

**Przepustowość:** minimum131Mp/s (dla pakietów 64Kb)

**Bufor pakietów:** minimum3 MB

**Ramki Jumbo:** minimum10k

**Tablicaadresów MAC:** minimum16k

**Adresy MAC – Multicast:** minimum 4k

**Tablica ACL:** minimum 512

**Tablica VLAN:** minimum 4k

**Taktowanie procesora:** minimum 800MHz

**Pamięć Flash:** minimum 32MB + Nand 128MB

**Pamięć RAM:** minimum 256MB

**Obsługa technologii PoE:** IEEE 802.3 af/at

**Budżet mocy PoE:** minimum 740W

**Temperatura pracy:** zakres minimum 0°C – 50°C

**Wilgotność względna:** zakres minimum 10% - 90% (bez kondensacji)

**Zasilanie:** zabudowany zasilacz 230V AC

**Pobór mocy:** maksymalnie 897W

**Zabezpieczenie przeciwprzepięciowe:** minimum 6kV

**Wymiary:** maksymalna: szerokość 440 mm, wysokość 44mm , głębokość 320mm

**Certyfikaty bezpieczeństwa**: CE, RoHS

**Algorytm:** Store and Forward

**VLAN:** Voice VLAN, Port based VLAN, MAC based VLAN, Protocol based VLAN, Private VLAN, VLAN Translation, N:1 VLAN Translation, GVRP, IEEE 802.1Q, Normal QinQ, Flexible QinQ

**DHCP:** Ipv4/Ipv6 DHCP Client,Ipv4/Ipv6 DHCP Relay, Option 82, Ipv4/Ipv6 DHCP Snooping,Ipv4/Ipv6 DHCP Server

**Spanning tree:** IEEE802.1D (STP), IEEE802.1W (RSTP), IEEE802.1S (MSTP), Multi-Process MSTP, Root Guard, BPDU guard, BPDU forwarding

**Protekcjaringowa:** ITU-T G.8032 – recovery time < 50ms, Fast Link, Loopback Detection

**Agregacjałączy:** IEEE 802.3ad (LACP), 64 groups per device / 8 ports per group, load balance

**Bezpieczeństwo:** Storm Control based on packets, Port Security, MAC Limit based on VLAN and Port, Anti-ARP-Spoofing , Anti-ARP-Scan, ARP Binding, Gratuitous ARP, ARP Limit, Anti ARP/NDP Cheat, Anti ARP Scan, ND Snooping, DAI, IEEE 802.1x, Authentication, Authorization, Accounting, Radius Ipv4/Ipv6, TACACS+, MAB, Port and MAC based authentication, Accounting based on time length and traffic, Guest VLAN and auto VLAN,

**Multicast:** IGMP v1/v2/v3 snooping and L2 Query, IGMP Fast leave, MVR, MLD v1/v2 Snooping, Ipv4/Ipv6 DCSCM, IGMP authentication

**QoS:** 8 queques per port, Bandwidth Control, Flow Control: HOL, IEEE802.3x, Flow Redirect, Classification based on ACL, COS, TOS, DiffServ, DSCP, port number; Traffic Policing, PRI Mark/Remark, IEEE 802.1p, Queuing Method: Strict Priority, Weighted Deficit Round Robin, Strict priority in Weighted Deficit Round Robin; DNS Client, DNS Relay

**Lista kontrolidostępu:** IP Src/Dst ACL, MAC Src/Dst ACL, MAC-IP ACL, User-Defined ACL, Time Range ACL, port number TCP/UDP ACL, VLAN ACL, REDIRECT and Statistics based on ACL, Precedence, Vlan Tag/Untag, Rules can be configured to port and VLAN

**Diagnostyka:** sFlow, Traffic Analysis, RSPAN, VCT, Ping, Trace Route

**Zarządzanie:** TFTP/FTP, CLI, Telnet, Console, Web/SSL (Ipv4/Ipv6), SSH (Ipv4/Ipv6), SNMP v1/v2c/v3, SNMP Trap, Public & Private MIB interface, RMON 1,2,3,9, Syslog (Ipv4/Ipv6), SNTP/NTP (Ipv4/Ipv6), Dual IMG, Multiple Configuration Files, Port Mirror, IEEE 802.3ah/802.1ag OAM, ULDP (like UDLD), LLDP/LLDP MED., VSF (4 devices in one stack) – hardware stacking

**Funkcje PoE:** Support IEEE 802.3at for all ports, PD failure detection, PoE scheduling, Continuous powering during switches restart

**Oprogramowanie oraz wsparcie techniczne:** oprogramowanie przełącznika (firmware) dostępne bez ograniczeń czasowych, przez cały okres cyklu życia urządzenia, poprzez Internet, wsparcie techniczne dystrybutora bez konieczności wykupu dodatkowych usług

3.3.7. System antywirusowy z EDR 200 szt.– rozbudowa i przedłużenie posiadanego wsparcia do 31.05.2029

Opis wymagań dostarczanego systemu:

1. Pełne wsparcie dla systemu Windows8/Windows 8.1/Windows 10/Windows 11
2. Wersja programu dla stacji roboczych Windows dostępna co najmniej w języku polskim.

Ochrona antywirusowa i antyspyware

1. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
2. Wbudowana technologia do ochrony przed rootkitami.
3. Wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
4. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
5. System ma oferować administratorowi możliwość definiowania zadań w harmonogramie w taki sposób, aby zadanie przed wykonaniem sprawdzało czy komputer pracuje na zasilaniu bateryjnym i jeśli tak – nie wykonywało danego zadania.
6. 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
7. Możliwość określania poziomu obciążenia procesora (CPU) podczas skanowania „na żądanie” i według harmonogramu.
8. Możliwość automatycznego wyłączenia komputera po zakończonym skanowaniu.
9. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji programu.
10. Użytkownik musi posiadać możliwość tymczasowego wyłączenia ochrony na czas co najmniej 10 min lub do ponownego uruchomienia komputera.
11. Ponowne włączenie ochrony antywirusowej nie może wymagać od użytkownika ponownego uruchomienia komputera.
12. 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.
13. Wbudowany konektor dla programów MS Outlook, Outlook Express, Windows Mail i Windows Live Mail (funkcje programu dostępne są bezpośrednio z menu programu pocztowego).
14. 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).
15. Automatyczna integracja skanera POP3 i IMAP z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.
16. Możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail.
17. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie.
18. Blokowanie możliwości przeglądania wybranych stron internetowych. Listę blokowanych stron internetowych określa administrator. Program musi umożliwić blokowanie danej strony internetowej po podaniu na liście całej nazwy strony lub tylko wybranego słowa występującego w nazwie strony.
19. Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji.
20. Program ma umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
21. Program ma zapewniać skanowanie ruchu HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe.
22. Możliwość zgłoszenia witryny z podejrzeniem phishingu z poziomu graficznego interfejsu użytkownika w celu analizy przez laboratorium producenta.
23. Program musi posiadać funkcjonalność która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika.
24. Procesy zweryfikowane jako bezpieczne mają być pomijane podczas procesu skanowania na żądanie oraz przez moduły ochrony w czasie rzeczywistym.
25. Użytkownik musi posiadać możliwość przesłania pliku celem zweryfikowania jego reputacji bezpośrednio z poziomu menu kontekstowego.
26. Wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne (heurystyka) i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji (zaawansowana heurystyka). Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej i/lub obu metod jednocześnie.
27. Możliwość automatycznego wysyłania nowych zagrożeń (wykrytych przez metody heurystyczne) do laboratoriów producenta bezpośrednio z programu (nie wymaga ingerencji użytkownika). Użytkownik musi mieć możliwość określenia rozszerzeń dla plików, które nie będą wysyłane automatycznie, oraz czy próbki zagrożeń mają być wysyłane w pełni automatycznie czy też po dodatkowym potwierdzeniu przez użytkownika.
28. Do wysłania próbki zagrożenia do laboratorium producenta aplikacja nie może wykorzystywać klienta pocztowego wykorzystywanego na komputerze użytkownika.
29. Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby użytkownik siedzący przy komputerze przy próbie dostępu do konfiguracji był proszony o podanie hasła.
30. Program ma mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku jakiejś aktualizacji – poinformować o tym użytkownika i administratora wraz z listą niezainstalowanych aktualizacji.
31. Po instalacji programu, użytkownik ma mieć możliwość przygotowania płyty CD, DVD lub pamięci USB, z której będzie w stanie uruchomić komputer w przypadku infekcji i przeskanować dysk w poszukiwaniu wirusów.
32. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma umożliwiać pełną aktualizację baz sygnatur wirusów z Internetu lub z bazy zapisanej na dysku.
33. Program ma 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 , urządzeń przenośnych oraz urządzeń dowolnego typu.
34. Funkcja blokowania nośników wymiennych bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ urządzenia, numer seryjny urządzenia, dostawcę urządzenia, model.
35. Program ma umożliwiać użytkownikowi nadanie uprawnień dla podłączanych urządzeń w tym co najmniej: dostęp w trybie do odczytu, pełen dostęp, ostrzeżenie brak dostępu do podłączanego urządzenia.
36. Program ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika.
37. W momencie podłączenia zewnętrznego nośnika aplikacja musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika.
38. Użytkownik ma posiadać możliwość takiej konfiguracji programu aby skanowanie całego nośnika odbywało się automatycznie lub za potwierdzeniem przez użytkownika
39. Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS).
40. Oprogramowanie musi posiadać zaawansowany skaner pamięci.
41. Program musi być wyposażona w mechanizm ochrony przed exploitami w popularnych aplikacjach np. czytnikach PDF, aplikacjach JAVA itp.
42. Program ma 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 procesach i połączeniach.
43. Funkcja generująca taki log ma oferować filtrowanie wyników pod kątem tego, które z nich są podejrzane dla programu i mogą stanowić dla niego zagrożenie bezpieczeństwa.
44. Program ma oferować funkcję, która aktywnie monitoruje i skutecznie blokuje działania wszystkich plików programu, jego procesów, usług i wpisów w rejestrze przed próbą ich modyfikacji przez aplikacje trzecie.
45. Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń dostępna z Internetu.
46. Możliwość określenia maksymalnego czasu ważności dla bazy danych sygnatur, po upływie czasu i braku aktualizacji program zgłosi posiadanie nieaktualnej bazy sygnatur.
47. Program musi posiadać funkcjonalność tworzenia lokalnego repozytorium aktualizacji.
48. Program musi być wyposażona w funkcjonalność umożliwiającą tworzenie kopii wcześniejszych aktualizacji w celu ich późniejszego przywrócenia (rollback).
49. Program wyposażony tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne, zapora sieciowa).
50. Program ma być w pełni zgodny z technologią CISCO Network Access Control.
51. Program ma być wyposażony w dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, pracy zapory osobistej, modułu antyspamowego, kontroli stron Internetowych i kontroli urządzeń, skanowania na żądanie i według harmonogramu, dokonanych aktualizacji baz wirusów i samego oprogramowania.
52. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.
53. Program musi posiadać możliwość aktywacji poprzez podanie konta administratora licencji, podanie klucza licencyjnego oraz możliwość aktywacji programu offline.
54. W programie musi istnieć możliwość tymczasowego wstrzymania polityk wysłanych z poziomu serwera zdalnej administracji.
55. Wstrzymanie polityk ma umożliwić lokalną zmianę ustawień programu na stacji końcowej.

