ZAŁĄCZNIK NR 2 DO SWZ

**OPIS PRZEDMIOTU ZAMÓWIENIA**

Strony zgodnie stwierdzają, że na potrzeby niniejszego OPZ wraz z załącznikami 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. **Zamawiający** – oznacza Zespół Opieki Zdrowotnej w Brodnicy im. R. Czerwiakowskiego
2. **Wykonawca** - podmiot, który ubiega się o udzielenie zamówienia, złożył ofertę albo zawarł umowę w sprawie zamówienia publicznego.
3. **Strony** - podmioty bezpośrednio uczestniczące w umowie zawiązanej na podstawie rozstrzygnięcia podstępowania dotyczącego zamówienia publicznego.
4. **System informatyczny** - zbiór powiązanych ze sobą elementów, którego funkcją jest przetwarzanie danych przy użyciu techniki komputerowej. W skład systemu wchodzą najczęściej elementy: Sprzęt komputerowy, Oprogramowanie narzędziowe, Oprogramowanie dziedzinowe.
5. **Zintegrowany System Informatyczny** (zwany dalej **Szpitalnym** **System Informatyczny** **SSI** lub **Systemem**) – system informatyczny wspomagający zarządzanie, w skład którego wchodzą zintegrowane systemy/moduły dziedzinowego oprogramowania aplikacyjnego (np. HIS, RIS, PACS, LIS itd.), działający na Sprzęcie Komputerowym z wykorzystaniem Oprogramowania Narzędziowego, udostępniający funkcjonalności opisane w dalszej części dokumentu.
6. **HIS-** (Hospital Information System) dostarczane w ramach niniejszego postępowania oprogramowanie służące do rejestrowania, przechowywania, przetwarzania i udostępniania danych związanych z realizacją procesu diagnostyczno- terapeutycznego w Szpitalu.
7. **Umowa** – umowa zawarta w ramach realizacji OPZ.
8. **SWZ** – Specyfikacja Warunków Zamówienia.
9. **Gwarancja i Serwis Oprogramowania** – Oznacza całokształt świadczonych przez Wykonawcę usług (gwarancyjno-serwisowych) związanych z zapewnieniem poprawnej pracy SSI i pozostałych składników będących przedmiotem zamówienia, szczegółowo określone w SWZ oraz w projekcie umowy.
10. **Sprzęt Komputerowy** – zestaw komputerów (w tym stacje robocze, sprzęt serwerowy) i oprzyrządowania, na którym pracuje HIS.
11. **Stacja Robocza** - oznacza komputer klasy PC lub/i terminal z monitorem, na którym pracuje HIS.
12. **Oprogramowanie Narzędziowe** – elementy oprogramowania zainstalowane na Sprzęcie Komputerowym, obejmujące w szczególności:
* systemy operacyjne (np. Windows, LINUX, UNIX),
* system zarządzania bazą danych (SZBD), zwane też oprogramowaniem bazodanowym (np. MSSQL, Oracle),
* oprogramowanie służące do administracji i zarządzania Sprzętem Komputerowym, systemem operacyjnym i systemem zarządzania bazą danych,
* oprogramowanie komunikacyjne umożliwiające podłączenie stacji dostępowych do serwera bazy;
1. **Instruktaże Administratora(ów)** – instruktaże użytkowników wskazanych przez Zamawiającego do pełnienia funkcji administratora HIS,
2. **Wdrożenie** – etap cyklu życia systemu informatycznego, polegający na instalacji i dostosowaniu oprogramowania do wymagań Zamawiającego, a także migracji danych oraz testowaniu i uruchomieniu systemu informatycznego. Podstawowe etapy procesu wdrożenia:
* Przygotowanie dokumentacji,
* Przygotowanie i skonfigurowanie infrastruktury technicznej,
* Zainstalowanie i skonfigurowanie systemu informatycznego do eksploatacji,
* Testowanie systemu,
* Uruchomienie produkcyjne systemu.
1. **Szczegółowym Harmonogramem Realizacji Zadania** – szczegółowy terminarz realizacji przedmiotu Umowy przygotowany przez Wykonawcę w terminie 14 dni roboczych od podpisania umowy, na podstawie terminów realizacji zamówienia ujętych w Umowie, i zaakceptowany przez Zamawiającego.
2. **Zadanie** – przedmiot zamówienia (przedmiot Umowy) wynikający łącznie z SWZ, Oferty Wykonawcy, Umowy.
3. **Etap** – główny element części Zadania, stanowiący funkcjonalną całość, podlegająca odrębnym odbiorom. Każdy Etap stanowi odrębną część (rozdział) niniejszego OPZ.
4. **Obszar** systemu – stanowiący funkcjonalną całość fragment HIS używany przy definiowaniu faz i Etapów (np. Obszar Oddział dla systemu HIS,).
5. **Elektroniczny System Zgłoszeń (ESZ)** – narzędzie posiadające interfejs WWW służące do rejestracji zgłoszeń (potencjalnych problemów, usterek) oraz kontroli ich cyklu życia (tzw. Issue Tracking System lub Defect Tracking System). System ESZ udostępniony zostanie przez Wykonawcę dla Zamawiającego na czas realizacji przedmiotu zamówienia.
6. **Protokół Odbiorczy** – protokół przygotowany przez Wykonawcę, będący potwierdzeniem przyjęcia przez Zamawiającego wykonanych przez Wykonawcę prac będących przedmiotem poszczególnych Etapów lub Faz.
7. **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.
8. **Protokół Rozbieżności –** dokument przygotowany przez Zamawiającego, zawierający precyzyjnie wyspecyfikowane przyczyny mające źródło w Systemie i wskazując nieprawidłowo działające funkcje Systemu, wraz z opisem tych nieprawidłowości, uniemożliwiające podpisanie Protokołu Odbiorczego.
9. **Dzień Roboczy** – każdy dzień od poniedziałku do piątku z wyłączeniem sobót i dni ustawowo wolnych od pracy.

**SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA**

Przedmiot zamówienia składa z następujących etapów:

1. Rozbudowa infrastruktury sprzętowej wraz z dostawą oprogramowania
2. Rozbudowa posiadanego przez Zamawiającego systemu HIS

Wymienione elementy będą dostarczone w ramach zamówienia publicznego realizującego projekt o nazwie:

Inwestycja modernizacji posiadanego systemu ZSI wraz z dostarczeniem oprogramowania systemowego i sprzętu modernizującego zasoby serwerowni oraz budowy sieci WiFi w ramach projektu: „Budowa kujawsko-pomorskiego systemu udostępniania elektronicznej dokumentacji medycznej – II etap” realizowanego w ramach Regionalnego Programu Operacyjnego Województwa Kujawsko-Pomorskiego na lata 2014-2020, Oś priorytetowa 2. Cyfrowy region, Działanie 2.1 Wysoka dostępność i jakość e-usług publicznych.

**OPIS RÓWNOWAŻNOŚCI:**

W przypadku gdy w dokumencie stanowiącym element opisu przedmiotu zamówienia pojawią się wskazania znaków towarowych, patentów lub pochodzenia, źródła lub szczególnego procesu, który charakteryzuje produkty lub usługi dostarczane przez konkretnego dostawcę (jeżeli mogłoby to doprowadzić do uprzywilejowania lub wyeliminowania niektórych wykonawców lub jego produktów), należy rozumieć, zgodnie z przepisem art. 99 ust. 5 ustawy Pzp, że zamawiający nie może opisać przedmiotu zamówienia w wystarczająco precyzyjny i zrozumiały sposób i w takich okolicznościach Zamawiający dopuszcza możliwość składania w ofercie rozwiązań równoważnych, wskazując, iż minimalne wymagania, jakim mają odpowiadać rozwiązania równoważne, to wymagania nie gorsze od parametrów wskazanych w tych dokumentach, a ich kryteria w celu oceny równoważności wskazane są w opisie przedmiotu zamówienia.

W przypadku, gdy Zamawiający opisuje przedmiot zamówienia przez odniesienie do norm, ocen technicznych, specyfikacji technicznych i systemów referencji technicznych, o których mowa w art. 101 ust. 1 pkt 2 i ust. 3 ustawy, zamawiający dopuszcza rozwiązania równoważne opisywanym.

Wykonawcy mogą składać oferty zawierające rozwiązania równoważne w stosunku do przedmiotu zamówienia przedstawionego w SWZ – zgodnie z art. 101 ust. 4, 5 i 6 ustawy PZP, jednak są zobowiązani wykazać, że oferowane przez nich rozwiązania spełniają wymagania określone przez Zamawiającego. Równoważność pod względem parametrów technicznych, użytkowych oraz eksploatacyjnych ma w szczególności zapewnić uzyskanie parametrów nie gorszych od założonych w niniejszym SWZ

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 niniejszym załączniku. Ciężar udowodnienia równoważności spoczywa na Wykonawcy

Wykonawca, który powołuje się na rozwiązania równoważne opisywanym przez Zamawiającego, jest obowiązany wykazać, że oferowany przedmiot zamówienia spełnia wymagania określone przez Zamawiającego poprzez złożenie opisu zaoferowanych produktów wraz z wykazaniem cech równoważności w stosunku do wymagań opisanych przez Zamawiającego w niniejszym załączniku oraz podanie nazwy handlowej i producenta.

W celu wykazania cech równoważności Zamawiający dopuszcza załączenie do opisu etykiet, zdjęć, kart katalogowych itp., z dopiskiem której pozycji asortymentowej (jakiego sprzętu) dotyczy dana informacja z zastrzeżeniem, że z tych dokumentów muszą wynikać parametry co najmniej określone przez Zamawiającego w załącznikach do OPZ i dane identyfikujące produkt.

**I. ROZBUDOWA INFRASTRUKTURY SPRZĘTOWEJ WRAZ Z DOSTAWĄ OPROGRAMOWANIA**

Poniżej wyspecyfikowano minimalne parametry sprzętu oraz oprogramowania, które należy dostarczyć w ramach realizacji przedmiotu zamówienia. W przypadku, gdy nie określono, że parametr określa maksymalną wartość jest to jego wartość minimalna.

Wymagania ogólne:

* Całość dostarczanego sprzętu i oprogramowania standardowego 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 2021.
* Całość dostarczanego rozwiązania, tzn. każde z dostarczonych urządzeń, w którym nie wskazano szczegółowych warunków gwarancji, musi być objęte minimum 24 miesięczną gwarancją jeśli w opisie parametrów nie wskazano inaczej
* 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. **Dostawa urządzeń do budowy sieci Wi-Fi – 1 komplet**Zamawiający oczekuje dostawy urządzeń do zbudowania i uruchomienia zarządzanej centralnie sieci Wi-Fi w Budynku Głównym ZOZ Brodnica. Infrastruktura kablowa niezbędna do podłączenia punktu dostępowego będzie dostarczona przez Zamawiającego.

**W ramach postępowania należy dostarczyć:

a) Przełącznik dostępowy Sieci 28 port POE - 1 szt.:**

|  |  |  |
| --- | --- | --- |
| LP  | Nazwa  | Parametr  |
| 1.  | Rozmiar  | 19-inch, 1U  |
| 2.  | Interfejsy  | * 24 x 10/100/1000Mbps POE
* 4 x 10G SFP+
 |
| 3.  | Konsola  | port konsolowy RJ45  |
| 4.  | Standardy PoE  | IEEE 802.3af, 802.3at  |
| 5.  | Budrzet Mocy POE  | Max. 370 W  |
| 6.  | Przełączanie  | 128 Gbps  |
| 7.  | Stackowanie  | Fizyczne: do 6 urzadzeń Virtualne: Do 32 urzadzeń  |
| 8.  | Tablica Mac Address  | min 16K  |
| 9.  | Spanning Tree  | 802.1D STP 802.1s MSTP 802.1w RSTP  |
| 10.  | Agregacja linków  | 802.3ad  |
| 11.  | QoS  | min 802.1p priority  |
| 12.  | Vlan  | min 4K  |
| 13.  | Typ VLAN  | GVRP w oparciu o adresację MAC w oparciu o port w oparciu o protokół  |
| 14.  | Routing  | ARP-256 Static ARP Default Routing Static Routing  |
| 15.  | Bezpieczeństwo  | Broadcast/Multicast/Unicast Storm Control Dynamic ARP Inspection D-Link Safeguard Engine DHCP Server Screening  |
| 16.  | Tablica Routingu  | IPv4 - min 64 wpisów statycznych  |
| 17.  | ACL  | Ingress VLAN-based  |
| 18.  | Obsługa  | Loopback Detection MLD Snooping  IGMP Snooping Jumbo Frame up to 9,216 Bytes Flow Control Command Line Interface (CLI) SSH LLDP, LLDP-MED. Web-based GUI  |

**b) Punkt Dostępowy Acces-Point POE - 20 szt.:**

|  |  |  |
| --- | --- | --- |
| LP  | Nazwa  | Parametr  |
| 1.  | Technologia bezprzewodowa  | Wireless AC Wave 2  |
| 2.  | Ilość pasm  | Dwupasmowy  |
| 3.  | Przepustowość  | 400 Mb/s 2.4 GHz  |
| 867 Mb/s 5 GHz  |
| 4.  | Anteny  | Wbudowana antena dookólna  |
| 5.  | Zysk mocy  | 3 dBi w 2.4 GHz  |
| 3 dBi w 5 GHz  |
| 6.  | PoE  | Tak  |
| 7.  | Porty  | 1 x Gigabit Ethernet LAN  |
| 8.  | Zasięg zakres wewnętrzny  | Min. 180 m  |
| 9.  | Montaż  | Wewnątrz  |
| 10.  | Obudowa  | Plastikowa  |
| 11.  | Tryb pracy  | Access Point (AP)  |
| 12.  | Szyfrowanie  | AES,TKIP,WEP,WPA,WPA-PSK,WPA2  |
| 13.  | Współpraca z kontrolerem  | Kompatybilny z kontrolerem accepoint w formie wirtualnej  |
| 14.  | Zarządzanie energią  | Maksymalne zużycie mocy 6,5 W  |
| 15.  | Zestaw montażowy  | Tak  |

1. **Dostarczenie routera dostępowego UTM do sieci Internet - 1 szt.**Zamawiający oczekuje dostarczenia routera dostępowego do sieci Internet klasy UTM wraz w niezbędnymi licencjami zapewniającymi ochronę sieci i wsparciem na 3 lata

Preferowane urządzenie do dostarczenia: Fortigate 60F z licencjami zapewniającymi ochronę Unified Threat Protection (UTP) (24x7 FortiCare plus Application Control, IPS, AV, Web Filtering and Antispam, FortiSandbox Cloud) oraz wsparciem na 3 lata lub równoważne.