Ochrona przed spamem

1. Ochrona antyspamowa dla programów pocztowych MS Outlook, Outlook Express, Windows Mail oraz Windows Live Mail.
2. Program ma umożliwiać uaktywnienie funkcji wyłączenia skanowania baz programu pocztowego po zmianie zawartości skrzynki odbiorczej.
3. Pełna integracja z programami pocztowymi MS Outlook, Outlook Express, Windows Mail oraz Windows Live Mail – antyspamowe funkcje programu dostępne są bezpośrednio z paska menu programu pocztowego.
4. Automatyczne wpisanie do białej listy wszystkich kontaktów z książki adresowej programu pocztowego.
5. Możliwość ręcznej zmiany klasyfikacji wiadomości spamu na pożądaną wiadomość i odwrotnie oraz ręcznego dodania wiadomości do białej i czarnej listy z wykorzystaniem funkcji programu zintegrowanych z programem pocztowym.
6. Możliwość definiowania swoich własnych folderów, gdzie program pocztowy będzie umieszczać spam.
7. Możliwość zdefiniowania dowolnego Tag-u dodawanego do tematu wiadomości zakwalifikowanej jako spam.
8. Program ma umożliwiać współpracę w swojej domyślnej konfiguracji z folderem „Wiadomości śmieci” obecnym w programie Microsoft Outlook.
9. Program ma umożliwiać funkcjonalność, która po zmianie klasyfikacji wiadomości typu spam na pożądaną zmieni jej właściwość jako „nieprzeczytana” oraz w momencie zaklasyfikowania wiadomości jako spam na automatyczne ustawienie jej właściwości jako „przeczytana”.
10. Program musi posiadać funkcjonalność wyłączenia modułu antyspamowego na określony czas lub do czasu ponownego uruchomienia komputera.

Zapora osobista (personal firewall)

1. Zapora osobista ma pracować jednym z 4 trybów:
   * tryb automatyczny – program blokuje cały ruch przychodzący i zezwala tylko na znane, bezpieczne połączenia wychodzące, jednocześnie umożliwia utworzenie dodatkowych reguł przez administratora
   * tryb interaktywny – program pyta się o każde nowe nawiązywane połączenie i automatycznie tworzy dla niego regułę (na stałe lub tymczasowo),
   * tryb oparty na regułach – użytkownik/administrator musi ręcznie zdefiniować reguły określające jaki ruch jest blokowany a jaki przepuszczany,
   * tryb uczenia się – umożliwia zdefiniowanie przez administratora określonego okresu czasu w którym oprogramowanie samo tworzy odpowiednie reguły zapory analizując aktywność sieciową danej stacji.
2. Program musi akceptować istniejące reguły w zaporze systemu Windows, zezwalające na ruch przychodzący
3. Możliwość tworzenia list sieci zaufanych.
4. Możliwość dezaktywacji funkcji zapory sieciowej poprzez trwałe wyłączenie
5. Możliwość określenia w regułach zapory osobistej kierunku ruchu, portu lub zakresu portów, protokołu, aplikacji i adresu komputera zdalnego.
6. Możliwość zdefiniowania wielu niezależnych zestawów reguł dla każdej sieci, w której pracuje komputer w tym minimum dla strefy zaufanej i sieci Internet.
7. Wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych*.*
8. Program musi umożliwiać ochronę przed przyłączeniem komputera do sieci botnet.
9. Wykrywanie zmian w aplikacjach korzystających z sieci i monitorowanie o tym zdarzeniu.
10. Program ma oferować pełne wsparcie zarówno dla protokołu IPv4 jak i dla standardu IPv6.
11. Możliwość tworzenia profili pracy zapory osobistej w zależności od wykrytej sieci.
12. Administrator ma możliwość sprecyzowania, który profil zapory ma zostać zaaplikowany po wykryciu danej sieci
13. Autoryzacja stref ma się odbywać min. w oparciu o: zaaplikowany profil połączenia, adres serwera DNS, sufiks domeny,adres domyślnej bramy, adres serwera WINS, adres serwera DHCP, lokalny adres IP, identyfikator SSID,szyfrowaniu sieci bezprzewodowej lub jego braku, aktywności połączenia bezprzewodowego lub jego braku, konkretny interfejs sieciowy w systemie.
14. Program musi możliwość ustalenia tymczasowej czarnej listy adresów IP, które będą blokowane podczas próby połączenia.
15. Program musi posiadać kreator, który umożliwia rozwiązać problemy z połączeniem.

Kontrola dostępu do stron internetowych

1. Aplikacja musi być wyposażona w zintegrowany moduł kontroli odwiedzanych stron internetowych.
2. Moduł kontroli dostępu do stron internetowych musi posiadać możliwość dodawania różnych użytkowników, dla których będą stosowane zdefiniowane reguły.
3. Profile mają być automatycznie aktywowane w zależności od zalogowanego użytkownika.
4. Podstawowe kategorie w jakie aplikacja musi być wyposażona to: materiały dla dorosłych, usługi biznesowe, komunikacja i sieci społecznościowe, działalność przestępcza, oświata, rozrywka, gry, zdrowie, informatyka, styl życia, aktualności, polityka, religia i prawo, wyszukiwarki, bezpieczeństwo i szkodliwe oprogramowanie, zakupy, hazard, udostępnianie plików, zainteresowania dzieci, serwery proxy, alkohol i tytoń, szukanie pracy, nieruchomości, finanse i pieniądze, niebezpieczne sporty, nierozpoznane kategorie oraz elementy niezaliczone do żadnej kategorii.
5. Moduł musi posiadać także możliwość grupowania kategorii już istniejących.
6. Aplikacja musi posiadać możliwość określenia uprawnień dla dostępu do kategorii url – zezwól, zezwól i ostrzeż, blokuj.
7. Program musi posiadać także możliwość dodania komunikatu i grafiki w przypadku zablokowania określonej w regułach witryny.

Ochrona serwera plików Windows

1. Wsparcie dla systemów: Microsoft Windows Server min 2012 R2, 2016 i nowsze
2. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
3. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.
4. Wbudowana technologia do ochrony przed rootkitami i exploitami.
5. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
6. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
7. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
8. System antywirusowy ma mieć możliwość wykorzystania wielu wątków skanowania w przypadku maszyn wieloprocesorowych.
9. Użytkownik ma mieć możliwość zmiany ilości wątków skanowania w ustawieniach systemu antywirusowego.
10. Możliwość skanowania dysków sieciowych i dysków przenośnych.
11. Skanowanie plików spakowanych i skompresowanych.
12. Program musi posiadać funkcjonalność pozwalającą na ograniczenie wielokrotnego skanowania plików w środowisku wirtualnym za pomocą mechanizmu przechowującego informacje o przeskanowanym już obiekcie i współdzieleniu tych informacji z innymi maszynami wirtualnymi.
13. Aplikacja powinna wspierać mechanizm klastrowania.
14. Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS).
15. Program powinien oferować możliwość skanowania dysków sieciowych typu NAS.
16. Aplikacja musi posiadać funkcjonalność, która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika.
17. Funkcja blokowania nośników wymiennych ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ urządzenia, numer seryjny urządzenia, dostawcę urządzenia, model i wersję modelu urządzenia.
18. Aplikacja ma umożliwiać użytkownikowi nadanie uprawnień dla podłączanych urządzeń w tym co najmniej: dostęp w trybie do odczytu, pełen dostęp, brak dostępu do podłączanego urządzenia.
19. Aplikacja ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika.
20. System antywirusowy ma automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.
21. Zainstalowanie na serwerze nowych usług serwerowych ma skutkować automatycznym dodaniem kolejnych wyłączeń w systemie ochrony.
22. Dodanie automatycznych wyłączeń nie wymaga restartu serwera.
23. Automatyczne wyłączenia mają być aktywne od momentu wykrycia usług serwerowych.
24. Administrator ma mieć możliwość wglądu w elementy dodane do wyłączeń i ich edycji.
25. W przypadku restartu serwera – usunięte z listy wyłączeń elementy mają być automatycznie uzupełnione.
26. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji systemu antywirusowego.
27. Możliwość przeniesienia zainfekowanych plików w bezpieczny obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej.
28. Wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne (heurystyka) i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji (zaawansowana heurystyka). Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej i/lub obu metod jednocześnie.
29. Możliwość automatycznego wysyłania nowych zagrożeń (wykrytych przez metody heurystyczne) do laboratoriów producenta bezpośrednio z programu (nie wymaga ingerencji użytkownika). Użytkownik musi mieć możliwość określenia rozszerzeń dla plików, które nie będą wysyłane automatycznie, oraz czy próbki zagrożeń będą wysyłane w pełni automatycznie czy też po dodatkowym potwierdzeniu przez użytkownika.
30. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.
31. W przypadku wykrycia zagrożenia, ostrzeżenie może zostać wysłane do użytkownika i/lub administratora poprzez e‑mail.
32. Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby użytkownik siedzący przy serwerze przy próbie dostępu do konfiguracji systemu antywirusowego był proszony o podanie hasła.
33. System antywirusowy ma być w pełni zgodny z technologią CISCO NAC.
34. System antywirusowy ma mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku jakiejś aktualizacji – poinformować o tym użytkownika wraz z listą niezainstalowanych aktualizacji.
35. Po instalacji systemu antywirusowego, użytkownik ma mieć możliwość przygotowania płyty CD, DVD lub pamięci USB, z której będzie w stanie uruchomić komputer w przypadku infekcji i przeskanować dysk w poszukiwaniu wirusów.
36. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma pracować w trybie graficznym.
37. System antywirusowy ma 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 procesach i połączeniach.
38. Funkcja generująca taki log ma oferować filtrowanie wyników pod kątem tego, które z nich są podejrzane dla programu i mogą stanowić dla niego zagrożenie bezpieczeństwa.
39. System antywirusowy ma oferować funkcję, która aktywnie monitoruje i skutecznie blokuje działania wszystkich plików programu, jego procesów, usług i wpisów w rejestrze przed próbą ich modyfikacji przez aplikacje trzecie.
40. Aktualizacja dostępna z Internetu, lokalnego zasobu sieciowego, nośnika CD, DVD lub napędu USB, a także przy pomocy protokołu HTTP z dowolnej stacji roboczej lub serwera (program antywirusowy z wbudowanym serwerem HTTP).
41. Obsługa pobierania aktualizacji za pośrednictwem serwera proxy.
42. Aplikacja musi wspierać skanowanie magazynu Hyper-V
43. Aplikacja musi posiadać możliwość wykluczania ze skanowania procesów
44. Możliwość utworzenia kilku zadań aktualizacji (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z własnymi ustawieniami (serwer aktualizacyjny, ustawienia sieci, autoryzacja).
45. System antywirusowy wyposażony w tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
46. Wsparcie techniczne do programu świadczone w języku polskim przezpolskiego dystrybutora autoryzowanego przez producenta programu.

Administracja zdalna

1. Serwer administracyjny musi oferować możliwość instalacji na systemach Windows Server 2012R2 i nowszych .
2. Musi istnieć możliwość pobrania ze strony producenta serwera zarządzającego w postaci gotowej maszyny wirtualnej w formacie OVA (Open Virtual Appliance).
3. Serwer administracyjny musi wspierać instalację w oparciu o co najmniej bazy danych MS SQL i MySQL.
4. Administrator musi posiadać możliwość pobrania wszystkich wymaganych elementów serwera centralnej administracji i konsoli w postaci jednego pakietu instalacyjnego lub każdego z modułów oddzielnie bezpośrednio ze strony producenta.
5. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW niezależnie od platformy sprzętowej i programowej.
6. Narzędzie musi być kompatybilne z protokołami IPv4 oraz IPv6.
7. Podczas logowania administrator musi mieć możliwość wyboru języka w jakim zostanie wyświetlony panel zarządzający co najmniej polski i angielski..
8. Komunikacja z konsolą powinna być zabezpieczona się za pośrednictwem protokołu SSL.
9. Narzędzie do administracji zdalnej musi posiadać moduł pozwalający na wykrycie niezarządzanych stacji roboczych w sieci.
10. Serwer administracyjny musi posiadać mechanizm instalacji zdalnej agenta na stacjach roboczych.
11. Instalacja serwera administracyjnego powinna oferować wybór trybu pracy serwera w sieci w przypadku rozproszonych sieci –serwer pośredniczący (proxy) lub serwer centralny.
12. Serwer proxy musi pełnić funkcję pośrednika pomiędzy lokalizacjami zdalnymi a serwerem centralnym.
13. Serwer administracyjny musi oferować możliwość instalacji modułu do zarządzania urządzeniami mobilnymi – MDM.
14. Serwer administracyjny musi oferować możliwość instalacji serwera http proxy pozwalającego na pobieranie aktualizacji baz sygnatur oraz pakietów instalacyjnych na stacjach roboczych bez dostępu do Internetu.
15. Komunikacja pomiędzy poszczególnymi modułami serwera musi być zabezpieczona za pomocą certyfikatów.
16. Serwer administracyjny musi oferować możliwość utworzenia własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy.
17. Centralna konfiguracja i zarządzanie ochroną antywirusową, antyspyware’ową, zaporą osobistą i kontrolą dostępu do stron internetowych zainstalowanymi na stacjach roboczych w sieci.
18. Zarządzanie oprogramowaniem zabezpieczającym na stacjach roboczych musi odbywać się za pośrednictwem dedykowanego agenta.
19. Agent musi posiadać możliwość pobrania listy zainstalowanego oprogramowania firm trzecich na stacji roboczej z możliwością jego odinstalowania.
20. Serwer administracyjny musi oferować możliwość wymuszenia połączenia agenta do serwera administracyjnego z pominięciem domyślnego czasu oczekiwania na połączenie.
21. Instalacja klienta na urządzeniach mobilnych musi być dostępna za pośrednictwem portalu WWW udostępnionego przez moduł MDM z poziomu urządzenia użytkownika.
22. W przypadku braku zainstalowanego klienta na urządzeniu mobilnym musi istnieć możliwość jego pobrania ze sklepu Google Play.
23. Administrator musi posiadać możliwość utworzenia listy zautoryzowanych urządzeń mobilnych, które mogą zostać podłączone do serwera centralnej administracji.
24. Serwer administracyjny musi oferować możliwość zablokowania, odblokowania, wyczyszczenia zawartości, zlokalizowania oraz uruchomienia syreny na zarządzanym urządzaniu mobilnym. Funkcjonalność musi wykorzystywać połączenie internetowe, nie komunikację za pośrednictwem wiadomości SMS.
25. Administrator musi posiadać możliwość utworzenia dodatkowych użytkowników/administratorów Serwer centralnego zarządzania do zarządzania stacjami roboczymi.
26. Serwer administracyjny musi oferować możliwość utworzenia zestawów uprawnień dotyczących zarządzania poszczególnymi grupami komputerów, politykami, instalacją agenta, raportowania, zarządzania licencjami, zadaniami, itp.
27. Administrator musi posiadać wymuszenia dwufazowej autoryzacji podczas logowania do konsoli zarządzającej
28. Dwu fazowa autoryzacja musi się odbywać za pomocą wiadomości SMS lub haseł jednorazowych generowanych na urządzeniu mobilnym za pomocą dedykowanej aplikacji.
29. Administrator musi posiadać możliwość nadania dwóch typów uprawnień do każdej z funkcji przypisanej w zestawie uprawnień: tylko do odczytu, odczyt/zapis.
30. Administrator musi posiadać możliwość przypisania kilku zestawów uprawnień do jednego użytkownika.
31. Serwer administracyjny musi posiadać możliwość konfiguracji czasu bezczynności po jakim użytkownik zostanie automatycznie wylogowany.
32. Agent musi posiadać mechanizm pozwalający na zapis zadania w swojej pamięci wewnętrznej w celu ich późniejszego wykonania bez względu na stan połączenia z serwerem centralnej administracji.
33. Instalacja zdalna programu zabezpieczającego za pośrednictwem agenta musi odbywać się z repozytorium producenta lub z pakietu dostępnego w Internecie lub zasobie lokalnym.
34. Serwer administracyjny musi oferować możliwość deinstalacji programu zabezpieczającego firm trzecich lub jego niepełnej instalacji podczas instalacji nowego pakietu.
35. Serwer administracyjny musi oferować możliwość wysłania komunikatu lub polecenia na stacje kliencką.
36. Serwer administracyjny musi oferować możliwość utworzenia grup statycznych i dynamicznych komputerów.
37. Grupy dynamiczne tworzone na podstawie szablonu określającego warunki jakie musi spełnić klient aby zostać umieszczony w danej grupie. Przykładowe warunki: Adresy sieciowe IP, Aktywne zagrożenia, Stan funkcjonowania/ochrony, Wersja systemu operacyjnego, itp.
38. Serwer administracyjny musi oferować możliwość przypisania polityki dla pojedynczego klienta lub dla grupy komputerów. Serwer administracyjny musi oferować możliwość przypisania kilku polityk z innymi priorytetami dla jednego klienta.
39. Edytor konfiguracji polityki musi być identyczny jak edytor konfiguracji ustawień zaawansowanych w programie zabezpieczającym na stacji roboczej.
40. Serwer administracyjny musi oferować możliwość nadania priorytetu „Wymuś” dla konkretnej opcji w konfiguracji klienta. Opcja ta nie będzie mogła być zmieniona na stacji klienckiej bez względu na zabezpieczenie całej konfiguracji hasłem lub w przypadku jego braku.
41. Serwer administracyjny musi oferować możliwość utworzenia raportów zawierających dane zebrane przez agenta ze stacji roboczej i serwer centralnego zarządzania.
42. Serwer administracyjny musi oferować możliwość wyboru formy przedstawienia danych w raporcie w postaci tabeli, wykresu lub obu elementów jednocześnie.
43. Serwer administracyjny musi oferować możliwość wygenerowania raportu na żądanie, zgodnie z harmonogramem lub umieszczenie raportu na Panelu kontrolnym dostępnym z poziomu interfejsu konsoli WWW.
44. Raport generowany okresowo może zostać wysłany za pośrednictwem wiadomości email lub zapisany do pliku w formacie PDF, CSV lub PS.
45. Serwer administracyjny musi oferować możliwość maksymalizacji wybranego elementu monitorującego.
46. Raport na panelu kontrolnym musi być w pełni interaktywny pozwalając przejść do zarządzania stacją/stacjami, której raport dotyczy.
47. Administrator musi posiadać możliwość wysłania powiadomienia za pośrednictwem wiadomości email lub komunikatu SNMP.
48. Serwer administracyjny musi oferować możliwość konfiguracji własnej treści komunikatu w powiadomieniu.
49. Serwer administracyjny musi oferować możliwość podłączenia serwera administracji zdalnej do portalu zarządzania licencjami dostępnego na serwerze producenta.
50. Serwer administracyjny musi oferować możliwość dodania licencji do serwera zarządzania na podstawie klucza licencyjnego lub pliku offline licencji.
51. Serwer administracyjny musi posiadać możliwość dodania dowolnej ilości licencji obejmujących różne produkty.
52. Serwer administracyjny musi być wyposażona w machizm autodopasowania kolumn w zależności od rozdzielczości urządzenia na jakim jest wyświetlana.
53. Serwer administracji musi umożliwić granulację uprawnień dla Administratorów w taki sposób, aby każdemu z nich możliwe było przyznanie oddzielnych uprawnień do poszczególnych grup komputerów, polityk lub zadań.