Dostarczone urządzenie musi spełniać minimalne wymagania techniczne i funkcjonalne określone poniżej oraz ich instalacja i konfiguracja. Wymaga się dostarczenia, instalacji, skonfigurowania i uruchomienia jednego urządzenia UTM

**Podane poniżej wymagana odnoszą się do pojedynczego urządzenia.**

|  |  |  |
| --- | --- | --- |
| LP  | Nazwa  | Parametr  |
| 1.  | Wymagania Ogólne | Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej Wykonawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall’a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu. |
| 2.  | Wymagania Funkcjonalne | System musi wspierać IPv4 oraz IPv6 w zakresie:• Firewall.• Ochrony w warstwie aplikacji.• Protokołów routingu dynamicznego. Redundancja, monitoring i wykrywanie awarii1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall. 2. W ramach postępowania musi zostać dostarczone jedno urządzenie3. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.4. Monitoring stanu realizowanych połączeń VPN. 5. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych. |
| 3.  | Wymagania Firewall | 1. System realizujący funkcję Firewall musi dysponować minimum: • 5 portami LAN Giga Ethernet RJ-45 • 2 portami WAN Giga Ethernet RJ-45 2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN’y w oparciu o standard 802.1Q.4. System musi być wyposażony w zasilanie AC.Parametry wydajnościowe:1. W zakresie Firewall’a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 35 tys. nowych połączeń na sekundę.2. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B.3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.7 Gbps.4. Wydajność szyfrowania IPSec VPN nie mniej niż 6 Gbps.5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1.4 Gbps.6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 700 Mbps.7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 600 Mbps. |
| 4.  | Funkcje Systemu Bezpieczeństwa: | W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.2. Kontrola Aplikacji. 3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.5. Ochrona przed atakami - Intrusion Prevention System.6. Kontrola stron WWW. 7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.8. Zarządzanie pasmem (QoS, Traffic shaping).9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). 10. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. 11. Analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2.12. Funkcja lokalnego serwera DNS ze wsparciem dla DNS over TLS (DoT) oraz DNS over HTTPS (DoH) z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez systemPolityki, Firewall13. 2. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 14. 3. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:• Translację jeden do jeden oraz jeden do wielu.• Dedykowany ALG (Application Level Gateway) dla protokołu SIP. 15. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.16. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików.17. Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu.• Amazon Web Services (AWS).• Microsoft Azure • Google Cloud Platform (GCP).• OpenStack.• VMware NSX.Połączenia VPN1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:• Wsparcie dla IKE v1 oraz v2.• Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).• Obsługa protokołu Diffie-Hellman grup 19 i 20.• Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.• Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.• Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.• Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.• Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.• Mechanizm „Split tunneling” dla połączeń Client-to-Site.2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:• Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.• Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.• Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.Routing i obsługa łączy WAN1. W zakresie routingu rozwiązanie powinno zapewniać obsługę:• Routingu statycznego. • Policy Based Routingu.• Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM. Funkcje SD-WAN1. System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.2. Reguły SD-WAN powinny umożliwiać określenie aplikacji jako argumentu dla kierowania ruchu.Zarządzanie pasmem1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.Ochrona przed malware1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).4. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze. 5. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.6. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta. Ochrona przed atakami1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.3. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.6. Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.Kontrola aplikacji1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.2. Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. 4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur. Kontrola WWW1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. 2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.5. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo.6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.7. W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych url - system nie będzie dokonywał inspekcji szyfrowanej komunikacji. Uwierzytelnianie użytkowników w ramach sesji1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:• Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.• Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.• Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych. 2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.Zarządzanie1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.6. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.7. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.Logowanie1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.2. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.4. Musi istnieć możliwość logowania do serwera SYSLOG.CertyfikatyPoszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:• ICSA lub EAL4 dla funkcji Firewall.Serwisy i licencjeW ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:• Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 36 miesięcy.  |
| 5.  | Gwarancja oraz wsparcie | System musi być objęty serwisem gwarancyjnym producenta przez okres 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7. |

1. **Dostarczenie przełącznika FC - 1 szt.**

|  |
| --- |
| MINIMALNE WYMAGANIA TECHNICZNE  |
| 1.  | Przełącznik FC musi być wykonany w technologii FC 32 Gb/s i posiadać możliwość pracy portów FC z prędkościami 32, 16, 8 z funkcją autonegocjacji prędkości.  |
| 2.  | Przełącznik FC musi posiadać minimum 24 sloty na moduły FC. Wszystkie wymagane funkcje muszą być dostępne dla 8 portów FC przełącznika.  |
| 3.  | Przełącznik musi być dostarczony wraz z minimum 8modułami SFP FC 16 Gb/s .  |
| 4.  | Rodzaj obsługiwanych portów: D\_Port (ClearLink Diagnostic Port), E\_Port, F\_Port, M\_Port (Mirror Port);  |
| 5.  | Przełącznik FC musi mieć wysokość maksymalnie 1U i szerokość 19” oraz zapewniać techniczną możliwość montażu w szafie 19”.  |
| 6.  | Przełącznik FC musi posiadać nadmiarowe wentylatory N+1  |
| 7.  | Przełącznik FC musi być wykonany w tzw. architekturze „non-blocking” uniemożliwiającej blokowanie się ruchu wewnątrz przełącznika przy pełnej prędkości pracy wszystkich portów.  |
| 8.  | Urządzenie musi umożliwiać połączenie przełączników w jeden „fabric” (funkcjonalność ISL), dostarczyć licencje jeśli wymagane.  |
| 9.  | Przełącznik FC musi udostępniać usługę Name Server Zoning – tworzenia stref (zon) w oparciu bazę danych nazw serwerów.  |
| 10.  | Przełącznik FC musi posiadać możliwość wymiany i aktywacji wersji firmware’u (zarówno na wersję wyższą jak i na niższą) w czasie pracy urządzenia, bez wymogu ponownego uruchomienia urządzeń w sieci SAN.  |
| 11.  | Przełącznik FC musi posiadać wsparcie dla następujących mechanizmów zwiększających poziom bezpieczeństwa: * Listy Kontroli Dostępu definiujące urządzenia (przełączniki i urządzenia końcowe) uprawnione do pracy w sieci Fabric
* Możliwość uwierzytelnienia (autentykacji) przełączników z listy kontroli dostępu w sieci Fabric za pomocą protokołów DH-CHAP i FCAP
* Możliwość uwierzytelnienia (autentykacji) urządzeń końcowych z listy kontroli dostępu w sieci Fabric za pomocą protokołu DH-CHAP
* Kontrola dostępu administracyjnego definiująca możliwość zarządzania przełącznikiem tylko z określonych urządzeń oraz portów
* Szyfrowanie połączenia z konsolą administracyjną. Wsparcie dla SSHv2,
* Wskazanie nadrzędnych przełączników odpowiedzialnych za bezpieczeństwo w sieci typu Fabric.
* Konta użytkowników definiowane w środowisku RADIUS lub LDAP
* Szyfrowanie komunikacji narzędzi administracyjnych za pomocą SSL/HTTPS
* Obsługa SNMP v3
 |
| 12.  | Przełącznik FC musi posiadać możliwość konfiguracji przez komendy tekstowe w interfejsie znakowym oraz  |
|  | przez przeglądarkę internetową z interfejsem graficznym.  |
| 13.  | Przełącznik FC musi mieć możliwość instalacji jednomodowych SFP umożliwiających bezpośrednie połączenie (bez dodatkowych urządzeń pośredniczących) z innymi przełącznikami na odległość minimum 10km.  |
| 14.  | Przełącznik FC musi zapewnić możliwość jego zarządzania przez zintegrowany port Ethernet, RS232 oraz inband IP-over-FC  |
| 15.  | Przełącznik FC musi zapewniać wsparcie dla standardu zarządzającego SMI-S v1.1 (powinien zawierać agenta SMI-S zgodnego z wersją standardu v1.1)  |
| 16.  | Przełącznik FC musi zapewniać możliwość nadawania adresu IP dla zarządzającego portu Ethernet za pomocą protokołu DHCP  |
| 17.  | Przełącznik FC musi zapewniać możliwość dynamicznego aktywowania portów za pomocą zakupionych kluczy licencyjnych.  |
| 18.  | Przełącznik FC musi zapewniać opóźnienie przy przesyłaniu ramek FC między dowolnymi portami nie większe niż 900ns.  |
| 19.  | Przełącznik FC musi zapewniać sprzętową obsługę zoningu na podstawie portów i adresów WWN  |
| 20.  | Urządzenie musi wspierać mechanizm balansowania ruchem w połączeniach wewnątrz wielodomenowych sieci fabric w oparciu OXID.  |
| 21.  | Możliwość wymiany w trybie „na gorąco”: minimum w odniesieniu do modułów portów Fibre Channel (SFP).  |
| 22.  | Wsparcie dla N\_Port ID Virtualization (NPIV). Obsługa co najmniej 255 wirtualnych urządzeń na pojedynczym porcie przełącznika.  |
| 23.  | Szyny do montażu w szafie rack 19’’.  |
| 24.  | Okres gwarancji min 24 miesiące Okres dostępności gwaranta 8x5xNBD |

1. **Dostarczenia licencji serwerowych systemów operacyjnych – 1 komplet**Zamawiający oczekują dostarczenia serwerowych systemów operacyjnych umożliwiających zbudowanie domenowych usług sieciowych opartych o mechanizm usług katalogowych typu Active Directory wraz z niezbędnymi licencjami umożliwiającymi połączenia urządzeń do usług katalogowych typy Active Directory (200 licencji). Dostarczone systemy operacyjne muszą umożliwiać uruchomienie oprogramowania serwerowego firm trzecich dedykowanego na system Windows Serwer 2012R2 lub nowszy. Dostarczone licencja nie mogą być ograniczone czasowo.

Zamawiający oczekuje dostarczenia:

- 2 sztuki licencji Microsoft Windows Server Datacenter 2022 16 rdzeni 64bit lub równoważne,

- 200 sztuk licencji dostępowych CAL per device lub równoważne.

|  |
| --- |
| MINIMALNE WYMAGANIA TECHNICZNE  |
| 1.  | 1. licencje muszą mieć możliwość nielimitowanych instalacji na serwerach wirtualnych
2. wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych
3. zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe
4. wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play)
5. graficzny interfejs użytkownika
6. obsługa systemów wieloprocesorowych
7. obsługa platform sprzętowych x86, x64
8. możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu
9. możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowego programowania:
* usługi sieciowe DNS i DHCP,
* usługi katalogowe pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe),
* zdalna dystrybucja oprogramowania na stacje robocze,
* praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej,
* PKI (Centrum Certyfikatów, obsługa klucza publicznego i prywatnego),
* szyfrowanie plików i folderów, szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec),
* możliwość rozłożenia obciążenia serwerów,
* serwis udostępniania stron WWW, serwis zarządzania polityką konsumpcji informacji w dokumentach (Digital Rights Management),
* wsparcie dla protokołu IP w wersji 6 (IPv6)
1. Możliwość tworzenie serwerów wirtualnych, oprogramowanie wspierające tworzenie serwerów wirtualnych musi spełniać następujące wymagania funkcjonalne:
* warstwa wirtualizacji musi być zainstalowana bezpośrednio na sprzęcie fizycznym bez dodatkowych pośredniczących systemów operacyjnych
* licencja musi umożliwiać zmianę wersji oprogramowania na niższą (downgrade)
* rozwiązanie musi zapewnić możliwość obsługi wielu instancji systemów operacyjnych na jednym serwerze
* możliwość skonfigurowania maszyn wirtualnych z których każda może mieć 1-4 wirtualnych kart sieciowych.
* możliwość przydzielania większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera w celu osiągnięcia maksymalnego współczynnika konsolidacji
* możliwość udostępniania maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie zarezerwowane na dyskach lokalnych serwera lub na macierzy
* konsola graficzną do zarządzania maszynami wirtualnymi i do konfigurowania innych funkcjonalności.
* możliwość bieżącego monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej np. wykorzystanie procesorów, pamięci RAM, wykorzystanie przestrzeni na dyskach/wolumenach
* możliwość wykonywania kopii migawkowych instancji systemów operacyjnych (tzw. snapshot) na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy.
* możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracjąi danymi
* możliwość integracji z usługami katalogowymi Microsoft Active Directory.
* mechanizm bezpiecznego uaktualniania warstwy wirtualizacyjnej (np. wgrywania krytycznych poprawek) bez potrzeby wyłączania wirtualnych maszyn
* obsługa przełączania ścieżek SAN (bez utraty komunikacji) w przypadku awarii jednej z kilku dostępnych ścieżek.
* możliwość przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy serwerami fizycznymi,
* mechanizm wysokiej dostępności HA, w przypadku awarii lub niedostępności serwera fizycznego wybrane przez administratora i uruchomione na nim wirtualne maszyny zostały uruchomione na innych serwerach z zainstalowanym oprogramowaniem wirtualizacyjnym
* funkcjonalność wirtualnego przełącznika (virtual switch) umożliwiającego tworzenie sieci wirtualnej w obszarze hosta i pozwalającego połączyć maszyny wirtualne w obszarze jednego hosta, a także na zewnątrz sieci fizycznej.
* pojedynczy wirtualny przełącznik musi posiadać możliwość przyłączania do niego dwóch i więcej fizycznych kart sieciowych aby zapewnić bezpieczeństwo połączenia w razie awarii karty sieciowej
* wirtualne przełączniki musza obsługiwać wirtualne sieci lokalne (VLAN)
1. Możliwość wykorzystania, co najmniej 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym
2. Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny.
3. Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania do 8000 maszyn wirtualnych.
4. Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.
5. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
6. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading.
7. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
8. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
9. Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET
 |

**Licencje dostępowe serwera:**

|  |
| --- |
| MINIMALNE WYMAGANIA TECHNICZNE  |
| 1.  | 200 licencji dostępowych na urządzenie, umożliwiających zarządzanie urządzeniami z poziomu serwera AD za pośrednictwem usługi Active Directory. |

**II. ROZBUDOWA POSIADANEGO PRZEZ ZAMAWIAJĄCEGO SYSTEMU HIS – 1 komplet**

Szpital użytkuje system oprogramowania składający się na Szpitalny System Informatyczny (SSI) w części „białej” HIS: Eskulap produkcji Nexus Polska Sp. z o.o.

Wykonawca zobowiązuje się dostarczyć Zamawiającemu wymagane funkcjonalności SSI poprzez zmodernizowanie i rozbudowanie istniejącego rozwiązania w taki sposób, aby w jak najszerszym zakresie zostały zaspokojone obecne i przyszłe potrzeby Zamawiającego. Koniecznym jest zachowanie pełnej wzajemnej interoperacyjności nowo wdrażanych modułów/grup funkcjonalności, a także pełnej interoperacyjności z modułami/grupami /systemami funkcjonalności już funkcjonującymi u Zamawiającego.

W przypadku rozbudowy i zmodernizowania istniejącego systemu Wykonawca ma obowiązek zachować (utrzymać status quo) funkcjonalnie pełną, istniejącą obecnie integrację z systemami i urządzeniami zewnętrznymi, które nie są przedmiotem wymiany lub rozbudowy w ramach Projektu oraz zapewnić dostęp do historycznych danych medycznych pacjentów bezpośrednio za pomocą nowego/zmodernizowanego rozwiązania.