EndpointDetection and Response

Serwer

1. Serwer administracyjny musi posiadać możliwość instalacji na systemach Windows Server 2012 i nowszych.
2. Serwer administracyjny musi wspierać instalację z użyciem nowego lub istniejącego serwera bazy danych MS SQL i MySQL.
3. System musi współpracować z serwerem administracyjnym produktu antywirusowego, tego samego producenta.
4. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW.
5. Serwer administracyjny musi posiadać możliwość konfiguracji zadania cyklicznego czyszczenia bazy danych.
6. Serwer administracyjny musi posiadać możliwość wysyłania zdarzeń do konsoli administracyjnej tego samego producenta.
7. Interfejs musi być zabezpieczony za pośrednictwem protokołu SSL.
8. Serwer administracyjny musi posiadać możliwość wprowadzania wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa.
9. Wykluczenia muszą dotyczyć procesu lub procesu „rodzica”.
10. Utworzenie wykluczenia musi automatycznie rozwiązywać alarmy, które pasują do utworzonego wykluczenia.
11. Kryteria wykluczeń muszą być konfigurowane w oparciu o przynajmniej: nazwę procesu, ścieżkę procesu, wiersz polecenia, wydawcę, typ podpisu, SHA-1, nazwę komputera, grupę, użytkownika.
12. Serwer musi posiadać ponad 800 wbudowanych reguł, po których wystąpieniu, nastąpi wyzwolenie alarmu bezpieczeństwa. Administrator musi też posiadać możliwość utworzenia własnych reguł i edycji reguł dodanych przez producenta.
13. Serwer administracyjny musi posiadać możliwość uruchomienia reguł w oparciu o dane historyczne.
14. Serwer administracyjny musi oferować możliwość blokowania plików po sumach kontrolnych. W ramach blokady musi istnieć możliwość dodania komentarza oraz konfiguracji wykonywanej czynności, po wykryciu wprowadzonej sumy kontrolnej.
15. Serwer musi posiadać możliwość ustawiania priorytetu zdarzeń z użyciem 4-stopniowej skali.
16. Administrator musi posiadać możliwość weryfikacji uruchomionych plików wykonywalnych na stacji roboczej z możliwością podglądu szczegółów wybranego procesu przynajmniej o: SHA-1, typ podpisu, wydawcę, opis pliku, wersję pliku, nazwę firmy, nazwę produktu, wersję produktu, oryginalną nazwę pliku, rozmiar pliku oraz reputację i popularność pliku.
17. Administrator, w ramach plików wykonywalnych oraz plików DLL, musi posiadać możliwość ich oznaczenia jako bezpieczne, pobrania do analizy oraz ich zablokowania.
18. Administrator musi posiadać możliwość weryfikacji uruchomionych skryptów na stacjach roboczych, wraz z informacją dotyczącą parametrów uruchomienia. Administrator musi posiadać możliwość oznaczenia skryptu jako bezpieczny lub niebezpieczny.
19. W ramach przeglądania wykonanego skryptu, administrator musi posiadać możliwość szczegółowego podglądu wykonanych przez skrypt czynności w formie tekstowej.
20. W ramach przeglądania wykonanego skryptu lub pliku exe, administrator musi posiadać możliwość weryfikacji powiązanych zdarzeń dotyczących przynajmniej: modyfikacji plików i rejestru, zestawionych połączeń sieciowych i utworzonych plików wykonywalnych.
21. Serwer administracyjny musi posiadać funkcję wyszukiwarki, w której administrator jest w stanie wyszukać dowolny element lub zdarzenie na podstawie wprowadzonej nazwy.
22. Serwer administracyjny musi oferować możliwość przekierowania do konsoli zarządzającej produktu antywirusowego tego samego producenta, w celu weryfikacji szczegółów wybranej stacji roboczej. W konsoli zarządzającej produktu antywirusowego, administrator musi mieć możliwość podglądu informacji dotyczących przynajmniej: podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe) oraz wylistowanie zainstalowanego oprogramowania firm trzecich.
23. Serwer administracyjny musi oferować możliwość bezpośredniego sprawdzenia SHA-1 pliku, na portalach służących do weryfikacji bezpieczeństwa (np. VirusTotal).
24. Administrator musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.
25. Konsola administracyjna musi mieć możliwość tagowania obiektów.
26. Konsola administracyjna musi umożliwiać audytowanie innych administratorów konsoli.
27. Konsola administracyjna musi pozwalać na włączenie izolacji komputera od sieci.
28. Konsola administracyjna musi umożliwiać połączenie się do stacji roboczej z możliwością wykonywania poleceń powershell.
29. Konsola administracyjna musi umożliwiać dodawanie emotikon do co najmniej komentarzy, tagów, nazw reguł.

Agent

1. Pełne wsparcie dla systemu Windows 7/Windows 8/Windows 8.1/Windows 10 oraz Windows Server 2008/2012/2016/2019.
2. Pełne wsparcie dla systemów macOS 10.12 i nowszych.
3. Wsparcie dla 32 i 64-bitowej wersji systemu Windows.
4. Agent musi współpracować z produktem antywirusowym tego samego producenta.
5. Agent nie może działać bez produktu antywirusowego tego samego producenta.
6. W ramach wprowadzonych reguł administracyjnych dotyczących blokowania/usuwania plików, użytkownik musi otrzymać stosowne powiadomienie, dotyczące czynności wykonanej przez agenta.
7. Połączenie agenta do serwera zarządzającego musi być szyfrowane.
8. Administrator musi posiadać możliwość utworzenia polityki z konsoli administracyjnej zawierającej wykluczenia dla procesów, które nie będą analizowane.
9. System EDR musi zapewniać dostępność do nowych definicji wykryć.
10. Zamawiający wymaga, aby Wykonawca realizując opisane usługi uwzględniał uwarunkowania środowiska aktualnie pracującego u Zamawiającego.

Przeprowadzenie szkoleń (stacjonarnych lub online) w zakresie cyberbezpieczeństwa zgodnie wymaganiami określonymi dla konkursu D1.1.2 w ramach Krajowego Planu Odbudowy – tryb naboru: konkurencyjny.