W przypadku, gdy Wykonawca dokonuje rozbudowy systemu posiadanego przez Zamawiającego przy użyciu produktu z innej linii produktowej (rozumianej jako produkt o innej nazwie handlowej lub innym zarejestrowanym znaku towarowym) Wykonawca zobowiązany jest zaktualizować wszystkie posiadane przez Zamawiającego moduły systemu do ich najnowszej wersji z linii produktowej wdrażanej jako rozbudowa.

Zamawiający wymaga by Wykonawca dostarczył dodatkowe bezterminowe licencje nowych modułów SSI lub równoważnego w takiej ilości, aby uzyskać wymaganą liczbę licencji zgodnie z poniższą tabelą oraz dokonał ich pełnej integracji z modułami systemu medycznego posiadanego przez Zamawiającego.

System HIS:

|  |  |
| --- | --- |
| Licencja na moduł | Rozbudowa |
| Pulpit Lekarski | Open\* |
| ePortal Pacjenta | Open\* |

\* nielimitowana liczba jednocześnie korzystających użytkowników

## Rozbudowa systemu oprogramowania medycznego do wymaganych funkcjonalności:

|  |
| --- |
| WYMAGANIA OGÓLNE  |
|  | **Architektura HIS** |
|  | HIS działa w architekturze trójwarstwowej – rozumianej jako sytuacja, w której baza danych znajduje się na serwerze centralnym obsługującym zarządzanie i przetwarzanie danych, natomiast klientem jest przeglądarka internetowa (co najmniej: Mozilla Firefox, Google Chrome, Internet Explorer) komunikująca się z użytkownikiem za pośrednictwem serwera aplikacji. Do podstawowej pracy z systemem nie jest wymagane żadne inne oprogramowanie (z zastrzeżeniem dwóch punktów poniżej). |
|  | Aplikacje ewidencji podstawowych danych i zdarzeń zapewniających bieżącą obsługę pacjentów działają zarówno w architekturze trójwarstwowej, gdzie klientem jest przeglądarka internetowa oraz dwuwarstwowej (klient serwer). W przypadku niedostępności serwerów aplikacji system musi nadal pracować w wersji dwuwarstwowej, w wymienionych obszarach posiadać tożsamy zakres funkcjonalny:* Ruchu pacjenta w obszarze izby przyjęć wraz z ewidencją danych niezbędnych do rozliczeń z NFZ,
* Obsługi zleceń medycznych w zakresie leków, diagnostyki laboratoryjnej i obrazowej w obszarze izby przyjęć,
* Ruchu pacjenta w obszarze hospitalizacji wraz z ewidencją danych niezbędnych do rozliczeń z NFZ,
* Obsługi zleceń medycznych w zakresie leków, diagnostyki laboratoryjnej i obrazowej w obszarze hospitalizacji,
* Ruchu pacjenta w obszarze porad specjalistycznych wraz z ewidencją danych niezbędnych do rozliczeń z NFZ,
* Rejestracji i wykonania badań laboratoryjnych w laboratorium,
* Rejestracji i wykonania badań diagnostycznych w pracowniach diagnostycznych,
* Bieżącego sprawozdawania świadczeń do NFZ.
* Operacji magazynowych w Aptece
* Generacji i podpisywania dokumentów EDM