1. Szkolenia kadry kierowniczej (8 osób), co najmniej z:

* Podstaw prawnych w obszarze cyberbezpieczeństwa.
* Typów ataków wraz z przykładami
* Reagowania na incydenty.
* Wykonywania testów bezpieczeństwa.
* Roli kadry zarządzającej w procesach bezpieczeństwa

1. Szkolenia pracowników administracji i pracowników medycznych (260 osób), co najmniej z:

* Podstawowych zasad cyberhigieny.
* Typów ataków wraz z przykładami
* Reagowania na incydenty
* Odpowiedzialności prawnej

3.7. Aktualizacja dokumentacji SZBI

Aktualizacja dokumentacji systemu zarządzania bezpieczeństwem informacji zgodnie z wymaganiami określonymi dla konkursu D1.1.2 w ramach Krajowego Planu Odbudowy – tryb naboru: konkurencyjny

3.8. Zakres przedmiotowy Etapu II –Usługa Security Operations Center – 36 miesięcy

3.8.1. Security Operations Center

System monitoringu infrastruktury IT i usługa SOC

1. MINIMALNE WYMAGANIA TECHNICZNE
2. Tworzenia wielu użytkowników systemu monitorowania IT bez dodatkowych opłat.
3. Zapewnienia równoległego dostępu do systemu dla wielu użytkowników.
4. Ograniczania użytkownikom dostępu do wybranych grup hostów.
5. Monitorowanie
6. Monitorowania serwerów fizycznych.
7. Monitorowania urządzeń sieciowych.
8. Monitorowania stanu połączeń.
9. Monitorowanie interfejsów sieciowych przełączników, routerów, serwerów
10. Monitorowanie maszyn wirtualnych pracujących pod kontrolą systemów operacyjnych Windows i Linux.
11. Dostęp do systemu monitorowania przez panel dla urządzeń mobilnych.
12. Możliwość rozbudowy systemu o monitorowanie kolejnych urządzeń.
13. Automatyczne wykrywanie usług na urządzeniach, powiadamianie o wykryciu nowych usług na urządzeniu.
14. Grupowanie hostów.
15. Definiowanie planowanych przerw serwisowych dla hostów i usług.
16. Możliwość zaznaczenia reakcji na awarię - odpowiadanie na alerty (ACK).
17. Wykonywanie operacji na grupach hostów (włączenie/wyłączenie monitorowania, powiadomień; konfiguracje przerw serwisowych).
18. Generowanie raportów dostępności monitorowanych urządzeń, usług i procesów biznesowych (raporty wyświetlane na stronie www).
19. Monitorowanie serwerów za pomocą agentów
20. Monitorowanieserwerówaplikacji: Tomcat, Oracle WebLogic Server, Oracle Application Server.
21. Monitorowanie Active Directory.
22. Monitorowanie serwerów plików, udziałów sieciowych.
23. Monitorowanie statusu serwerów Apache.
24. Monitorowanie baz danych:

* ORACLE,
* MySQL,
* Postgress.
* MSSQL Server
* DB2

1. Monitorowanie urządzeń przez następujące protokoły:

* SNMP,
* WMI,
* IPMI.

1. Konfigurację oprogramowania systemu monitorowania poprzez interfejs WWW.
2. Monitorowanie poprawności działania DNS.
3. Monitorowanie środowiska VMware.
4. Monitorowanie środowiska Hyper-V.
5. Monitorowanie działania serwera czasu NTP.
6. Monitorowanie offsetu czasu na serwerach.
7. Monitorowanie ping - czasy odpowiedzi, straty pakietów.
8. Monitorowanie zajętości miejsca na poszczególnych partycjach.
9. Monitorowanie obciążenia dysków.
10. Monitorowanie wykorzystania pamięci RAM.
11. Monitorowanie obciążenia CPU.
12. Monitorowanie logów systemowych Windows.
13. Monitorowanie macierzy dyskowych, status urządzenia statusów dysków urządzenia.
14. Dodawanie własnych wtyczek / agentów dla urządzeń i usług, które standardowo nie są obsługiwane.
15. Zgodność z wtyczkami programu Nagios służącego do monitorowania sieci, urządzeń sieciowych, aplikacji oraz serwerów działający w systemach Linux i Unix.
16. Agregację usług niskiego poziomu do procesów biznesowych (tzw. Business Intelligence)
17. Symulację awarii elementów infrastruktury i badanie jej wpływu na procesy biznesowe
18. Monitorowanie rozproszone (podgląd w pojedynczym panelu stanu wielu instancji monitorujących, np. z kilku lokalizacji/oddziałów).
19. Wykrywanie niestabilnie działających usług.
20. Monitorowanie dostępności stron internetowych.
21. Konfigurację hierarchiczną (dziedziczenie konfiguracji dla grup urządzeń).
22. Prezentacja
23. Prezentację stanu urządzeń na mapie.
24. Prezentację danych na dashboardach.
25. Elastyczną konfigurację dashboardów, wybór elementów.
26. Wizualizację stanu działania całej infrastruktury na jednym dashboardzie.
27. Tworzenie indywidualnych dashboardów przez użytkowników
28. Powiadomienia
29. Globalne wyłączanie powiadomień.
30. Powiadamianie użytkownika o problemach przez e-mail.
31. Eskalację powiadomień do kolejnych użytkowników w przypadku braku reakcji na powiadomienie.
32. Definiowanie przedziałów czasowych w których wysyłane są powiadomienia do poszczególnych użytkowników.
33. Definiowanie różnych wartości progowych alertów na poziomie globalnym, grupy urządzeń, pojedynczych urządzeń, pojedynczych usług
34. Konfiguracja
35. Konfigurację oprogramowania systemu monitorowania poprzez interfejs WWW
36. Automatyczna konfiguracja i działanie z REST-API
37. Centralne zarządzanie agentami
38. Integracja danych z różnych źródeł danych (JSON, XML, SNMP)
39. Monitoring bazy danych systemu HIS
40. Możliwość monitorowania bazy danych systemu HIS w zakresie co najmniej:

* Instancestate
* Version
* Jobs
* Locks
* Processes
* Number of activesessions
* Recoveryarea
* Log switchactivity
* General tablespaceinformation
* Tablespaces performance
* Longactivesessions
* Undoretention
* Checkpoint and online backup state
* CustomSQLs
* RMAN backup status
* RMAN backups
* ASM diskgroups
* Apply and transport lag of Oracle Data-Guard

1. Możliwość dodania własnych zapytań SQL i monitorowanie zwracanych wartości
2. Kolektor logów
3. System posiada własny kolektor logów syslog
4. Może odbierać wiadomości bezpośrednio z syslog lub SNMP traps
5. Za pomocą agentów potrafi oceniać logi tekstowe oraz logi Windows Event
6. Klasyfikuje wiadomości bazując na zdefiniowanych przez użytkownika regułach, potrafi korelować, podsumowywać, liczyć, opisywać i przepisywać wiadomości, a także uwzględniać ich relacje czasowe.
7. Cyberbezpieczeństwo
8. System monitoruje urządzenia klasy UTM minimum w zakresie:

* wykrywanie włamań i szybkość blokowania WARN lub CRIT, jeśli wskaźnik wykrywania przekracza poziomy konfigurowane przez użytkownika
* monitoruje stan synchronizacji klastra High-Availability. Status „zsynchronizowany” ustawienie stanu na OK, a status „niezsynchronizowany” na CRIT.
* monitoruje ogólny stan alarmów czujników urządzenia Firewall. Status kontroli jest OK, jeśli wszystkie czujniki mają status alarmu „fałsz” (0) i CRIT, jeśli co najmniej jeden czujnik ma stan alarmu „prawda” (1).
* monitoruje aktualną liczbę sesji na urządzeniu
* monitoruje liczbę dostępnych tuneli IPSec VPN
* monitoruje wykrywanie wirusów i szybkość blokowania systemów FortiGate AntiVirus. Przechodzi WARN lub CRIT, jeśli wskaźnik wykrywania przekracza poziomy konfigurowane przez użytkownika.
* monitoruje poziom wykorzystania procesora
* Górne domyślne poziomy to 80,0, 90,0 procent. Poziomy są konfigurowalne.

1. System ma możliwość odbierania i prezentacji danych z UTM z wykorzystaniem kolektora logów syslog
2. System ma możliwość odbierania danych z systemu EDR z wykorzystaniem kolektora logów syslog.
3. Zakres monitorowanych zdarzeń powinien uwzględniać minimum:

* Powiadomienia o zagrożeniach ze stacji roboczych oraz serwerów, w szczególności generowane z narzędzi ochrony,
* Powiadomienia o dezaktywacji narzędzi bezpieczeństwa na danym hoście,
* Powiadomienia z modułów ochrony / bezpieczeństwa urządzeń brzegowych oraz wewnętrznych urządzeń sieciowych,
* Zdarzenia dotyczące nieudanych, wielokrotnych prób logowania dla wszystkich monitorowanych aktywów,
* Kluczowe zdarzenia (np. utworzenie konta, zmiana hasła, usunięcie konta, zmiana grupy) związane z kontami uprzywilejowanymi dla wszystkich monitorowanych aktywów,
* Zdarzenia sieciowe oraz systemowe (np. enumeracja, skanowanie portów i adresacji) mogące świadczyć o rekonesansie infrastruktury,
* Zdarzenia związane z modyfikacją mechanizmów harmonogramu w systemach operacyjnych,
* Zdarzenia związane z modyfikacją audytu zdarzeń / dzienników systemowych,
* Zdarzenia dotyczące integralności plików, w szczególności zasobów sieciowych mogące świadczyć o zainfekowaniu oprogramowaniem złośliwym
* Zdarzenia związane z logowaniem zdalnym.

1. Warunki świadczenia usługi
2. Operacyjne Centrum Bezpieczeństwa; centrum kompetencyjne, które zajmować się będzie monitorowaniem infrastruktury teleinformatycznej, analizą zdarzeń, detekcją zagrożeń bezpieczeństwa i reagowaniem na wykryte incydenty naruszające bezpieczeństwo teleinformatyczne chronionych organizacji za pomocą analizy zbieranych logów z urządzeń, systemów IT oraz aplikacji, korelacją zdarzeń i detekcją zagrożeń oraz odpowiednią reakcję na pojawiające się incydenty
3. W ramach realizacji zamówienia, Wykonawca będzie świadczył usługę monitorowania i analizy danych prezentowanych w Systemie monitorowania zgodnie z opisanymi poniżej wymaganiami.
4. Aktualizacje dostarczonego Systemu SIEM do nowych wersji oprogramowania przez okres 36 miesięcy.
5. Szkolenia administratorów on-line z nowych funkcjonalności,
6. Usługi konsultacyjne w zakresie funkcjonalności, eksploatacji i administrowania Systemem, bieżące aktualizacje dokumentacji technicznej dla Systemu,
7. Przyjmowania zgłoszeń serwisowych przez dedykowany serwisowy moduł internetowy oraz mail 24/7
8. Monitorowanie zdarzeń naruszenia cyberbezpieczeństwa oraz ciągłości pracy infrastruktury w trybie 24/7/365, zgodnie z określonymi poniżej warunkami SLA
9. Dokumentowanie wykonanych czynności zgodnie z przygotowanymi i zaakceptowanymi Scenariuszami Reakcji.
10. Eskalowanie zdarzenia w ramach ustalonego Scenariusza Reakcji.
11. Zamykanie zdarzeń błędnie rozpoznanych przez system bezpieczeństwa jako zagrożenie (tzw. False-Positive
12. Przygotowywanie dziennych raportów wykrytych zdarzeń bezpieczeństwa
13. Modyfikacja polityk bezpieczeństwa systemów, aplikacji, rozwiązań podmiotu celem dostosowania ich do skuteczniejszego wykrywania zagrożeń (tuning systemów bezpieczeństwa).

Usługa Drugiej Linia Wsparcia minimum w zakresie:

1. Analiza zgłoszonych przez Pierwszą Linię Wsparcia Incydentów cyberbezpieczeństwa oraz przygotowanie raportów i zaleceń poincydentalnych
2. Realizacja Scenariuszy Reakcji zgodnie z wymaganiami.
3. Przygotowanie miesięcznych raportów z realizacji prac.
4. Oczekiwana dostępność usługi Drugiej Linii Wsparcia - 8 godzin dziennie, 5 dni w tygodniu

Usługa przygotowania i wdrożenia Scenariuszy Reakcji dla zidentyfikowanych zagrożeń (playbooki).

Usługa udostępnienia, administrowania i utrzymania systemu Security Incident and Event Management oraz integracja ze źródłami logów podmiotu, takimi jak Active Directory, Serwery Windows i Linux, DNS, system antywirusowy, WAF, Firewall, IPS / IDS, VPN, Routery i przełączniki.

1. Zgłoszenia i Incydenty są klasyfikowane na podstawie potencjalnego wpływu na Klienta. Wykorzystywane są 4 poziomy klasyfikacji, jak przedstawiono w poniższej tabeli:

|  |  |  |  |
| --- | --- | --- | --- |
| **Poziom** | **Opis** | **Zagrożenie** | **Przykład** |
| Krytyczny | Niezbędne natychmiastowe działanie | - Przerwa w działaniu serwera/systemu | Wyciek danych |
|  | złagodzić obecne złośliwe oprogramowanie | - Brak odbioru danych z |  |
|  | Działalność | lokalizacja klienta |  |
| 3 | Wysokie prawdopodobieństwo incydentu, jeśli | - Znaczące zmiany w SIEM | Brak potwierdzenia |
|  | nie podejmuje się działań zapobiegawczych | - wskazanie natężenia ruchu danych obniżona wydajność potencjał |  |
| 2 | Niski potencjalny incydent | - Użytkownik nie zaktualizował hasła w wymaganym odstępie czasu | Znaleziony wirus na stacji roboczej |
| 1 | Aktywności utrzymaniowe lub informacyjne | - | Raport |

1. W oparciu o klasyfikację i rodzaj zdarzenia/zgłoszenia wsparcie reaguje zgodnie z poniższymi interwałami.

|  |  |  |  |
| --- | --- | --- | --- |
| **Poziom** | **Opis** | **Zagrożenie** | **SLA** |
| Critical | 1 godzina | 1 godzina | 96% |
| 3 | 24 godziny | 2 godziny | 96% |
| 2 | 72 godziny | 8 godzin | 96% |
| 1 | 5 dni | 24 godzin | 96% |

1. W ramach usługi Wykonawca monitoruje krytyczne elementy infrastruktury IT:

* Serwery 5 sztuk
* Macierze 2 sztuki
* Przełączniki FC 2 sztuki
* Przełączniki LAN 10 sztuk
* Serwer Backupu 1 sztuka
* Biblioteka taśmowa LTO 1 sztuka
* NAS 1 sztuki
* UPS 3 sztuki
* Serwer aplikacji
* Serwer usług
* IIS 2. sztuki
* Serwer wirtualizacji 3 sztuki
* Serwer AD 2 sztuki
* Serwer Bazy Danych Oracle 1 sztuka

W przypadku instalacji przez Zamawiającego nowego rozwiązania będącego jednym z powyższych elementów musi ono zostać objęte systemem monitorowania w ramach usługi SOC.

1. W ramach usługi wykonawca monitoruje krytyczne elementy systemu HIS:

* Monitorowanie komunikacji z platformą P1
* Monitorowanie komunikacji bramek HL7
* Monitorowanie komunikacji EWUŚ
* Monitorowanie KOWAL
* Monitorowanie komunikacji AP-KOLCE
* Monitorowanie RZM
* Monitorowanie bazy danych systemu HIS

3.9. Zakres przedmiotowy Etapu III - świadczenia przez Wykonawcę na rzecz Zamawiającego Usług Gwarancji w zakresie dostarczanej Infrastruktury IT– 36 miesięcy

Dostarczone środowisko i usługi objęte są wsparciem i gwarancją przez okres 36 miesięcy od daty podpisania Protokołu Odbioru Końcowego.

1. WDROŻENIE ROZWIĄZAŃ AI I PODŁĄCZENIE DO CENTRALNEGO REPOZYTORIUM DANYCH MEDYCZNYCH
2. Termin realizacji zadania

Wykonawca zobowiązuje się wykonać przedmiot Umowy od dnia podpisania umowy w terminach poszczególnych Etapów, które wynoszą:

Etap I – Dostawa licencji Modułu: Integracja RIS/PACS z Platformą Usług Inteligentnych (PUI) - do 30 dni kalendarzowych od daty podpisania Umowy

Etap II - Wdrożenie Modułu: Integracja RIS/PACS z Platformą Usług Inteligentnych (PUI) – do 29.05.2026r

Etap III – świadczenie przez Wykonawcę na rzecz Zamawiającego Usług Gwarancji i Opieki Serwisowej w zakresie Modułu: Integracja RIS/PACS z Platformą Usług Inteligentnych (PUI) – 36 miesięcy od daty podpisania Protokołu Odbioru Końcowego.

UWAGA: Całość zadania musi zostać zrealizowana nie później niż do 29.05.2026r

1. Zakres przedmiotowy Etapu I - Dostawa licencji
2. Wykaz Licencji objętych przedmiotem Umowy:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Lp. | Nazwa modułu | Ilość | Rodzaj licencji | Okres |
|  | Integracja PUI | 1 | SRW | bezterminowa |

1. Warunki licencji:
2. Zamawiający oczekuje udzielenia licencji Serwerowej (SRW) dla Modułu tz. Zamawiający jest uprawniony do korzystania z danego Modułu na maksymalnie takiej liczbie serwerów, na jaką została udzielona przez nieograniczoną liczbę użytkowników na nieograniczonej liczbie komputerów lub terminali. Licencja reglamentuje także systemy operacyjne serwera do liczby tożsamej z ilością serwerów, na które została udzielona,
3. Licencja nie może wprowadzać ograniczenia na tzw. „nazwanych użytkowników”
4. Licencją objęte zostaną również wszelkie poprawki i aktualizacje Modułu pojawiające się w trakcie obowiązywania przedmiotowej Umowy a także w trakcie następnych umów serwisowych.
5. Wykonawca zobowiązany jest udzielić licencji na Moduł, jego rozwinięcia i uaktualnienia oraz towarzyszącą dokumentację na czas nieoznaczony.
6. Zakres przedmiotowy Etapu II - Wdrożenie Modułu
7. Usługi Wdrożeniowe
8. Wdrożenie należy rozumieć jako szereg uporządkowanych i zorganizowanych działań mających na celu wykonanie Przedmiotu Zamówienia.
9. Wykonawca umożliwi Zamawiającemu udział we wszystkich pracach realizowanych przez Wykonawcę w ramach realizacji Przedmiotu Zamówienia (m.in. w czasie dostaw, instalacji, konfiguracji i pozostałych elementach wdrożenia).
10. Wykonawca zobowiązany jest przeprowadzić dostawy Przedmiotu Zamówienia w dokładnych terminach i godzinach uzgodnionych z Zamawiającym.
11. Wdrożenie będą realizowane w ramach powołanych do tego celu struktur organizacyjnych po stronie Wykonawcy i Zamawiającego.
12. Wykonawca zorganizuje prace tak, aby w maksymalnym stopniu nie zakłócać ciągłości funkcjonowania prac u Zamawiającego. 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.
13. Wykonawca musi uwzględnić, że wszystkie prace wykonywane będą w użytkowanych obiektach przy dużym ruchu pracowników i chorych, tzn. organizacja prac powinna przede wszystkim zapewniać bezpieczeństwo przebywających w oddziałach pracowników i chorych oraz zachowanie ciszy nocnej w godzinach właściwych dla Zamawiającego.
14. Po zakończeniu prac instalacyjnych Moduł musi zostać skonfigurowany i wdrożony w sposób kompleksowy tak, aby oferował wszystkie funkcjonalności w zakresie opisanych w OPZ wymagań funkcjonalnych.
15. Moduł musi zostać zainstalowany przez Wykonawcę w środowiskach informatycznych Zamawiającego. Moduł musi zostać zainstalowany i skonfigurowany w sposób kompleksowy.
16. Wymagania funkcjonalne Modułu: Integracja RIS/PACS z Platformą Usług Inteligentnych (PUI)

|  |  |
| --- | --- |
| Lp. | PUI - WYMAGANIA MINIMALNE |
| 1. | Integracja RIS/PACS z Platformą Usług Integralnych (PUI). |
| 2. | Wykorzystanie interfejsu REST API do komunikacji z serwerem autoryzacyjnym. |
| 3. | Komunikacja powinna być zabezpieczona protokołem TLS. |
| 4. | Uwierzytelnienie i autoryzacja powinno odbywać się zgodnie ze standardem OAuth 2.0. |
| 5. | Możliwość wysłania badań diagnostycznych do Platformy Usług Inteligentnych (PUI). |
| 6. | Możliwość odebrania wyników analizy SI z Platformy Usług Inteligentnych (PUI). |