Obie wersje muszą posiadać te same funkcjonalności z dokładnością do pojedynczych argumentów, a zakres używanych skrótów klawiszowych musi być spójny między wersjami architektury systemu. |
|  | Raporty są tworzone przynajmniej w formacie PDF (w przypadku występowania raportów, dopuszcza się wymaganie instalacji na stacjach klienckich wskazanej przez dostawcę systemu przeglądarki PDF). |
|  | W szczególnych przypadkach (np. komunikacja ze sprzętem, operacje na systemie plików na stacji klienckiej) dopuszcza się instalowanie i uruchamianie aplikacji zewnętrznych ze stacji klienckiej. System sam uruchamia takie aplikacje, kiedy operacje użytkownika tego wymagają. W przypadku występowania takich zastosowań, dostawca systemu może wymagać instalacji dodatkowego oprogramowania (np. rozszerzeń lub wtyczek do przeglądarek) umożliwiającego wykonanie takich operacji. |
|  | HIS posiada architekturę modułową i jest zintegrowany pod względem przepływu informacji oraz użyteczności danych. Wszystkie modułu HIS pracują w oparciu o tą samą strukturę danych w wyniku czego informacja raz wprowadzona do HIS w jakimkolwiek z modułów jest wykorzystywana we wszystkich innych. |
|  | Rozliczenia z NFZ są realizowane z obszaru całego systemu z jednej aplikacji. Nie dopuszcza się sprawozdawania świadczeń z jakichkolwiek dziedzin medycznych (POZ, diagnostyka, transport medyczny) z innych modułów.  |
|  | **Aplikacja** |
|  | HIS jest komercyjnie dostępnym rozwiązaniem, w którym wymagania określone w niniejszej tabeli, jak również dla poszczególnych aplikacji muszą być dostępne w systemie na dzień składania ofert.  |
|  | Wszystkie Aplikacje muszą być dostarczone w najnowszych dostępnych na rynku wersjach, a w zakresie funkcjonalnym zgodnie z Dokumentacją Systemu. Zamawiający wymaga, aby funkcjonalność była nie mniejsza niż zadeklarowana w niniejszym załączniku. |
|  | System zapewnia dwa mechanizmy spójności danych tego samego rekordu edytowanych w równoległych sesjach: |
|  | * edycja wyłącznie w jednej sesji: rozpoczęcie edycji w jednej sesji blokuje edycję w pozostałych sesjach, które mogą jednak uzyskać dostęp do danych w trybie odczytu. Przed rozpoczęciem edycji w kolejnej sesji pierwsza sesja musi zatwierdzić zmiany, a druga odświeżyć dane przed rozpoczęciem ich edycji
 |
|  | * edycja równoległa (minimum dla karty pacjenta, pozycji wypisu, opisu wizyty w poradni, opisu zabiegu operacyjnego): ten sam rekord może być edytowany równolegle w wielu sesjach. Zmiany niekonfliktowe (różnych atrybutów) wykonane w innej sesji są automatycznie odświeżane w momencie zapisania zmian w bieżącej sesji. Zmiany konfliktowe (dwie sesje równolegle zmodyfikowały ten sam atrybut) są obsługiwane wg różnych zasad:
 |
|  | * automatyczne nadpisanie (np. data ostatniej edycji rekordu)
 |
|  | * pytanie użytkownika:
 |
|  | * które dane mają być ostatecznie zapisane w bazie: te, które zostały wpisane w innej sesji (i aktualnie znajdują się w bazie), czy nowe dane z jego sesji (np. dane lekarza kwalifikującego do zabiegu); dodatkową opcją w tym przypadku jest przerwanie całej operacji zatwierdzenia danych
 |
|  | * możliwość scalenia modyfikacji z różnych sesji (np. opis zabiegu - to samo pole mogą edytować równolegle różni użytkownicy, ostatecznie wszystkie zmiany są scalane w jeden tekst)
 |
|  | * blokada zatwierdzenia danych w przypadku wykrycia równoległej edycji kluczowych danych w różnych sesjach (np. status zabiegu)
 |
|  | System posiada narzędzie prezentujące ścieżkę zagłębienia użytkownika w danym momencie w aplikacji (np. breadcrumb). Funkcja umożliwia śledzenie jego aktualnej lokalizacji w aplikacji oraz przyspieszoną nawigację dzięki umożliwieniu powrotu do dowolnego miejsca ścieżki. |
|  | System posiada funkcjonalność, która automatycznie zapamiętuje w polach przewidzianych do wprowadzania treści opisowych bieżące zmiany zalogowanego użytkownika. Treści zapamiętywane są na czas edycji i można z nich skorzystać (na zasadzie schowka) w przypadku utraty sesji użytkownika do czasu trwałego zapisu w systemie bazodanowym. |
|  | HIS posiada możliwość pracy na platformach systemowych Windows wspieranych przez jego producenta. W odniesieniu do aplikacji z interfejsem dedykowanym na tablety wymaga się, żeby pracowały na systemie Android. |
|  | Językiem obowiązującym w HIS musi być język polski. Dotyczy to wszystkich menu, ekranów, raportów, wszelkich komunikatów, wprowadzania, wyświetlania, sortowania i drukowania. Polskie znaki diakrytyczne będą, w chwili instalacji, dostępne w każdym miejscu i dla każdej funkcji w HIS łącznie z wyszukiwaniem, sortowaniem (zgodnie z kolejnością liter w polskim alfabecie), drukowaniem i wyświetlaniem na ekranie. |
|  | HIS musi zapewniać proces wyszukiwania danych z zastosowaniem znaków polskich, znaków polskich diakrytycznych oraz znaków specjalnych, zastępujących co najmniej fragment wyszukiwanego tekstu lub pojedynczy znak(np. „\*” - fragment tekstu, „?” – pojedynczy znak). |
|  | W przypadku braku interakcji z systemem użytkownika (tj. operacji na systemie plików i komunikacji z zewnętrznymi aplikacjami), system działa na systemach operacyjnych innych niż Windows (co najmniej Linux i Android). |
|  | System ma możliwość integracji z innymi aplikacjami działającymi na stacji klienckiej (np. oprogramowaniem innych producentów) w taki sposób, że wybrany ekran systemu można wywołać z zewnętrznej aplikacji bez konieczności logowania do systemu przez użytkownika (jeżeli użytkownik ma konto w systemie, logowanie odbywa się "w tle"). |
|  | System umożliwia operacje na plikach na stacji klienckiej. |
|  | HIS posiada funkcję/narzędzie, dzięki któremu uaktualnienia aplikacji w sposób automatyczny (uprzednio zdefiniowany) są rozpowszechniane na wszystkie stacje robocze/terminale bez konieczności wykonywania jakichkolwiek czynności poza obszarem serwerowym.  |
|  | W procesach wymagających nanoszenia/prezentacji obszernej ilości danych wykorzystywana jest tzw. zakładkowa architektura okienek umożliwiająca poruszanie się pomiędzy nimi bez konieczności kolejnego ich otwierania i zamykania. |
|  | Użytkownik może z poziomu aplikacji zmniejszyć lub powiększyć formularz, z którym pracuje oraz wyzerować powiększenie. |
|  | System ma kilka wersji kolorystycznych (minimum 3), użytkownik ma możliwość wybrania zestawu kolorów dla wszystkich formularzy (zmiana zestawu kolorów nie zmienia układu formularzy). |
|  | W HIS zaimplementowana jest obsługa skrótów klawiaturowych (kombinacje kilku klawiszy) dla najczęściej używanych funkcji. |
|  | W HIS zaimplementowana jest obsługa skrótów klawiaturowych (kombinacje kilku klawiszy) dedykowanych Administratorowi oraz zaawansowanym użytkownikom (definiowane na poziomie uprawnień) umożliwiająca realizację następujących funkcji:  |
|  | * uzyskanie z poziomu aplikacji informacji o elemencie bazodanowym reprezentowanym przez dany obiekt interfejsu użytkownika (przyciski, pola edycyjne) wraz z prezentacją wszystkie schematów uprawnień w których wybrany obiektu można użyć do przydzielenia/modyfikacji uprawnień
 |
|  | * uzyskania z poziomu aplikacji informacji o lokalizacji rekordu danych w bazie danych powiązanego z polem, w którym znajduje się kursor
 |
|  | * stworzenia z poziomu aplikacji zapytania za pomocą sql do bazy danych w celu uzyskania żądanego wykazu danych
 |
|  | * uzyskania z poziomu aplikacji informacji o nazwie i wersji formularza na którym obecnie użytkownik pracuje
 |
|  | * uzyskania z poziomu aplikacji informacji o identyfikatorach zewnętrznych nadanych przez płatnika NFZ w komunikacji za pomocą formatu otwartego.
 |
|  | Pola obligatoryjne, opcjonalne i wypełniane automatycznie muszą być jednoznacznie rozróżnialne przez użytkownika (np. inny kształt, kolor, itp.). |
|  | HIS dynamicznie w zależności od kontekstu pokazuje lub ukrywa przyciski. |
|  | HIS zapewnia możliwość przenoszenia sesji użytkownika z jednego stanowiska komputerowego na drugie. |
|  | W przypadku uruchomienia na jednej stacji wielu sesji przez użytkownika system zapewnia możliwość przeniesienia tylko jednej, wskazanej sesji. |
|  | HIS zapewnia możliwość przeniesienia sesji z wypełnionymi polami, niezapisanymi zmianami do bazy danych bez utraty tych zmian po przeniesieniu. |
|  | System wyświetla na ekranie, z którego sesja została przeniesiona, informacje dokąd przeniesiono sesję.  |
|  | Dla funkcjonalności przenoszenia sesji system HIS ma zapewnić możliwość: |
|  | * włączenia i wyłączenia funkcjonalności przenoszenia
 |
|  | * odebrania definiowalnym użytkownikom funkcjonalności przenoszenia sesji
 |
|  | * odebrania definiowalnym adresom IP możliwości przenoszenia sesji
 |
|  | * ograniczenia widoków, z których w systemie można przenosić sesje.
 |
|  | System HIS zapewnia obsługę listy wartości w cechami: |
|  | * dynamiczne filtrowanie wyników na podstawie wprowadzanego tekstu.
 |
|  | * stronicowanie list wartości
 |
|  | * możliwość decydowania przez użytkownik o rozmiarze strony na liście wartości.
 |
|  | * administrator ma możliwość ustalenia wielkości domyślnej rozmiaru listy wartości dla wszystkich użytkowników
 |
|  | * prezentacja łącznej liczby wszystkich elementów w liście.
 |
|  | **Zarządzanie Systemem** |
|  | Moduł agreguje funkcje administracyjne z wszystkich modułów stanowiących przedmiot zamówienia lub jego zakres licencyjny i pozwala administratorowi na uruchomienie tych modułów. |
|  | System w wersji przeglądarkowej posiada dla administratora Menedżer sesji w zakresie zapewnienia podglądu: |
|  | * wszystkich aktywnych sesji użytkowników w systemie w wersji przeglądarkowej z zapewnieniem prezentacji numeru IP każdej sesji, z czasem startu oraz czasem pracy
 |
|  | * wszystkich sesji aplikacji, na których użytkownik się nie zalogował wraz z numerami IP, z których utworzono te sesje, z czasem startu oraz czasem pracy.
 |
|  | Możliwość zakończenia przez administratora wybranej sesji z Menedżera sesji. |
|  | Możliwość wysłania wiadomości z Menedżera sesji:  |
|  | * do wszystkich użytkowników
 |
|  | * do wybranej sesji użytkownika, tak aby nie pokazała się w innych sesjach tego samego użytkownika
 |
|  | * do wybranej sesji, na której nie zalogował się użytkownik.
 |
|  | Administrator posiada możliwość przeglądu: |
|  | * aktualnie pracujących w systemie użytkowników wraz z podaniem modułu i formularza, z którym pracują
 |
|  | * obiektów bazy danych blokowanych przez sesje użytkowników.
 |
|  | Administrator posiada możliwość: |
|  | * rekonfiguracji formularzy wskazanych w procesie wdrożenia, w szczególności podpięcie wywołania innych formularzy lub raportów pod przyciski występujące na formularzach. Funkcja powinna być dostępna co najmniej na karcie pobytu pacjenta oraz w dokumentacji medycznej wskazanej w procesie wdrożenia
 |
|  | * dodawania nowych przycisków na formatkach z przypisaniem uprawnień do ich uruchomienia, jak również przyporządkowania przyciskom już istniejącym nowego znaczenia bez ingerowania w kod źródłowy
 |
|  | * ustawiania parametrów pracy całego systemu, poszczególnych modułów i jednostek organizacyjnych.
 |
|  | HIS zapewnia możliwość wywoływania danego formularza lub raportu z różnych miejsc w systemie. |
|  | System zapewnia zarządzanie informacją o modułach (wchodzących w ich skład formularzach, raportach i obiektach bazy danych wraz z informacją o wersjach).  |
|  | System zapewnia kontrolę poprawności wersji uruchamianych formularzy. |
|  | Obsługa połączenia z systemem: logowanie, wybór modułu, screenlock, zmiana hasła, informacje o wersji formularza. |
|  | System zapewnia zarządzanie w zakresach:  |
|  | * zarządzanie księgami szpitalnymi wraz z wykonaniem operacji zamknięcia roku
 |
|  | * definiowanie list oczekujących, zdarzeń i produktów kontraktowych nimi związanych
 |
|  | * przechowywanie, wprowadzanie i zarządzanie informacją o formularzach, raportach i raportach definiowalnych.
 |
|  | HIS posiada możliwość ewidencji komunikatów o błędach pojawiających się w systemie. |
|  | System zapewnia administratorowi możliwość zastąpienia standardowych komunikatów własnymi. |
|  | Usuwanie (łączenie) kartotek pacjenta wraz z prezentowaniem listy usuniętych kartotek. |
|  | System zapewnia obsługę automatycznej numeracji dokumentów, ksiąg. |
|  | Administrator posiada możliwość wyboru danych, które mają być monitorowane w logach systemu z dokładnością do poszczególnych kolumn w tabelach danych, a zarządzanie nimi może odbywać się z poziomu narzędzi do zarządzania bazami danych (dopuszcza się narzędzie na poziomie motoru bazy danych).  |
|  | HIS posiada mechanizmy umożliwiające zapis i przeglądanie danych o logowaniu użytkowników do HIS pozwalające na uzyskanie informacji o czasie i miejscach ich pracy. |
|  | System zapewnia rejestrację zmian danych: |
|  | * rejestracja odbywa się niezależnie od mechanizmów wykorzystywanych przez bazę danych
 |
|  | * możliwość konfiguracji przez administratora dowolnych tabel w bazie danych, dla których odbywa się rejestracja zmian
 |
|  | * rejestracja obejmuje zmiany wykonywane za pomocą HIS, ja również dowolnej aplikacji umożliwiającej dostęp do bazy danych (np. sql).
 |
|  | * każda modyfikacja jest opisywana danymi:
 |
|  | * czas modyfikacji zapisany z maksymalną dostępną dokładnością (przynajmniej tysięczne części sekundy)
 |
|  | * identyfikator sesji w bazie danych (do powiązania wpisu z logami bazy danych)
 |
|  | * nazwa użytkownika zalogowanego do bazy danych
 |
|  | * nazwa użytkownika zalogowanego do systemu operacyjnego
 |
|  | * adres IP sesji, z której dokonano modyfikacji
 |
|  | * narzędzie, za pomocą którego dokonano modyfikacji (nazwa modułu i formularza systemu HIS lub nazwa innego programu, za pomocą którego dokonano modyfikacji)
 |
|  | * każdy rekord zmiany zawiera wyłącznie zmodyfikowane kolumny / dane, bez zapisu danych, które nie uległy zmianie
 |
|  | * w przypadku usunięcia rekordu zapisywana jest jego pełna wartość przed usunięciem
 |
|  | * tabela objęta mechanizmem logu zostanie zmodyfikowana podczas aktualizacji systemu, odpowiednie mechanizmy rejestru zmian (logu) zostaną automatycznie modyfikowane dostosowując go do nowej struktury tabeli
 |
|  | * wyłączenie logu na danej tabeli nie ma powodować usunięcia danych z logu, jedynie rezygnację z zapisu nowych modyfikacji do logu. Każda operacja włączenia i wyłączenia mechanizmu logu jest rejestrowana w odpowiedniej tabeli logu
 |
|  | * wszystkie operacje włączenia i wyłączenia mechanizmu logu na poszczególnych obiektach oraz operacje zmiany na obiektach logu są rejestrowane
 |
|  | Aplikacja zapewnia narzędzia do pielęgnowania i przeglądania danych logu. |
|  | Możliwość przeglądu danych rejestru zmian (logu) bezpośrednio w aplikacji w ujęciach: |
|  | * przekrojowym:
 |
|  | * lista zmian filtrowana wg rożnych kryteriów (czas, użytkownik, sesja)
 |
|  | * pozwalającym na ustalenie, co się działo w bazie o określonym czasie, albo co robił konkretny użytkownik
 |
|  | * opis zmian prezentowany w postaci pełnego opisu zmienionych danych lub listy zmodyfikowanych kolumn
 |
|  | * Zapewniający bezpośrednie przejście do formularza prezentującego historię zmian wskazanego rekordu
 |
|  | * historii zmian jednego rekordu:
 |
|  | * możliwość ograniczenia listy do modyfikacji wybranej kolumny
 |
|  | * możliwość automatycznego wyświetlenia logu tabel powiązanych przez klucze obce z synchronizacją czasu rekordów w logu
 |
|  | * wyróżnianie rekordów rejestru zmian (logu), w których wykryto manipulację danymi
 |
|  | * możliwość przejścia do prezentacji przekrojowej opisującej okres wybranej zmiany.
 |
|  | System umożliwia administratorowi podgląd i analizę zmian wybranego wpisu w bazie danych bezpośrednio z okien ewidencyjnych w systemie.  |
|  | System zapewnia rejestrację dostępu do danych: |
|  | * dla wszystkich formularzy zdefiniowanych w konfiguracji
 |
|  | * z informacją o kontekście wywołania, uzupełnioną w konfiguracji.
 |
|  | System zapewnia rejestrację dostępu do danych, z zapisaniem: |
|  | * czas dostępu
 |
|  | * użytkownik bazy dany
 |
|  | * identyfikator sesji
 |
|  | * nazwa formularza
 |
|  | * identyfikator pacjenta, w kontekście którego zrealizowano dostęp (jeśli jest dostępny)
 |
|  | * dodatkowy opis kontekstu (np. identyfikator pobytu na oddziale).
 |
|  | **Uwierzytelnianie i zarządzanie uprawnieniami** |
|  | HIS w zakresie wszystkich aplikacji oprócz mobilnych musi zostać zintegrowany z usługą Active Directory w ten sposób, że użytkownik po zalogowaniu do systemu operacyjnego nie musiał się ponownie logować do aplikacji.  |
|  | * Integracja z AD musi być realizowana w zakresie minimum: tworzenia, modyfikacji, usuwania, blokowania użytkowników.
 |
|  | * Każdy użytkownik w AD musi mieć swój unikalny odpowiednik w bazie danych (Nie dopuszcza się rozwiązań, w których kilku użytkowników w AD jest reprezentowanych w bazie danych w postaci jednego użytkownika).
 |
|  | * Wszystkie hasła użytkowników HIS są przechowywane w bazie danych w postaci niejawnej (zaszyfrowanej).
 |
|  | * Hasła użytkowników mogą być tworzone ręcznie lub automatycznie. Mechanizm automatyczny generuje ciąg losowych znaków (30 znaków lub więcej) i przypisuje go jako hasło użytkownika.
 |
|  | * Dla każdego użytkownika istnieje możliwość skonfigurowania sposobu logowania do systemu w trzech następujących trybach: tylko hasłem, tylko kartą, tylko czytnikiem biometrycznym, zarówno hasłem, jak i kartą, (lub za pomocą innego nośnika certyfikatów obsługiwanego w systemie Windows).
 |
|  | W celu przyspieszenia procesu logowania i rozpoczęcia pracy w systemie przez użytkownika system umożliwia administratorowi definiowanie domyślnego modułu oraz domyślnej jednostki organizacyjnej dla każdego użytkownika indywidualnie: |
|  | * niezależnie od stanowiska komputerowego
 |
|  | * z możliwością rozróżnienia ustawień dla poszczególnych stanowisk komputerowych.
 |
|  | HIS zapewnia wykorzystanie tego samego mechanizm logowania przez wersję trójwarstwową i aplikacje mobilne. |
|  | HIS umożliwia w trakcie logowania wybór bazy danych, do której użytkownik chce się zalogować. Funkcja jako domyślną przyjmuje bazę produkcyjną i wymaga wskazania bazy jedynie w przypadku logowania do innej bazy (np. testowej). Wywołanie funkcji zmiany bazy jest dostępne także za pomocą skrótu klawiaturowego.  |
|  | HIS zapewnia możliwość niezależnego zalogowania kilku różnych użytkowników w tej samej sesji przeglądarki, w sąsiednich kartach tego samego okna. |
|  | HIS zapewnia możliwość niezależnego zalogowania kilku różnych użytkowników w tej samej sesji przeglądarki bez potrzeby korzystania z tzw. trybu prywatnego przeglądarki. |
|  | HIS umożliwia automatyczne wylogowanie użytkownika z systemu (przy przekroczeniu zadanego czasu bezczynności ustanowionego uprzednio przez Administratora). |
|  | HIS umożliwia przechowywanie, wprowadzanie i zarządzanie informacją: o użytkownikach i administratorach systemu oraz pracownikach szpitala nie mających dostępu do aplikacji. |
|  | HIS umożliwia automatyczne blokowanie niewykorzystywanych kont użytkowników po zidentyfikowaniu braku logowania przez zadany okres czasu. |
|  | W HIS są zaimplementowane mechanizmy walidacji haseł zgodnie z wymaganiami ustawowymi przewidzianymi dla rodzaju danych przetwarzanych przez HIS. Umożliwia w szczególności określenie reguł powtarzalności haseł minimum w zakresie:* okresu, w jakim nie może być ponownie wykorzystane hasło
* liczby znaków, którą muszą różnić się kolejne hasła.
 |
|  | HIS umożliwia niezależną konfigurację reguł złożoności haseł dla administratorów i użytkowników. |
|  | HIS umożliwia wygenerowanie hasła tymczasowego w przypadku np. zagubienia karty (innego nośnika certyfikatu). |
|  | HIS umożliwia zdefiniowanie super\_użytkowników, nie będących administratorami, posiadającymi możliwość zmiany hasła innych użytkowników (w celu scedowania zadań związanych ze zmianą haseł z administratorów np. na kierowników komórek organizacyjnych, pion organizacyjny). |
|  | HIS umożliwia konfigurację dla każdego super\_użytkownika listy użytkowników, dla których może on zmieniać hasło. |
|  | HIS umożliwia administratorowi z poziomu aplikacji definiowanie i zmianę praw dostępu (uprawnień) dla poszczególnych użytkowników i grup użytkowników z dokładnością do poszczególnych: |
|  | * Modułów
 |
|  | * jednostek organizacyjnych
 |
|  | * opcji menu
 |
|  | * formularzy, w tym również przycisków w obrębie formularzy
 |
|  | * Raportów
 |
|  | * obiektów bazy danych (tabel, perspektyw, funkcji itd.) z rozróżnieniem praw.
 |
|  | HIS umożliwia przydzielenie pracownikowi różnych schematów uprawnień osobno dla każdej jednostki organizacyjnej, w której pracownik ma pracować w systemie. |
|  | HIS umożliwia administratorowi:  |
|  | 1. eksportowanie, importowanie, przenoszenie, duplikowanie schematów uprawnień
 |
|  | 1. kopiowanie schematów uprawnień z jednego pracownika na innego pracownika
 |
|  | 1. raportowanie różnic pomiędzy poszczególnymi schematami
 |
|  | 1. ręczne zablokowanie konta użytkownika przez administratora
 |
|  | * ewidencję daty zablokowania konta w przyszłości, z zapewnieniem automatycznego zablokowania kontra przez system po upływie wprowadzonej daty
 |
|  | 1. możliwość usuwania konta użytkownika.
 |
|  | **Słowniki, współprace** |
|  | HIS umożliwia administratorowi zarządzanie danymi podmiotu (nazwa, adres, NIP, REGON). |
|  | HIS umożliwia administratorowi i uprawnionym użytkownikom z poziomu aplikacji definiowanie i zmianę następujących słowników: |
|  | * rozpoznań zgodnie z klasyfikacją ICD-10
 |
|  | * procedur medycznych zgodnie z nową edycją klasyfikacji procedur ICD-9
 |
|  | * kodów terytorialnych
 |
|  | * Województw
 |
|  | * Powiatów
 |
|  | * Gmin
 |
|  | * Miejscowości
 |
|  | * Ulic
 |
|  | * kodów pocztowych
 |
|  | * płatników (w tym oddziałów NFZ)
 |
|  | * jednostek i lekarzy kierujących
 |
|  | * Kontrahentów
 |
|  | * innych uznanych przez producenta za niezbędne.
 |
|  | HIS ma możliwość budowania wewnętrznego szpitalnego katalogu procedur medycznych, którym jest nadrzędnym katalogiem w stosunku do ICD-9 i głównym wykorzystywanym przez użytkowników systemu. Katalog procedur wewnętrznych jest powiązany z ICD-9 w relacji jeden do n. (tzn. wiele procedur wewnętrznych może być skorelowane z jedną procedurą ICD-9). Celem katalogu procedur wewnętrznych jest jak najlepsze semantyczne odwzorowanie przypadków klinicznych, natomiast cała sprawozdawczość do NFZ ma być realizowana w oparciu o ICD-9. |
|  | HIS zapewnia przechowywanie, wprowadzanie i zarządzanie informacją o jednostkach organizacyjnych wraz ustaleniem ich hierarchii.  |
|  | HIS współpracuje z wieloma bazami produktów leczniczych jednocześnie w tym co najmniej BAZYL i BLOZ. |
|  | W miejscach przyjęć Pacjenta HIS współpracuje z klawiaturami z wbudowanym OCR umożliwiającym skanowanie imienia i nazwiska Pacjenta z dowodu osobistego. |
|  | W aplikacjach umożliwiających digitalizację dokumentów wchodzących w zakres dokumentacji medycznej HIS jest zintegrowany z urządzaniami skanującymi (co najmniej dwóch niezależnych producentów). Użytkownik z wykorzystaniem terminala wbudowanego w urządzeniu może wybrać pacjenta oraz rodzaj digitalizowanego dokumentu, następnie po zakończonym procesie skanowania, dokument zapisze się w Elektronicznym Rekordzie Pacjenta.  |
|  | Wykonawca zobowiązany będzie trakcie realizacji umowy lub powiązanego z nią okresu gwarancyjnego do opracowania elektronicznych dokumentów: karty informacyjnej leczenia szpitalnego, karty odmowy przyjęcia do szpitala, informacji dla lekarza kierującego, recepty, skierowania w postaci elektronicznej zgodnej z wytycznymi CSIOZ. Ponadto jeżeli CSIOZ opublikuje nowe szablony dokumentów w ramach Polskiej Implementacji Krajowej HL7 CDA, wykonawca zobowiązany będzie ująć je w HIS w okresie wdrożenia i gwarancji. |
|  | System pozwala na generowania kodów kreskowych zgodnych ze standardem GS1. |
|  | System pozwala na generowanie i wydruk kodów kreskowych w formacie Code 128: |
|  | * kod musi zawierać dowolne znaki ASCII z zakresu 32-127 (cyfry, duże i małe litery, znaki specjalne)
 |
|  | * do zapisu ciągów cyfr wykorzystywany musi być zestaw kodów C podwójnej gęstości (dwie cyfry na symbol)
 |
|  | * podczas kodowania wykonywana ma być optymalizacja długości kodu - ciągi cyfr występujące w treści alfanumerycznej przedstawiane są za pomocą symboli podwójnej gęstości, jeżeli jest to korzystne
 |
|  | * powyższe zasady dotyczą również generowanych kodów GS1-128.
 |
|  | Kody mogą być drukowane z systemu na różnych nośnikach: |
|  | * kartkach z raportami, wydrukami z systemu
 |
|  | * naklejkach drukowanych w postaci arkuszy naklejek lub pojedynczo na specjalizowanych drukarkach naklejek
 |
|  | * opaskach identyfikujących
 |
|  | * innych nośniki minimum na kasetkach i szkiełkach w histopatologii.
 |
|  | System musi współpracować z dowolnym czytnikiem kodów kreskowych symulującym wejście z klawiatury. |
|  | **Raporty** |
|  | System umożliwia drukowanie, wyświetlanie i zapisywanie raportów. |
|  | Generowanie raportów i zestawień może być automatycznie przekierowywane na drukarkę i nie wymaga ich wyświetlania ani żadnego dodatkowego potwierdzania wydruku (wymóg nie dotyczy raportów wymagających podpisu elektronicznego). |
|  | System obsługuje drukowanie raportów przeznaczonych na dedykowane drukarki (np. na drukarkę kodów kreskowych) bez pytania użytkownika o wybór drukarki (o ile taka została skonfigurowana w systemie). |
|  | System zapewnia możliwość wydrukowania raportu bez wyświetlenia tego raportu na dedykowaną drukowaną. |
|  | System zapewnia możliwość włączenia/wyłączenia powiadomienia użytkownika o wysłaniu wydruku na drukarkę. |
|  | W ramach HIS zapewnione jest oprogramowanie narzędziowe pozwalające na definiowanie i generowanie dowolnych zestawień i raportów związanych z zawartością informacyjną bazy danych. Raporty takie muszą mieć możliwość wywołania przez użytkownika z poziomu aplikacji: |
|  | * raporty umożliwiają eksport danych do formatu xls
 |
|  | * raporty umożliwiają eksport danych do formatu MS Office/ Open Office
 |
|  | * raporty umożliwiają eksport danych do formatu html
 |
|  | * w HIS jest możliwy podgląd wszystkich dostępnych raportów z jednego miejsca
 |
|  | * każdej jednostce organizacyjnej można zdefiniować odrębny zakres raportów.
 |
|  | **Wymagania ogólne dla rozwiązań mobilnych** |
|  | Działanie na tabletach z system operacyjnym Google Android 4.0 lub nowszym. |
|  | Działanie na tabletach z ekranem 5.88 cali lub większym. |
|  | Możliwość wyboru zestawu kolorów aplikacji z listy predefiniowanych zestawów. |
|  | Możliwość wyboru rozmiaru czcionki w aplikacji z listy predefiniowanych rozmiarów. |
|  | Możliwość ograniczenia hasłem dostępu do konfiguracji aplikacji na urządzeniu mobilnym. |
|  | Możliwość zalogowania do aplikacji z wykorzystaniem nazwy użytkownika i hasła. |
|  | Możliwość zalogowania do aplikacji z wykorzystaniem karty inteligentnej zgodnej z normą PKN-CEN/TS 15480-2. |
|  | Obsługa skanowania kodów kreskowych za pomocą czytnika kodów kreskowych wbudowanego w tablet. |
|  | **Motor bazy danych** |
|  | Motor bazy danych (RDBMS) musi być dostępny na platformy systemów operacyjnych: Windows, Linux, Unix. |
|  | RDBMS zapewnia niezależność platformy systemowej dla oprogramowania klienckiego od platformy systemowej bazy danych. |
|  | RDBMS posiada komercyjne wsparcie producenta. Nie dopuszcza się zastosowania RBD typu open-source. |
|  | RDBMS umożliwia eksport i import danych z bazy danych w formacie tekstowym z uwzględnieniem polskiego standardu znaków. |
|  | Odtwarzanie musi umożliwiać odzyskanie stanu danych z chwili wystąpienia awarii bądź cofnąć stan bazy danych do punktu w czasie. W przypadku odtwarzania do stanu z chwili wystąpienia awarii odtwarzaniu może podlegać cała baza danych bądź pojedyncze pliki danych |
|  | Przeniesienie i tuning bazy danych do nowego środowiska. Wymagane przeniesienie konfiguracji aktualnie działającego środowiska. W celu weryfikacji poprawności działania Zamawiający oczekuję przeprowadzenia testów działania klastra na podstawie kopi zapasowej udostępnionej przez Zamawiającego wraz wykonaniem dokumentacji powykonawczej. Wymagane jest przygotowanie diagramu wdrożenia wraz z dokumentacją i opisem zastosowanych procedur i wykorzystanych technologii na wypadek awarii. Powyższe usługi muszą zostać wykonane w sposób zapewniający po ich realizacji bezawaryjną pracę eksploatowanego przez Zamawiającego systemu HIS  |
|  | Dostarczone licencje nie mogą ograniczać liczby użytkowników końcowych korzystających z oprogramowania ani liczby przetwarzanych lub przechowywanych dokumentów, plików, rekordów, żądań, etc. Licencje nie mogą być ograniczone czasowo. |
|  | Dostępność narzędzi migracji baz danych pomiędzy platformami na poziomie fizycznym (kopiowanie / konwersja plików danych) oraz logicznym (narzędzia eksportu / importu), wymaganie nie musi zostać spełnione w przypadku dostarczenia oprogramowania działającego w oparciu o jedną bazę danych. |
|  | RDBMS zapewnia wsparcie dla protokołu XA. |
|  | RDBMS zapewnia wsparcie dla standardu JDBC 3.0. |
|  | RDBMS zapewnia zgodność ze standardem ANSI/ISO SQL 2003 lub nowszym. |
|  | RDBMS zapewnia obsługę wyrażeń regularnych zgodną ze standardem POSIX dostępna z poziomu języka SQL jak i procedur/funkcji składowanych w bazie danych. |
|  | RDBMS posiada możliwość zagnieżdżania transakcji – uruchomienia niezależnej transakcji wewnątrz transakcji nadrzędnej. |
|  | RDBMS umożliwia zmianę domyślnego trybu izolowania transakcji (Read Commited) na inny (Read Only, Serializable) za pomocą komend serwera bazy danych. |
|  | RDBMS umożliwia migrację bazy danych utrzymujących dane znakowe w 8-bitowej stronie kodowej do Unicode. |
|  | RDBMS umożliwia definiowanie w przestrzeni danych (plików) dla danych użytkownika obszarów o innym niż domyślny rozmiarze bloku. |
|  | RDBMS umożliwia budowanie indeksów o strukturze B-drzewa. Baza danych powinna umożliwiać założenie indeksu jednej lub większej liczbie kolumn tabeli, przy czym ograniczenie liczby kolumn na których założony jest 1 indeks nie powinno być mniejsze niż 16. |
|  | RDBMS umożliwia wykonywanie i katalogowanie kopii bezpieczeństwa bezpośrednio przez serwer bazy danych. Umożliwia zautomatyzowane usuwanie zbędnych kopii bezpieczeństwa przy zachowaniu odpowiedniej liczby kopii nadmiarowych - stosownie do założonej polityki nadmiarowości backup'ów. Wykonywanie kopii bezpieczeństwa musi być możliwe w trybie offline oraz w trybie online(hot backup). |
|  | Przywileje użytkowników bazy danych powinny być określane za pomocą przywilejów systemowych (np. prawo do podłączenia się do bazy danych - czyli utworzenia sesji, prawo do tworzenia tabel itd.) oraz przywilejów dostępu do obiektów aplikacyjnych (np. odczytu / modyfikacji tabeli, wykonania procedury). Baza danych powinna umożliwiać nadawanie ww. przywilejów za pośrednictwem mechanizmu grup użytkowników / ról bazodanowych. W danej chwili użytkownik może mieć aktywny dowolny podzbiór nadanych ról bazodanowych. |
|  | RDBMS umożliwia budowanie widoków zmaterializowanych odzwierciedlających stan danych zdefiniowanych przez zapytanie SQL. Widok zmaterializowany przechowuje rezultat zapytania, którego aktualizacja odbywa się w jednej z dostępnych strategii – na żądanie, okresowo bądź po każdym zatwierdzeniu transakcji modyfikującej tabele, na której oparty jest widok zmaterializowany. |
|  | RDBMS powinien umożliwiać wskazywanie optymalizatorowi SQL preferowanych metod optymalizacji na poziomie konfiguracji parametrów pracy serwera bazy danych oraz dla wybranych zapytań. Powinna istnieć możliwość umieszczania wskazówek dla optymalizatora w wybranych instrukcjach SQL. |
|  | RDBMS musi mieć możliwość rozbudowy do wersji wspierającej możliwość synchronicznej replikacji danych w dwóch niezależnych centrach danych. |

|  |
| --- |
| PULPIT LEKARSKI – WYMAGANIA MINIMALNE |
|  | Pulpit musi umożliwiać lekarzom szybki i w pełni konfigurowalny dostęp do najważniejszych elementów pobytu szpitalnego oraz dokumentacji medycznej wielu pacjentów odwzorowując metodykę pracy użytkownika. W miejscach umożliwiających uzupełnianie danych, w których Pulpit powiela funkcje standardowego modułu ewidencji dokumentacji medycznej w obszarze lekarskim Zamawiający dopuszcza realizację wymogu wyłącznie z poziomu Pulpitu z zastrzeżeniem, że zakres powielającego się wymogu nie jest uboższy niż w module dokumentacji medycznej.  |
|  | Aplikacja musi posiadać menu górne, które zawiera, co najmniej następujące pozycje:* 1. pacjenci,
	2. lista konsultacji (wraz z szybką informacją w postaci cyfrowej informującej o liczbie konsultacji czekających na obsłużenie),
	3. lista dokumentów EDM (wraz z szybką informacją w postaci cyfrowej informującej o liczbie dokumentów oczekających na podpisanie).
 |
|  | Pozycje w menu górnym muszą reprezentować podstawowe konteksty pracy lekarza:1. Pacjenci - podczas pracy z pacjentami lekarz może oglądać i ewidencjonować dokumentację medyczną pacjenta,
2. Konsultacje - lekarz ma podgląd dokumentacji w celu wykonania konsultacji lekarskiej,
3. Dokumenty EDM - lekarz ma podgląd powstającej elektronicznej dokumentacji medycznej.
 |
|  | Po wyborze z menu górnego odpowiedniego kontekstu, aplikacja musi prezentować 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. |
|  | Obszary robocze muszą prezentować dane zorganizowane w dziedzinowe bloki danych. |
|  | Z obszarów roboczych możliwe jest przejście do ekranów szczegółowych umożliwiających podgląd i ewidencję danych dziedzinowych. |
|  | Pulpit musi wykorzystywać tzw. pływający przycisk (ang. floating button). 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. |
| Opis wymagań dotyczących kontekstu pacjentów |
|  | Po wyborze z menu górnego pozycji pacjenci, aplikacja musi prezentować wykaz pacjentów na oddziale z możliwością przełączania między trybami: pełna listy pacjentów (prezentowana na całej szerokości ekranu), skrócona listy pacjentów (prezentowana jest tylko z lewej strony ekranu). |
|  | Aplikacja musi zapewniać pełny widok listy pacjentów, prezentuje dane w zakresie co najmniej:1. nr księgi głównej,
2. nr księgi oddziałowej,
3. nazwisko,
4. imię,
5. PESEL,
6. data przyjęcia,
7. lekarz prowadzący,
8. oddział,
9. łóżko,
10. sala.
 |
|  | Aplikacja musi prezentować skrócony widok listy pacjentów prezentuje dane w zakresie co najmniej:1. imię,
2. nazwisko.
 |
|  | Moduł musi umożliwiać wyszukiwanie pacjentów na listach pacjentów minimum według następujących filtrów: 1. imię,
2. nazwisko,
3. PESEL,
4. nr księgi głównej,
5. nr księgi oddziałowej,
6. lekarz prowadzący,
7. data przyjęcia na oddział (zakres od-do),
8. data urodzenia pacjenta (zakres od-do).
 |
|  | Moduł musi posiadać możliwość sortowania pacjentów na liście minimum według następujących kryteriów:1. nr księgi oddziałowej,
2. nr księgi głównej,
3. nazwisko,
4. imię,
5. data przyjęcia.
 |
|  | Moduł musi umożliwiać grupowanie pacjentów na liście minimum według następujących kryteriów:* 1. według sali,
	2. według lekarza prowadzącego,
	3. według daty przyjęcia.
 |
|  | Skrócona lista pacjentów musi być ukrywana i ujawniana za pomocą jednego kliknięcia myszką. |
|  | Po wyborze pacjenta na liście pacjentów system musi prezentować dane i dokumentację medyczną wytypowanego pacjenta w formie obszaru roboczego, tj. panelu prezentującego zbiorczo wiele zakładek i bloków zawierających dane i dokumentację pacjenta. |
|  | W przypadku zmiany pacjenta na skróconej liście pacjentów system musi automatycznie zaktualizować dane prezentowane w obszarze roboczym i zaprezentować je w kontekście wybranego pacjenta. |
|  | Dane w obszarze roboczym muszą być prezentowane 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:* 1. podgląd zużytych leków i materiałów (Apteczka),
	2. udostępnianie danych zleconych badań diagnostycznych i ich wyników (Pracownia Diagnostyczna),
	3. udostępnianie danych zleconych badań laboratoryjnych i ich wyników (Laboratorium),
	4. udostępnianie danych zleconych badań histopatologicznych i danych o ich wykonaniu (Histopatologia),
	5. podgląd danych uzupełnianych przez pielęgniarki (Dokumentacja medyczna pielęgniarska),
	6. dostęp do danych dotyczących zabiegów operacyjnych (Blok operacyjny).
 |
| Opis wymagań dotyczących obszaru roboczego |
|  | W obszarze roboczym system musi umożliwiać prezentację danych pogrupowanych w zakładkach. |
|  | Liczba i nazwy zakładek muszą być konfigurowane przez administratora dla każdego oddziału oddzielnie w oparciu o dostępne w systemie dziedzinowe bloki danych. |
|  | Użytkownik musi mieć możliwość dowolnego konfigurowania obszaru roboczego poprzez utworzenie własnego układu zakładek i dziedzinowych bloków danych. |
|  | Użytkownik musi mieć możliwość wyboru między układem domyślnym stworzonym przez administratora, a układem stworzonym przez siebie. |
|  | Na każdej zakładce można umieścić wiele dziedzinowych bloków danych, prezentujących merytorycznie powiązaną treść minimum w zakresach:* 1. karta pacjenta,
	2. wywiad,
	3. badanie przedmiotowe,
	4. skierowania na badania diagnostyczne,
	5. wyniki badań diagnostycznych,
	6. skierowania na badania laboratoryjne,
	7. wyniki badań laboratoryjnych,
	8. skierowania na badania histopatologiczne,
	9. wyniki badań histopatologicznych,
	10. obserwacje lekarskie,
	11. konsultacje lekarskie,
	12. zabiegi operacyjne,
	13. rozpoznania,
	14. zrealizowane procedury medyczne,
	15. wypis,
	16. szczegóły pobytu,
	17. zużyte środki,
	18. lista dostępnych raportów,
	19. lista dostępnych dodatkowych formularzy w systemie HIS,
	20. lista dostępnych do wglądu zakresów informacji w dokumentacji pielęgniarskiej.
 |
|  | Każdy z bloków danych musi być wykorzystywany w minimum 2 różnych rozmiarach z dostępnych poniżej:* 1. 1/2 ekranu,
	2. 1/4 ekranu,
	3. 1/8 ekranu,
	4. 1/16 ekranu.
 |
|  | Dane w każdym bloku muszą być ładowane niezależnie od pozostałych. Ładowanie danych w bloku nie blokuje pozostałych elementów systemu. |
|  | System musi umożliwiać filtrowanie danych wyświetlanych w dziedzinowych blokach danych na podstawie zakresów:* 1. pobyt oddziałowy,
	2. hospitalizacja,
	3. dane przyjęciowe,
	4. wszystkie dostępne dane pacjenta.
 |
|  | System musi umożliwiać filtrowanie danych na podstawie zakresów, w co najmniej poniższych dziedzinowych blokach danych:* 1. badanie przedmiotowe,
	2. obserwacje lekarskie,
	3. skierowania na badania diagnostyczne,
	4. wyniki badań diagnostycznych,
	5. skierowania na badania laboratoryjne,
	6. wyniki badań laboratoryjnych,
	7. skierowania na badania histopatologiczne,
	8. wyniki badań histopatologicznych,
	9. konsultacje lekarskie,
	10. zabiegi operacyjne,
	11. rozpoznania,
	12. zrealizowane procedury medyczne,
	13. zużyte środki.
 |
|  | 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 musi umożliwiać filtrowanie według wybranego przez użytkownika:* 1. rodzaju zdarzeń medycznych (np. skierowania, wyniki, obserwacje),
	2. czasu wystąpienia zdarzenia,
	3. zakresu danych.
 |
|  | Wybór bloku dziedzinowego (lub zdarzenia medycznego z osi czasu) musi powodować wywołanie odpowiedniego widoku prezentującego dane szczegółowe poszczególnych obszarów merytorycznych. |
| Opis wymagań dotyczących ekranów szczegółowych |
|  | Ekrany szczegółowe muszą być uruchamiane z poziomu obszaru roboczego lub poprzez tzw. pływający przycisk (ang. floating button). 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 musi umożliwiać ewidencję danych co najmniej w ekranach szczegółowych:* 1. wywiad,
	2. badania przedmiotowe,
	3. skierowania na badania diagnostyczne,
	4. skierowania na badania laboratoryjne,
	5. skierowania na badania histopatologiczne,
	6. obserwacje lekarskie,
	7. konsultacje lekarskie,
	8. zabiegi operacyjne,
	9. rozpoznania,
	10. wypis.
 |
|  | W ekranach szczegółowych aplikacja musi umożliwiać podzielenie ekranu w celu jednoczesnego wprowadzania danych i wyświetlaniem danych z innej dziedziny (w zakresach dostępnych ekranów szczegółowych). Przykładowym oczekiwanym efektem są np.:1. system umożliwia jednoczesne wprowadzanie danych dotyczących zlecenia medycznego i wyświetlanie poprzednich wyników pacjenta,
2. system umożliwia jednoczesne wprowadzenie danych dotyczących konsultacji i wyświetlanie danych dotyczących wywiadu.
 |
|  | Moduł musi dysponować dodatkowym menu bocznym, umożliwiającym szybkie przełączanie pomiędzy ekranami szczegółowymi, bez konieczności powrotu do obszaru roboczego. Ekrany szczegółowe prezentują dane minimum w poniższych zakresach, w przypadku, gdy dane istnieją w HIS:* 1. karta pacjenta,
	2. wywiad,
	3. badanie przedmiotowe,
	4. obserwacje lekarskie,
	5. historia pobytów pacjenta,
	6. skierowania na badania diagnostyczne,
	7. wyniki badań diagnostycznych,
	8. skierowania na badania laboratoryjne,
	9. wyniki badań laboratoryjnych,
	10. skierowania na badania histopatologiczne,
	11. wyniki badań histopatologicznych,
	12. konsultacje lekarskie,
	13. zabiegi operacyjne,
	14. rozpoznania,
	15. zrealizowane procedury medyczne,
	16. zużyte środki,
	17. wypis,
	18. dieta pacjenta,
 |
| Opis wymagań dotyczących pływającego przycisku |
|  | Użytkownik musi mieć możliwość z każdego miejsca pracy w systemie łatwego przejścia do akcji dostępnych w systemie poprzez kliknięcie pływającego przycisku (ang. floating button). |
|  | Na dostępne akcje muszą składać się:* 1. przejścia do ekranów szczegółowych, (co najmniej do karty pacjenta, wywiadu i wypisu),
	2. polecenia ewidencji nowych danych (co najmniej skierowania na badania diagnostyczne / laboratoryjne / histopatologiczne, obserwacje lekarskie, konsultacje lekarskie, zabiegi operacyjne, badania przedmiotowe, rozpoznania),
	3. dodatkowe akcje skojarzone z odpowiednimi dziedzinowymi blokami (co najmniej w zakresie uzupełniania badań przedmiotowych).
 |
|  | Dostępne akcje wyświetlane po kliknięciu pływającego przycisku muszą być podzielone na trzy zbiory:* 1. wszystkie dostępne akcje,
	2. najczęściej wykorzystywane przez użytkownika akcje,
	3. akcje powiązane z bieżącym ekranem.
 |
|  | W ramach listy najczęściej używanych akcji, wyświetlanej poprzez kliknięcie na pływający przycisk, użytkownik musi mieć możliwość wyszukania interesującej go akcji po jej nazwie. |
| Opis wymagań dotyczących komunikatora |
|  | Użytkownik musi mieć dostęp do powiadomień generowanych przez wewnętrzny system komunikacji. |
|  | Obsługa powiadomień nie może blokować bieżącej pracy użytkownika za wyjątkiem powiadomień wymuszających taką blokadę. |
|  | System musi informować użytkownika o liczbie nieprzeczytanych powiadomień. |
|  | Z poziomu pulpitu lekarskiego system musi umożliwiać obsługę powiadomień:1. systemowych (np. informacja o pojawieniu się wyniku do zleconego badania, informacja o konieczności udzielenia konsultacji),
2. przysłanych przez administratora (np. informacja o aktualizacji sytemu HIS),
3. przysłanych przez innych użytkowników (np. w postaci wewnętrznego komunikatora).
 |
| Opis wymagań dotyczących kontekstu dokumentów |
|  | Po wyborze z menu górnego pozycji Dokumenty EDM, aplikacja musi prezentować 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 musi umożliwiać wyszukiwanie dokumentów EDM po nazwie. |
|  | Możliwość ograniczania listy dokumentów według zakresów: * 1. wszystkie dokumenty użytkownika w oddziale,
	2. wszystkie dokumenty w oddziale,
	3. wszystkie dokumenty użytkownika.
 |
|  | Moduł musi umożliwiać filtrowanie dokumentów. Dostępne filtry:* 1. podpisany,
	2. do podpisu,
	3. bez podpisu,
	4. aktualne.
 |
|  | Dla każdego dokumentu EDM moduł musi prezentować:1. dane o autorze dokumentu,
2. czy dokument jest podpisany,
3. dane pracownika, który podpisał dokument,
4. cel podpisu,
5. datę podpisu,
6. podgląd dokumentu.
 |
|  | Aplikacja musi umożliwiać wydruk dokumentu EDM. |
| Opis rozbudowanych wymagań dotyczących ekranów szczegółowych w zintegrowanym pulpicie lekarskim |
|  | **Karta pacjenta i szczegóły pobytu** |
|  | Moduł musi umożliwiać podgląd karty pacjenta. |
|  | Moduł musi umożliwiać podgląd danych dotyczących pobytu pacjenta na oddziale. |
|  | **Obserwacje lekarskie** |
|  | Użytkownik musi posiadać możliwość przeglądania obserwacji lekarskich wybranego pacjenta.  |
|  | W ramach przeglądania obserwacji możliwe jest wykorzystanie z predefiniowanych filtrów:1. pokaż wpisy z bieżącego pobytu oddziałowego,
2. pokaż wpisy z bieżącej hospitalizacji.
 |
|  | System musi umożliwiać wprowadzenie informacji o obserwacjach lekarskich. |
|  | Możliwość wykorzystania klasyfikacji i szablonów dla obserwacji lekarskich. |
|  | Możliwość generowania obserwacji lekarskich na podstawie udzielonych konsultacji. |
|  | Możliwość pobierania wyników diagnostycznych oraz laboratoryjnych z danego dnia do obserwacji lekarskich. |
|  | **Konsultacje lekarskie** |
|  | Użytkownik musi posiadać możliwość przeglądania konsultacji lekarskich wybranego pacjenta. |
|  | Na liście konsultacji system musi prezentować dla każdej konsultacji jej status oraz pilność. |
|  | Moduł musi umożliwiać wysłanie prośby o konsultację do danej jednostki z wskazaniem lekarza konsultującego lub bez wskazania lekarza. |
|  | Możliwość oznaczenia konsultacji jako pilnej. |
|  | Moduł musi umożliwiać przyjęcie konsultacji do opisu.  |
|  | **Badania przedmiotowe** |
|  | Użytkownik musi posiadać możliwość przeglądania badań przedmiotowych wybranego pacjenta w postaci listy. |
|  | Możliwość ewidencji danych dotyczących badań przedmiotowych. |
|  | Możliwość oznaczenia badania przedmiotowego, aby zostało ujęte na wypisie. |
|  | Możliwość skopiowania poprzedniego wyniku badania do bieżącego z możliwością jego edycji po skopiowaniu. |
|  | **Rozpoznania** |
|  | Użytkownik systemu musi posiadać możliwość przeglądania rozpoznań wybranego pacjenta w postaci listy:1. z aktualnego pobytu,
2. z poprzednich pobytów.
 |
|  | Użytkownik musi mieć możliwość dodawania informacji dotyczących:1. rozpoznań pacjenta,
2. karty zgłoszenia choroby zakaźnej,
3. karty nowotworowej,
4. rozpoznań dodatkowych VY i \*\*.
 |
|  | Możliwość ewidencji rozpoznań pacjenta. |
|  | Możliwość oznaczenia rozpoznania jako kontynuacja leczenia. |
|  | **Zrealizowane procedury medyczne** |
|  | Użytkownik systemu musi mieć możliwość przeglądania ewidencji zrealizowanych procedur ICD-9 PL. |
|  | Możliwość filtrowania listy procedur medycznych według minimum: * 1. dat realizacji procedur,
	2. pokaż wszystkie,
	3. pokaż procedury ICD-9 PL.
 |
|  | Możliwość wyszukiwania na liście procedur według symbolu czy nazwy procedury. |
|  | **Wywiad** |
|  | Moduł musi umożliwiać prezentację danych dotyczących zebranego wywiadu pacjenta. |
|  | Moduł musi umożliwiać prezentację danych o stosowanych lekach i alergiach. |
|  | Moduł musi umożliwiać prezentację danych o przebytych chorobach pacjenta i chorobach w jego rodzinie. |
|  | Moduł musi umożliwiać prezentację danych ginekologicznych dla pacjentek. |
|  | Moduł musi umożliwiać kopiowanie danych z poprzedniego wywiadu lub z innego dowolnego wcześniejszego wywiadu pacjenta. |
|  | Moduł musi umożliwiać edycję danych wywiadu lekarskiego. |
|  | **Zużyte środki** |
|  | Moduł musi umożliwiać przeglądanie listy zużytych środków na pacjenta oraz podgląd danych szczegółowych. |
|  | **Skierowania na badania** |
|  | Moduł musi prezentować listę zleconych badań wraz z informacją o statusie skierowania i jego pilności. |
|  | Dla każdego skierowania system musi prezentować dane szczegółowe. |
|  | Użytkownik musi mieć możliwość powtórzenia danego skierowania lub skopiowania badań z poprzedniego skierowania. |
|  | W ramach skierowania laboratoryjnego i diagnostycznego moduł musi umożliwiać przetwarzanie danych dot. rozpoznań i informacji dodatkowych. |
|  | **Wyniki zleconych badań** |
|  | Moduł musi prezentować listę wyników do zleconych badań. |
|  | Dla każdego wyniku badań system musi prezentować dane szczegółowe wyniku. |
|  | **Zabiegi operacyjne** |
|  | Moduł musi prezentować listę zleconych oraz wykonanych zabiegów chirurgicznych. |
|  | Moduł musi umożliwiać dodanie nowego skierowania na zabieg. |
|  | **Wypis** |
|  | Moduł musi umożliwiać prezentację danych dotyczących wypisu pacjenta. |
|  | Możliwość automatycznego pobierania danych do pozycji wypisu na karcie informacyjnej w oparciu o zgromadzone dane o leczeniu (np. wyniki laboratoryjne, diagnostyczne, rozpoznania, procedury).  |
|  | Możliwość definiowania przez administratora szablonów dla poszczególnych pozycji zawartych w karcie informacyjnej. |
|  | Możliwość korzystania przez użytkownika z szablonów dla poszczególnych pozycji zawartych w karcie informacyjnej. |
|  | Możliwość pobrania do karty informacyjnej wpisów z poprzedniego lub wybranego pobytu.  |
|  | **Raporty** |
|  | Moduł musi prezentować listę dostępnych raportów dla danego użytkownika. |
|  | Użytkownik musi mieć możliwość przeszukiwania listy raportów według nazwy raportu. |
|  | Dla każdego raportu użytkownik musi mieć możliwość:1. wprowadzenia liczby kopii do wydrukowania zaznaczonego raportu,
2. możliwość wyboru przeznaczenia wybranego raportu, czy wydruk ma zostać zaprezentowany na ekranie, czy od razu wydrukowany za pomocą drukarki.
 |
|  | **Podgląd dokumentacji pielęgniarskiej** |
|  | Moduł prezentuje listę dostępnych formularzy dot. dokumentacji pielęgniarskiej. |
|  | Użytkownik systemu musi mieć możliwość przeglądania dokumentacji pielęgniarskiej w minimum w poniższym zakresie, jeżeli dane występują w HIS: * 1. karty parametrów życiowych,
	2. realizacji opieki,
	3. karty indywidualnej opieki,
	4. karty gorączkowej,
	5. profilaktyki odleżyn,
	6. pielęgnacji odleżyn,
	7. gospodarki wodnej,
	8. ewidencji wkłuć,
	9. kategorii pielęgniarskich.
 |