1. Zakres przedmiotowy Etap III- świadczenie przez Wykonawcę na rzecz Zamawiającego Usług Gwarancji i Opieki Serwisowej w zakresie Modułu: Integracja RIS/PACS z Platformą Usług Inteligentnych (PUI) – 36 miesięcy od daty wykonania przedmiotu zamówienia tj. podpisania Protokołu Odbioru Końcowego
2. Wykonawca w ramach realizacji Przedmiotu Zamówienia przez 36 miesiące od wykonania przedmiotu zamówienia tj. podpisania Protokołu Odbioru Końcowego będzie świadczył na rzecz Zamawiającego Usługi Opieki serwisowej i aktualizacji w zakresie eksploatacji dostarczanego w ramach realizacji zadania Modułu.
3. ZASADY ŚWIADCZENIA USŁUG DOSTĘPU DO NOWYCH WERSJI ORAZ USŁUG SERWISOWYCH DLA MODUŁU.

[ZASADY OGÓLNE]

1. Usługi Serwisowe są świadczone w odniesieniu do dostarczanego w ramach realizacji zadania Modułu: Integracja RIS/PACS z Platformą Usług Inteligentnych zgodnie z postanowieniami rozdziału: Warunki brzegowe realizacji usług.

[UŻYTKOWNICY]

1. Wraz z podpisaniem Umowy ZAMAWIAJĄCY otrzymuje dane identyfikacyjne (login, hasło) umożliwiające Użytkownikom ZAMAWIAJĄCEGO uwierzytelnienie w systemie „Help Desk” zwanym dalej „HD” udostępnionym przez WYKONAWCĘ.
2. W zależności od woli ZAMAWIAJĄCEGO poszczególnym Użytkownikom zostaną przyznane prawa do ewidencji lub/i edycji Zgłoszeń Serwisowych.
3. Użytkownicy są zobligowani do ochrony danych identyfikacyjnych przed dostępem osób trzecich. Użytkownicy przyjmują także do wiadomości, że wszystkie operacje wykonywane w serwisie HD są rejestrowane.
4. Użytkownicy systemu HD posiadają możliwość dokonywania zmian swoich danych kontaktowych oraz podstawowych danych podmiotowych ZAMAWIAJĄCEGO. System HD będzie komunikował się z Użytkownikami wyłącznie w oparciu o informacje zamieszczone w HD.

Powinnością Użytkowników jest bieżące śledzenie informacji pojawiających się w systemie HD.

1. Powinnością Administratora jest zapoznanie się z postanowieniami Umowy, jak również przeszkolenie w zakresie jej zakresu oraz treści pozostałych Użytkowników.
2. Użytkownicy dołożą wszelkich starań, żeby dane osobowe nie były zamieszczane w Zgłoszeniach Serwisowych. Jeżeli jest to niezbędne do obsłużenia Zgłoszenia Serwisowego Użytkownicy zamieszczą informacje oraz dane wyłącznie w postaci zanonimizowanej lub zaszyfrowanej, jak również oznaczą Zgłoszenia Serwisowego zawierające takie dane w sposób określony w HD.

[EWIDENCJA I OBSŁUGA ZGŁOSZEŃ]

1. Ewidencja i uzupełnianie Zgłoszenia Serwisowego przez ZAMAWIAJĄCEGO jest realizowane wyłącznie w systemie HD. Obsługa przez Serwis Zgłoszenia Serwisowego w zależności od usługi jest realizowana w systemie HD lub z wykorzystaniem innych mediów bądź wizyt osobistych, przy czym każdorazowo w HD ewidencjonowany jest status zgłoszenia.
2. Użytkownik może zaewidencjonować w systemie HD następujące typy Zgłoszeń Serwisowych:
   * Błąd Aplikacji
   * Awaria
   * Usterka programistyczna
   * Konsultacja
   * Zamówienie indywidualne: Nowa funkcjonalność/Usługa odpłatna
   * Zapytanie handlowe
3. Zamawiający dopuszcza, by w systemie HD zgłoszenia uzyskiwały inne typy niż ww. odpowiadające rodzajowo powyższym Zgłoszeniom serwisowym.
4. Ewidencja Zgłoszenia Serwisowego odbywa się poprzez wprowadzenie przez Użytkownika do systemu HD wszystkich niezbędnych dla danego Zgłoszenia Serwisowego informacji.

Po zaewidencjonowaniu przez Użytkownika Zgłoszenia Serwisowego system HD nadaje mu status „oczekujące” oraz unikalny numer.

1. Każde Zgłoszenie Serwisowe obejmować może wyłącznie jedno zagadnienie. W przypadku, gdy Zgłoszenie Serwisowe obejmuje kilka zagadnień WYKONAWCA może takie Zgłoszenie Serwisowe odrzucić lub wydzielić zagadnienia do odrębnych Zgłoszeń Serwisowych.
2. Jeżeli do Zgłoszenia Serwisowego pozostającego w toku Użytkownik wprowadzi nowe zagadnienie WYKONAWCA może je przenieść do odrębnego Zgłoszenia Serwisowego lub odrzucić realizację. Jeżeli nowe zagadnienie zostaje przeniesione do wyodrębnionego Zgłoszenia Serwisowego Termin realizacji usług określony w Warunkach brzegowych realizacji usług wszczyna swój bieg od początku.
3. Po wstępnej weryfikacji kompletności oraz formy Zgłoszenia Serwisowego, nie później niż w Czasie reakcji określonym w Warunkach brzegowych realizacji usług w systemie HD zostaje Zgłoszeniu Serwisowemu nadany status „zarejestrowane”. Alternatywnie, jeżeli weryfikacja wykaże, że Zgłoszenie Serwisowe nie spełnia wymogów Umowy lub dotyczy wątku stanowiącego przedmiot innego Zgłoszenia Serwisowego, zostaje mu nadany status odpowiednio „odrzucone” lub „duplikat”.
4. Dalsza obsługa Zgłoszenia Serwisowego przebiega na zasadach określonych w procedurach realizacji przewidzianych dla poszczególnych usług. W zależności od typu Zgłoszenia Serwisowego, fazy obsługi Zgłoszenia Serwisowego oraz jego zawartości, Zgłoszenie Serwisowe przyjmie jeden z następujących statusów:
   * nowe,
   * zarejestrowane,
   * u klienta,
   * aktywne,
   * odrzucone,
   * zrealizowane,
   * zamknięte.
5. Zamawiający dopuszcza, by w systemie HD zgłoszenia uzyskiwały inne statusy niż ww. odpowiadające aktualnemu etapowi realizacji Zgłoszenia.
6. Zamówienia indywidualne: Nowa funkcjonalność/Usługa Odpłatna – nie są objęte żadnym reżimem proceduralnym, w szczególności finansowym czy czasowym z wyłączeniem uzgodnień poczynionych w samej treści Zgłoszenia Serwisowego.
7. Szczególnym typem Zgłoszenia Serwisowego jest zapytanie handlowe. Jego ewidencja w HD służy jedynie celom informacyjnym o charakterze handlowym, natomiast obsługa nie jest objęta żadnym reżimem proceduralnym, w szczególności finansowym czy czasowym.
8. W każdym momencie Użytkownik może Zgłoszenie Serwisowe anulować, co spowoduje, że Zgłoszenie Serwisowe od momentu anulowania nie będzie przez Serwis dalej obsługiwane.
9. Po realizacji przez WYKONAWCĘ Zgłoszenia Serwisowego i wykonaniu przez WYKONAWCĘ testu poprawnego działania Modułu, zaakceptowanego przez Zamawiającego, Zgłoszenie Serwisowe traktowane jest jako zakończone.
10. Zgłoszenie Serwisowe jest ostatecznie zamykane, jeżeli upłynęło 7 dni od terminu przejścia Zgłoszenia w status zrealizowane, a Zamawiający nie wniósł w tym czasie zastrzeżeń do wyniku realizacji Zgłoszenia Serwisowego.