|  |
| --- |
| PORTAL PACJENTA – WYMAGANIA MINIMALNE |
| Bezpieczeństwo |
|  | Portal obsługuje dostarczony przez Zamawiającego certyfikat SSL. Wymagany jest certyfikat typu wildcard. |
|  | Portal umożliwia nadanie odpowiedniej nazwy domenowej uzgodnionej z Zamawiającym. W dostarczonym certyfikacie nazwa domenowa będzie umieszczona w certyfikacie (pole Common Name) i musi być zgodna z adresem wpisywanym w przeglądarce. |
|  | Portal zapewnia bezpieczną, zaszyfrowaną komunikację przez sieć między stacją kliencką, a serwerem. |
|  | Zamawiający utworzy adres poczty elektronicznej (e-mail) do powiadomień przekazywanych z portalu. |
|  | Portal pacjenta będzie zainstalowany na dedykowanej do tego celu maszynie. |
|  | E-usługi dostępne w ramach Portalu Pacjenta to zestaw funkcji, które umożliwiają interakcję z użytkownikiem (szczególnie pacjentem i lekarzem) metodą zdalną, między innymi za pośrednictwem Internetu, w tym niektóre są zabezpieczone dodatkowymi kanałami szyfrowanej komunikacji jak HTTPS. Moduły są zintegrowane z częścią białą systemu, tj. HIS/RIS/PACS. |
|  | E-usługi dla pacjentów opublikowane w Internecie łączą się z modułami systemu HIS poprzez dodatkowy zabezpieczony interfejs komunikacji w celu podniesienia bezpieczeństwa bazy danych osobowych i wrażliwych danych medycznych przetwarzanych w systemie HIS/RIS/PACS. |
|  | E-usługi dostępne w Internecie dla pacjentów do komunikacji z częścią systemu w intranecie placówki (system HIS/RIS/PACS) wykorzystują zabezpieczony kanał komunikacji. |
| Graficzny interfejs użytkownika |
|  | Interfejs użytkownika jest zgodny z WCAG 2.1 (ang. Web Content Accessibility Guidelines), na poziomie co najmniej AA. |
|  | Portal udostępnia graficzny interfejs użytkownika, zaprojektowany w technice RWD (Responsive Web Design), dostosowujący się do wielkości ekranu urządzenia, na którym jest użytkowany.  |
|  | W Portalu Pacjenta jest możliwe użytkowanie systemu w przeglądarkach smartphonów, tabletów i komputerów osobistych. |
|  | Portal udostępnia interfejs użytkownika w języku polskim. |
| Architektura rozwiązania eUsług |
|  | Portal posiada modułową budowę. |
|  | Portal udostępnia interfejs programowy (API) umożliwiający jego ewentualną integrację z innym oprogramowaniem działającym obecnie lub w przyszłości w Szpitalu. |
|  | Możliwe jest użytkowanie portalu na najnowszych wersjach popularnych przeglądarek internetowych, minimum: Google Chrome, Firefox, Microsoft Edge bez konieczności instalacji dodatkowych elementów środowiska uruchomieniowego. |
| W ramach realizacji przedmiotu zamówienia muszą zostać wdrożenie eUsługi: |
|  | Portal pacjenta, którego zadaniem będzie zapewnienie prostszej i szybszej komunikacji pacjenta z placówką medyczną bez konieczności fizycznego pojawiania się pacjenta w placówce medycznej o ile stan zdrowia pacjenta pozwala na taki kontakt i nie wymaga osobistego stawiennictwa u lekarza. Portal pacjenta będzie dostępny zarówno z komputerów, notebooków jak również urządzeń mobilnych takich jak tablet i smartfon. Portal będzie zrealizowany przynajmniej jako strona responsywna umożliwiając swobodną prace na każdym z wymienionych urządzeń. Konto w portalu pacjent będzie mógł utworzyć samodzielnie lub poprosić o wsparcie personel placówki medycznej.  |
|  | ePowiadomienia – ePortal, który będzie realizować różne mechanizmy powiadomień email/sms pacjenta o zdarzeniach w portalu (informacja o umówieniu na wizytę, przypomnienie o zbliżającej się wizycie, informacje o zmianach terminu wizyt, informacja o pojawieniu się wyniku badania, informacja o pojawieniu się nowego dokumentu z procesu leczenia, przypomnienie o uzupełnieniu dzienniczka, o przyjęciu zleconych leków, Pacjent w ramach konfiguracji własnego profilu będzie posiadać możliwość określania zdarzeń, o których będzie informowany oraz sposobu informowania email/sms. Dla zdarzeń typu przypomnienie o wizycie może zostać wysłany SMS z zapytaniem czy planuje się stawić na wizytę i w przypadku braku odpowiedzi wizyta może zostać anulowana zwalniając miejsce w harmonogramie dla innych pacjentów.  |
|  | EDM – ePortal, który będzie udostępniać potwierdzonemu użytkownikowi wgląd w dokumentację medyczną, która została wytworzona w placówce medycznej i która została oznaczona jako widoczna dla pacjenta w ePortalu. Dla dokumentów zgromadzonych w archiwum lokalnym eUsług, a które nie podlegają indeksacji w P1 pacjent powinien posiadać możliwość ich świadomego udostępniania innym lekarzom (np. dokumenty z poradni urologicznej umawiając się na wizytę/konsultację/telekonsultację u chirurga). Ponadto dla dokumentacji medycznej zgromadzonej w archiwum portalu lokalnego pacjent będzie posiadać możliwość jej udostępnienia dowolnemu innemu lekarzowi (posiadającemu konto w systemie) . Wskazany lekarz uzyska wgląd w udostępnione dokumenty. Lekarz placówki medycznej będzie posiadać domyślnie wgląd w dokumenty pacjenta, które zostały wytworzone w ramach jednostki organizacyjnej, w której jest zatrudniony i obsługuje zdarzenia medyczne pacjenta. Do pozostałych dokumentów uzyska dostęp po ich udostępnieniu przez pacjenta w portalu. |
|  | eDzienniczek pacjenta - lekarz w ramach procesu leczenia będzie mieć możliwość określenia listy parametrów, które pacjent powinien monitorować przez zadany okres czasu np. w domu pomiędzy wizytami. Badane parametry mogą być liczbowe jak również subiektywne opisowe np. pytanie o samopoczucie. Dla badań liczbowych mogą zostać przypisane indywidualne parametry krytyczne po przekroczeniu których system umożliwi wprowadzenie przez personel medycznych zaleceń dla pacjenta lub zainicjuje wykonanie odpowiednich akcji automatycznych kończąc na wysłaniu informacji o konieczności konsultacji z lekarzem.  |
|  | Telekonsultacje/konsultacje będą posiadały możliwość zlecania i przeprowadzania konsultacji przypadku medycznego. Będzie mogła się ona odbyć w formie telekonsultacji lub pytania do lekarza. Telekonsultacja będzie mogła być również realizowana jako konsultacja pacjent-lekarz lub pomiędzy kilkoma specjalistami. Do zlecanej konsultacji będzie istniała możliwość załączenia zdarzeń medycznych i dokumentacji zgromadzonej w portalu w tym również dokumentacji, która nie podlega indeksacji w P1 oraz dokumentacji załączonej do archiwum eUsług przez pacjenta. W przypadku telekonsultacji będzie istniała możliwość realizacji połączenia audiowizualnego, którego przebieg będzie może zostać w pełni zarejestrować i zapisany w archiwum eUsług. |
|  | Biuro podawcze w celu ograniczenia konieczności przybycia pacjenta do placówki medycznej zwłaszcza w obecnej sytuacji epidemiologicznej będzie istniała możliwość wprowadzenia w systemie biura podawczego np. z prośbą o udostępnienie dokumentacji pacjenta. Placówka medyczna będzie mogła zdigitalizować żądaną dokumentację medyczną i udostępnić ją pacjentowi w ramach lokalnego archiwum eUsług.  |