[USŁUGI SERWISOWE]

1. UsługarealizowanabędzieprzezWYKONAWCĘpoprzez:
   * wizytyserwisowewsiedzibieZAMAWIAJĄCEGO,
   * połączeniaZdalnego Dostępu.
2. Wizyty serwisowe realizowane będą przez Wykonawcę w zależności od potrzeb ZAMAWIAJĄCEGO.
3. Zgłoszenie wizyty serwisowej przez ZAMAWIAJĄCEGO nastąpi z 7 dniowym wyprzedzeniem. Każde Zgłoszenie zawierać będzie szczegółowo zakres prac do wykonania przez WYKONAWCĘ- zapotrzebowanie na wizytę konsultanta będzie zakładać pobyt konsultanta nie krótszy niż 5 godzin w siedzibie ZAMAWIAJĄCEGO.
4. W sytuacjach szczególnych i uzasadnionych termin wizyty serwisowej może zostać zmieniony za zgodą ZAMAWIAJĄCEGO, jednakże różnica dni w terminie wizyty nie może przekraczać 5 dni liczonych od wcześniej ustalonego terminu.
5. Połączenia zdalne realizowane będą przez Wykonawcę w godzinach pracy ZAMAWIAJĄCEGO, po wcześniejszym uzgodnieniu terminu, godziny połączenia i rodzaju prac do wykonania z osobami upoważnionymi przez ZAMAWIAJĄCEGO. Terminy realizacji usług zdalnych będą obowiązywały wówczas, kiedy ZAMAWIAJĄCY udostępni połączenie zdalne. W przypadku braku takiego dostępu terminy realizacji usług mogą się przedłużać i tym samym mogą być niedochowane co nie będzie miało odzwierciedlenia w konsekwencjach dochowania terminów realizacji określonych dla WYKONAWCY
6. Rozliczenie czasu trwania usługi wykonanej poprzez połączenie zdalne WYKONAWCA winien przesłać ZAMAWIAJĄCEMU w narzędziu HD do akceptacji. Usługa może zostać rozliczona w limicie godzin przeznaczonych na Usługi serwisowe wyłącznie po pozytywnym wykonaniu prac (osiągnięciu zamierzonego przez Zamawiającego celu i efektu) i zaakceptowaniu rozliczenia czasu trwania usługi.
7. Każdorazowe wykonanie w siedzibie ZAMAWIAJĄCEGO przez Serwis WYKONAWCY zgłoszonych prac zakończone zostanie zarejestrowaniem przez ZAMAWIAJĄCEGO lub WYKONAWCĘ w HD tych prac, zawierających w szczególności zakres wykonanych prac i liczbę przepracowanych przez Serwis WYKONAWCY godzin, a protokół będzie generowany automatycznie na podstawie zgłoszeń o statusie „zamknięte” z narzędzia HelpDesk, który to nie wymaga podpisu ze strony ZAMAWIAJĄCEGO i WYKONAWCY.

[DOSTĘP DO AKTUALIZACJI]

1. WYKONAWCA zapewni dostęp do aktualizacji za pomocą FTP z indywidualnie przydzielonym kontem Użytkownika - czas dostępu 24h/dobę w dni robocze, wolne i święta,
2. Każdy zestaw/paczka musi posiadać dokumentację opisującą wprowadzane zmiany w zakresie technicznym, funkcjonalnym i wynikającym ze zmian w prawie,
3. WYKONAWCA zapewni gwarancje zgodności zgromadzonych w systemie danych historycznych, pod kątem technicznym, funkcjonalnym i wynikającym ze zmian w prawie,
4. WYKONAWCA zapewni gwarancję zachowania pełnej sprawności systemów oraz poprawności i stabilności w zakresie przechowywania danych po wprowadzonych aktualizacjach,
5. W przypadku stwierdzenia wystąpienia wad i błędów w Module po wprowadzeniu aktualizacji WYKONAWCA zobowiązany jest do nieodpłatnego usunięcia przyczyn oraz skutków wad i błędów w terminie do 7 Dni Roboczych od momentu otrzymania zgłoszenia o tym fakcie lub innym ustalonym i po akceptacji obu stron,
6. W przypadku wystąpienia Awarii uniemożliwiającej korzystanie z Aplikacji po wprowadzeniu aktualizacji wykonawca zobowiązany jest do nieodpłatnego usunięcia przyczyn i skutków Awarii w terminie do 24 godzin od momentu otrzymania zgłoszenia o tym fakcie,
7. Dostęp do nowych wersji zapewnia:

* utrzymanie Modułu w wersji polskojęzycznej z pełną dokumentacją w języku polskim
* zabezpieczenia przed nieautoryzowanym dostępem;
* monitorowanie wszystkich zdarzeń związanych z eksploatacją Modułu, przechowując informacje o Użytkowniku obsługującym zdarzenie;

1. WARUNKI BRZEGOWE REALIZACJI USŁUG SERWISOWYCH

|  |  |  |  |
| --- | --- | --- | --- |
| Lp. lp. | Nazwa | Terminy realizacji usług | Uwagi |
| 1. | Godziny pracy Serwisu | 8:00-16:00 | W dni robocze, tj. od poniedziałku do piątku z wyłączeniem dni wolnych od pracy w rozumieniu art. 1 oraz art. 1a ustawy z dnia 18 stycznia 1951 r. o dniach wolnych od pracy (tekst jedn.: Dz. U. z 2020 r. poz. 1920). Dni robocze stosuje się także w odniesieniu do wszystkich terminów przewidzianych w Załączniku na automatyczne czynności HD oraz do terminów zastrzeżonych dla ZAMAWIAJĄCEGO. |
| 2. | Czas reakcji Serwisu | 8h | Czas liczony w Godzinach pracy serwisu od momentu zaewidencjonowania Zgłoszenia Serwisowego do momentu przyjęcia zgłoszenia tj. nadania mu statusu „zarejestrowane”. |
| 3. | Czas usunięcia Błędu Aplikacji | 10 dni | 1. Czas liczony w godzinach lub dniach roboczych od upłynięcia Czasu reakcji w Godzinach pracy Serwisu.   Od Czasu obsługi zgłoszenia odlicza się okres, w którym WYKONAWCA oczekuje na uzupełnienie Zgłoszenia przez ZAMAWIAJĄCEGO lub udostępnienie zdalnego dostępu (jeżeli dotyczy).   1. W odniesieniu do Aplikacji, których WYKONAWCA nie jest Producentem przewidziane czasy realizacji usług mogą ulec dwukrotnemu wydłużeniu, o czym ZAMAWIAJĄCY zostaje powiadomiony w Zgłoszeniu. 2. WYKONAWCA gwarantuje udostępnianie co najmniej 4 zbiorczych pakietów aktualizacji zawierających Rozwinięcia wybranych Aplikacji rocznie, publikowanych nie rzadziej niż jedna na kwartał. Jeżeli Zgłoszenie zaklasyfikowane jako Usterka Programistyczna zostanie zaewidencjonowane w HD w terminie krótszym niż 20 dni przed planowanym terminem publikacji aktualizacji zbiorczej, Uaktualnienie zostanie uwzględnione najpóźniej w kolejnej aktualizacji zbiorczej. |
| 4. | Czas usunięcia Awarii | 48h |
| 5. | Czas usunięcia Usterki Programistycznej | Następna aktualizacja zbiorcza |
| 6. | Czas obsługi Konsultacji | 10 dni |
| 7. | Termin przystąpienia Serwisu do realizacji usług zleconych | Niegwarantowany | 1. Dotyczy usług wynikających z zamówień indywidualnych. |

1. WYKAZ OBLIGATORYJNYCH USŁUG SERWISOWYCH

|  |  |  |
| --- | --- | --- |
| Lp. | Nazwa Usługi | Przedmiot Usługi |
|  | Serwis Aplikacji  [SA] | Gotowość WYKONAWCY do usuwania Błędów Modułu w posiadanym przez ZAMAWIAJĄCEGO zakresie funkcjonalnym w szczególności poprzez udostępnianie Uaktualnień Modułu. |
|  | Konserwacja [KS] | Usługa realizowana przez WYKONAWCĘ bezpośrednio lub pośrednio, jeżeli WYKONAWCA nie jest jednocześnie Producentem Modułu. Subskrypcja usługi zapewnia dostosowanie specyfikacji funkcjonalnej Modułu posiadanej przez ZAMAWIAJĄCEGO do zmian legislacyjnych. W ramach usługi Producent gwarantuje:   * udostępnienie portalu HD umożliwiającego ewidencję Zgłoszeń Serwisowych, * prowadzeniu stałego audytu w zakresie zgodności funkcji Modułu z powszechnie obowiązującymi przepisami prawa polskiego o randze co najmniej rozporządzenia, w rozumieniu art. 87 ust.1 Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. i wprowadzanie do Modułu zmian stanowiących konsekwencję wejścia w życie tychże w postaci Rozwinięć. * prowadzeniu stałego audytu w zakresie zgodności funkcji Modułu z obowiązującymi ZAMAWIAJĄCEGO zarządzeniami Prezesa Narodowego Funduszu Zdrowia i wprowadzanie do Modułu zmian stanowiących konsekwencję wejścia w życie tychże. |
|  | Ewaluacja [EW] | Usługa realizowana przez WYKONAWCĘ bezpośrednio lub pośrednio, jeżeli WYKONAWCA nie jest jednocześnie Producentem Modułu. Subskrypcja usługi zapewnia poprawę jakości i rozszerzenie specyfikacji funkcjonalnej Modułu posiadanej przez ZAMAWIAJĄCEGO w zakresie jakim Producent Modułu dokonuje Ewaluacji. W ramach usługi WYKONAWCA gwarantuje:   * wprowadzanie do Modułu nowych funkcji oraz usprawnień funkcji już w nich istniejących, stanowiących wynik inwencji twórczej Producenta, * wprowadzanie do Modułu nowych funkcji oraz usprawnień funkcji już w nich istniejących wnioskowanych przez Użytkowników. * Rozwinięcia wprowadzane w Module w wyniku inwencji twórczej Producenta rozpowszechniane w ramach Licencji są udostępniane odpłatnie i uwzględnione w opłacie zryczałtowanej wnoszonej za subskrypcję usługi. |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*(podpis osoby uprawnionej   
 do reprezentowania Wykonawcy)*