1. Wymagania dotyczące wdrożenia modułów licencji
2. W ramach usług wdrożeniowych wchodzić będzie w szczególności:
3. Instalacja, konfiguracja oraz parametryzacja dostarczanych wyżej opisanych modułów medycznego oprogramowania aplikacyjnego na serwerze oraz na stacjach roboczych w miejscach wskazanych przez Zamawiającego,
4. Integracja dostarczanego systemu z systemami posiadanymi przez Zamawiającego.
5. Zamawiający wymaga by moduły oprogramowania medycznego wdrożone przez Wykonawcę w ramach realizacji przedmiotu zamówienia były wdrożone w pełnej ich funkcjonalności opisanej w powyżej funkcjonalności.
6. Instalacja i wdrożenie winny odbywać się w godzinach pracy pracowników Zamawiającego tj. w dni robocze, w godz. 7.30-14:30. Zamawiający dopuszcza wykonywanie prac w innym czasie niż wskazany, po odpowiednim uzgodnieniu i jego akceptacji.
7. Po dokonaniu instalacji i wdrożenia modułów systemu medycznego, docelowo system medyczny powinien:
8. spełniać wymagania określone niniejszym dokumentem,
9. spełniać wymagania obowiązujących przepisów prawa i uwzględniać charakter prowadzonej przez Zamawiającego działalności.
10. Po zakończeniu realizacji przedmiotu zamówienia oraz po stwierdzeniu poprawności funkcjonowania wdrożonych modułów zintegrowanych z systemem medycznym działającym u Zamawiającego, podpisany zostanie przez Zamawiającego i Wykonawcę Końcowy Protokół Odbioru – bezusterkowy.
11. Po zakończeniu realizacji przedmiotu zamówienia Wykonawca wykona i przekaże Zamawiającemu dokumentację powykonawczą dla administratorów zawierającą dokładny opis funkcjonalny dostarczanych modułów systemu medycznego.
12. Zamawiający wymaga by docelowo wdrożone moduły systemu medycznego były zintegrowane z systemem medycznym, z którego korzysta Zamawiający, korzystały z jednorodnej bazy danych - ze względu na konieczność zapewnienia jednolicie wysokiego bezpieczeństwa gromadzonych wrażliwych danych medycznych oraz ich spójności.
13. Zamawiający wymaga by docelowo wdrożone moduły systemu medycznego zintegrowane z systemem medycznym, z którego korzystał dotychczas Zamawiający spełniały następujące warunki:
14. zapewnienie jednolitego sposobu wprowadzania danych za pomocą jednego interfejsu,
15. zapewnienie pełnego wykorzystania i dostępu do danych zgromadzonych w obecnie funkcjonującym u Zamawiającego systemie medycznym,
16. zachowanie ciągłości obecnie stosowanej przez Zamawiającego numeracji dokumentacji medycznej,
17. zapewnienie jednego modułu/ aplikacji systemu medycznego do prowadzenia sprawozdawczości i rozliczeń z NFZ,
18. zapewnienie możliwości wykonywania archiwalnych statystyk i raportów,
19. muszą być wyposażone w zabezpieczenia przed nieautoryzowanym dostępem. Wszystkie moduły systemu medycznego muszą korzystać z baz danych zapewniających odpowiedni poziom bezpieczeństwa gromadzonych danych zgodnie z wymogami prawa. Zabezpieczenia muszą funkcjonować na poziomie Klienta (aplikacja) i Serwera (serwer baz danych);
20. muszą pozwalać na wykonywanie kopii zapasowych struktur danych w trakcie ich pracy;
21. muszą posiadać sprawny mechanizm archiwizacji danych i mechanizmy gwarantujące spójność danych. Wymagane jest wzajemne współdziałanie modułów systemu medycznego poprzez powiązania logiczne i korzystanie ze wspólnych danych przechowywanych na serwerach;
22. muszą współpracować z aplikacjami typu MS Word, MS Excel w zakresie eksportu danych;
23. muszą zapewniać aktualizację informacji w bazach danych podczas rutynowych czynności wykonywanych na stanowiskach pracy;
24. winny być w języku polskim i komunikować się z użytkownikiem w języku polskim, udostępniając mu możliwość korzystania z rozbudowanych podpowiedzi;
25. winny posiadać dokumentację w języku polskim – instrukcję obsługi każdego dostarczanego modułu systemu medycznego dla użytkownika (w wersji elektronicznej) pozwalającą na samodzielną naukę obsługi każdego modułu. Wykonawca dostarczy do wszystkich komórek organizacyjnych Zamawiającego ww. dokumentację w wersji elektronicznej w języku polskim.
26. Zamawiający wymaga, aby moduł/y był/y zainstalowany/wdrożony/zintegrowany w ramach istniejącej instalacji Szpitalnego Systemu Medycznego z uwzględnieniem posiadanej konfiguracji, oraz zapewni ciągłość pracy systemów.
27. Oprogramowanie powinno posiadać interfejs w języku polskim.
28. Wymagane jest, aby uruchomienie zakończyło się szkoleniem z zakresu obsługi dla Użytkownika.
29. Wykonawca musi być producentem lub posiadać aktualną autoryzację producenta oprogramowania uprawniającą do świadczenia usług wdrożeniowych oraz serwisowych
30. Dostawa, instalacja, konfiguracja i wdrożenie Oprogramowania aplikacyjnego
31. Zadanie dostawy, instalacji, konfiguracji i wdrożenia Oprogramowania aplikacyjnego obejmuje dostarczany w ramach realizacji zamówienia system HIS
32. Dostawa i instalacja mają być wykonana w lokalizacji Zamawiającego.
33. Po zakończeniu prac instalacyjnych Oprogramowanie musi zostać skonfigurowane i wdrożone w sposób tzw. „pod klucz” oraz tak, aby oferowało funkcjonalności opisane w SWZ oraz zgodnie z Dokumentacją.
34. Oprogramowanie aplikacyjne musi zostać zainstalowane przez Wykonawcę w szczególności z wykorzystaniem Sprzętu i w środowiskach informatycznych Zamawiającego. Oprogramowanie aplikacyjne musi zostać zainstalowane i skonfigurowane w sposób tzw. „pod klucz” na wszystkich wskazanych stanowiskach komputerowych Podmiotu Leczniczego.
35. Oprogramowanie aplikacyjne musi zostać zainstalowane w taki sposób aby zachować w całości dotychczasowe integracje z oprogramowaniem posiadanym przez Szpital w szczególności obejmujące zakres integracji, interfejsy integracji oraz model wymiany danych.
36. Instruktaże stanowiskowe
37. Wykonawca zaplanuje w uzgodnieniu z Przedstawicielem Zamawiającego Instruktaże stanowiskowe. Instruktaże stanowiskowe zostaną przeprowadzone w miejscach instalacji Oprogramowania z zakresu obsługi, administracji i utrzymania.
38. Instruktaże stanowiskowe będą prowadzone w języku polskim i obejmą w szczególności:
39. pomoc użytkownikom w korzystaniu z Oprogramowania w miejscu instalacji,
40. pomoc w administracji i konfiguracji Systemu,
41. wykonywanie dodatkowych prac konfiguracyjnych,
42. konsultacje.
43. Instruktaże stanowiskowe będą prowadzone w dwóch kategoriach:
44. dla użytkowników Oprogramowania aplikacyjnego,
45. dla administratorów technicznych - wyznaczonych spośród pracowników Zamawiających, obejmujących zakres konfiguracji i użytkowania HIS oraz nadzoru nad użytkownikami oraz wydawania uprawnień (poświadczeń/certyfikatów),
46. Wykonawca winien w ramach oferty uwzględnić poniższą ilość godzin szkoleniowych:
47. Dla użytkowników oprogramowania aplikacyjnego, szacowana liczba godzin szkoleniowych dla wszystkich dostarczanych modułów/systemów: do 100 godz.
48. dla administratorów technicznych szacowana liczba godzin szkoleniowych dla wszystkich dostarczanych modułów/systemów: do 50 godz.
49. Wykonawca wykona i uzgodni z Zamawiającymi plan instruktaży stanowiskowych w etapie wykonania Dokumentacji Analizy Przedwdrożeniowej.
50. Po ukończeniu instruktaży stanowiskowych uczestnicy mają w szczególności umieć posługiwać się Oprogramowaniem i jego modułami odpowiednio do swojej roli, a także znać i rozumieć ich funkcjonowanie w Systemie.
51. Administratorzy techniczni po zakończeniu instruktaży muszą w szczególności umieć wykonywać czynności administracji, a także instalacji Oprogramowania aplikacyjnego, 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 dostarczone Oprogramowanie, jak również znać jego wdrożoną konfigurację.
52. W przypadku potrzeby Zamawiający zapewni we własnym zakresie pomieszczenia dla przeprowadzenia Instruktaży stanowiskowych. Wykonawca może realizować Instruktaże stanowiskowe również na stanowiskach pracy pracowników oraz zdalnie przy użyciu środków komunikacji typu Skype itp.
53. Testy
54. W ramach tego zadania zostaną przeprowadzone wszystkie testy opisane w Dokumentacji. Celem testów jest weryfikacja przez Zamawiającego, czy wszystkie prace wykonane w trakcie realizacji Przedmiotu Zamówienia zostały wykonane prawidłowo i zgodnie z założeniami funkcjonalnymi i jakościowymi. Testy będą przeprowadzane przez Wykonawcę przy współudziale Zamawiającego jak i wskazanych przez Zamawiającego osób.
55. Pozytywne zakończenie testów wraz z ewentualnym usunięciem wskazanych Błędów Aplikacji jest niezbędne, aby dla poszczególnych Komponentów oraz całego Przedmiotu Zamówienia dokonać odbiorów w ramach Odbioru Końcowego.
56. Dodatkowe zobowiązania Wykonawcy
57. Oferowane rozwiązanie ma być rozwiązaniem działającym, gotowym do wdrożenia i zapewniającym realizację wszystkich wymaganych w SWZ i OPZ funkcjonalności na dzień składania ofert. Rozwiązanie nie może być w fazie budowy, testów, projektowania itp.
58. Wykonanie Przedmiotu Zamówienia z efektywnością oraz zgodnie z praktyką i wiedzą zawodową.
59. Wykonanie w całości Przedmiotu Zamówienia w zakresie określonym w Umowie i SWZ.
60. Dokonanie z Zamawiającym wszelkich koniecznych ustaleń mogących wpływać na zakres i sposób realizacji Przedmiotu Zamówienia oraz ciągła współpraca z Zamawiającym na każdym etapie realizacji.
61. Stosowanie się do wytycznych i polityk bezpieczeństwa informacji u Zamawiającego.
62. Udzielanie na każde żądanie Zamawiającego pełnej informacji na temat stanu realizacji Przedmiotu Zamówienia.
63. Współdziałanie z osobami wskazanymi przez Zamawiającego.
64. Oprogramowanie aplikacyjne – Wymagania ogólne
65. Wykonawca zobowiązuje się dostarczyć Zamawiającemu określone funkcjonalności systemu SSI, poprzez dostawę nowego rozwiązania lub zmodernizowanie i rozbudowanie istniejącego w taki sposób, aby w jak najszerszym zakresie zostały zaspokojone obecne i przyszłe potrzeby Zamawiającego. Koniecznym jest równoczesne zachowanie pełnej wzajemnej interoperacyjności nowo wdrażanych modułów/grup funkcjonalności, a także w przypadku rozbudowy, pełnej interoperacyjności z modułami/grupami funkcjonalności już funkcjonującymi u Zamawiającego.
66. Wykonawca oświadcza, że dostarczone Oprogramowanie po jego konfiguracji w obszarze serwerowym (logicznymi fizycznym) jest wystarczające do realizacji Umowy i osiągnięcia parametrów eksploatacyjnych opisanych przez Zamawiającego w Umowie.
67. Dane zaimportowane do SSI z aktualnie użytkowanego oprogramowania muszą być spójne z nowo wprowadzanymi, edytowalne, podlegające analizie i spełniające warunki walidacji dla określonych typów pól.
68. Zamawiający wymaga także, aby wszystkie posiadane lub dostarczane systemy zewnętrzne integrowały się z rozbudowywanym systemem informatycznym. Pełną odpowiedzialność za integracje z systemami zewnętrznymi ponosi Wykonawca.
69. Wykonawca w przypadku rozbudowy SSI obecnie użytkowanego przez Zamawiającego zobowiązany jest zapewnić wzajemną integrację wszystkich dostarczanych modułów SSI, oraz systemów, w zakresie funkcjonalnie nie mniejszym niż obecnie istniejący.
70. Szczegółowy zakres wymaganych funkcjonalności systemu, został opisany powyżej.
71. Warunki usług serwisowych i nadzoru autorskiego

Wykonawca ma obowiązek świadczyć usługi nadzoru autorskiego i serwisu dla dostarczonego SSI przez okres zadeklarowany w ofercie.

W ramach usług obsługi serwisowej wraz z nadzorem autorskim oraz asystą techniczną Wykonawca jest zobowiązany zapewnić:

1. Nieodpłatne udostępnienie i wdrożenie poprawek (Łat) do Szpitalnego Systemu Informatycznego, w przypadku stwierdzenia przez Zamawiającego błędu aplikacji:
2. w przypadku wystąpienia tzw. Awarii (błędu krytycznego), tj. sytuacji która uniemożliwia użytkowanie Zintegrowanego Systemu Informatycznego w zakresie jego podstawowej funkcjonalności wskazanej w dokumentacji użytkownika:
* czas reakcji Wykonawcy na zgłoszenie Zamawiającego, (tj. czas od momentu potwierdzenia przyjęcia zgłoszenia i podjęcie przez Wykonawcę kontaktu z przedstawicielem Zamawiającego. W jego następstwie dokonywana jest weryfikacja zgłoszonego problemu oraz ustalenie dalszego sposobu postępowania w celu rozwiązania problemu - ustalenie terminu wizyty serwisu - jeśli konieczna), wynosi do 12 godzin;
* czas naprawy SSI, (tj. czas od momentu potwierdzenia przyjęcia zgłoszenia, do momentu przystąpienia przez Wykonawcę do usuwania nieprawidłowości, aż po ich usunięcie i przywrócenie Systemu do stanu sprzed zgłoszenia ), wyniesie do 56 godzin;
* przypadku dalsza obsługa usunięcia dotychczasowego błędu krytycznego będzie traktowana jako błąd zwykły;
1. w pozostałych przypadkach:
* czas reakcji Wykonawcy na zgłoszenie Zamawiającego (tj. czas od momentu potwierdzenia przyjęcia zgłoszenia i podjęcie przez Wykonawcę kontaktu z przedstawicielem Zamawiającego. W jego następstwie dokonywana jest weryfikacja zgłoszonego problemu oraz ustalenie dalszego sposobu postępowania w celu rozwiązania problemu - ustalenie terminu wizyty serwisu - jeśli konieczna) wynosi do 24 godzin;
* czas naprawy SSI, (tj. czas od momentu potwierdzenia przyjęcia zgłoszenia, do momentu przystąpienia przez Wykonawcę do usuwania nieprawidłowości, aż po ich usunięcie i przywrócenie Systemu do stanu sprzed zgłoszenia), wyniesie do 7 dni roboczych;
1. ewentualne przekwalifikowanie błędu zgłoszonego przez Zamawiającego jako zwykły, na Awarię, wymagać będzie osobnego zgłoszenia i oznaczać będzie uruchomienie procedury opisanej w pkt. a).
2. zgłoszenie błędów (w tym Awarii) przez Zamawiającego odbywać się będzie poprzez serwisową witrynę internetową – Elektroniczny System Zgłoszeń, lub dedykowany portal Wykonawcy. W razie trudności z rejestracją zgłoszenia w w/w aplikacji, Zamawiający może dokonać zgłoszenia telefonicznie pod wskazany przez Wykonawcę numer telefonu lub za pomocą poczty elektronicznej na wskazany adres e-mail. W przypadku, gdy formularz zgłoszenia błędu zostanie przyjęty przez Wykonawcę:
* w godzinach pomiędzy 16.00 a 24.00 dnia roboczego – traktowany jest jak przyjęty o godz. 8.00 następnego dnia roboczego;
* w godzinach pomiędzy 0.00 a 8.00 dnia roboczego - traktowany jest jak przyjęty o godz. 8.00 danego dnia roboczego;
* w dniu ustawowo lub dodatkowo wolnym od pracy - traktowany jest jak przyjęty o godz. 8.00 najbliższego dnia roboczego;
* wyjątkiem od reguł opisanych w punktach a) - c), będą formularze zgłoszenia Awarii (błędu krytycznego), które traktowane będą jako przyjęcia bez obwarowań czasowych i realizowane będą jak najpilniej.
1. Nieodpłatne wprowadzanie zmian w Szpitalnym Systemie Informatycznym objętym niniejszą Umową, w zakresie wymaganym zmianami powszechnie obowiązujących przepisów prawa lub przepisów prawa wewnętrznie obowiązujących, wydanych na podstawie delegacji ustawowej, z zastrzeżeniem, że Wykonawca zobowiązany jest do:
2. przekazywania Zamawiającemu informacji o nowych wersjach SSI, ukazujących się w trakcie trwania Umowy, odbywać się będzie poprzez ESZ lub inną serwisową witrynę internetową Wykonawcy;
3. udostępniania aktualizacji SSI poprzez wskazany serwer ftp,
4. przeprowadzenia procesu Aktualizacji lub Unowocześnienia Systemu, na żądanie i w czasie uzgodnionym z Zamawiającym,
5. Możliwość zgłoszenia uwag i propozycji modyfikacji Szpitalnego Systemu Informatycznego.
6. Zapewnienie w ramach serwisu oprogramowania oraz asysty technicznej, nieodpłatnego (w limicie 100 godzin serwisowych):
* dostarczenia i wdrożenia nowych wersji (Unowocześnienia lub Aktualizacji) Szpitalnego Systemu Informatycznego otrzymanych w ramach świadczeń z tytułu nadzoru autorskiego (w tym w szczególnych przypadkach dodatkowe szkolenie użytkowników) objętego niniejszą umową;
* podjęcia starań w celu usunięcia Awarii Szpitalnego Systemu Informatycznego objętego niniejszą umową, powstałej z winy Zamawiającego lub wskutek wypadków losowych;
* bieżącego optymalizowania konfiguracji Zintegrowanego Systemu Informatycznego, uwzględniające potrzeby Zamawiającego;
* pomocy w awaryjnym odtwarzaniu, na wniosek Zamawiającego, stanu Szpitalnego Systemu Informatycznego i zgromadzonych danych archiwalnych, poprawnie zabezpieczonych w Środowisku Zapasowym, skonfigurowanym przez Wykonawcę w trakcie wdrożenia;
* pomocy w przygotowaniu danych przekazywanych przez Zamawiającego do jednostek nadrzędnych i współpracujących (np. do Narodowego Funduszu Zdrowia, Wydziału Zdrowia odpowiedniego urzędu, banków itp.) w formie elektronicznej (np. poprzez odpowiednie formaty plików, na wymaganych nośnikach danych, łącza telekomunikacyjne itp);
* doradztwa w zakresie rozbudowy środków informatycznych, dokonywanie ponownych instalacji Szpitalnego Systemu Informatycznego objętego niniejszą Umową w przypadkach rozbudowy infrastruktury informatycznej Zamawiającego;
* prowadzenia rejestru kontaktów z Zamawiającym, obejmującego wizyty serwisowe i wykonane czynności, w tym zmiany konfiguracji oprogramowania.
1. Usługi serwisu oraz asysty technicznej, określone powyżej, świadczone będą przez Wykonawcę w dni robocze tj. dni od poniedziałku do piątku z wyłączeniem dni ustawowo wolnych od pracy, w godzinach od 8:00 do 16:00.
2. Wyjątkiem będą sytuacje dotyczące Awarii (błędów krytycznych), dla których Wykonawca będzie świadczył usługi serwisu w trybie 24/7/365. Zgłoszenia Awarii dla tego rodzaju sytuacji, będą przyjmowane pod specjalnym, wskazanym przez Wykonawcę numerem telefonu.
3. Wszelkie koszty związane z wizytami (dojazd, nocleg, diety) przedstawicieli Wykonawcy, realizujących usługi wdrożeniowe i serwisowe, powinny zostać uwzględnione w ofercie Wykonawcy.