Numer referencyjny postępowania:

 **WSZ-EP-35/2022**

**Załącznik nr 1 do SWZ**

**Załącznik nr 1 do Umowy nr 35/2022**

**OPIS PRZEDMIOTU ZAMÓWIENIA (OPZ)**

Strony ustalają następujące definicje:

1. **Strony** - podmioty bezpośrednio uczestniczące w umowie zawiązanej na podstawie rozstrzygnięcia podstępowania przetargowego.
2. **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.
3. **Zintegrowany System Informatyczny** (zwany dalej **ZSI**, **Systemem** lub **Oprogramowaniem Aplikacyjnym**) – system informatyczny wspomagający zarządzanie, w skład którego wchodzą zintegrowane systemy/moduły dziedzinowego oprogramowania aplikacyjnego (np. HIS, ERP, RIS, PACS, LIS, eUsługi itd.), działający na Sprzęcie Komputerowym z wykorzystaniem Oprogramowania Narzędziowego, udostępniający funkcjonalności opisane w OPZ.
4. **Umowa** – umowa zawarta w ramach realizacji OPZ.
5. **Gwarancja i Serwis Oprogramowania** – Oznacza całokształt świadczonych przez Wykonawcę usług (gwarancyjno-serwisowych) związanych z zapewnieniem poprawnej pracy składników będących przedmiotem zamówienia, szczegółowo określone w niniejszym dokumencie oraz w projekcie umowy.
6. **Unowocześnienie systemu / aplikacji** (ang. Upgrade) – dostosowanie oprogramowania do nowych potrzeb użytkowników. Obejmuje zmiany zakresu funkcjonalnego i użytkowego oprogramowania w ramach poszczególnych modułów lub całości oprogramowania, oznaczające przynajmniej jedną z poniższych modyfikacji:
	* + usprawnienia dotychczasowych mechanizmów,
		+ poszerzenia funkcjonalności zastosowanych mechanizmów,
		+ dodanie nowych mechanizmów,
		+ zmiany estetyczne i formalne.

Unowocześnienie oprogramowania powoduje konieczność dostarczenia Zamawiającemu nowej Dokumentacji i ewentualnie przeprowadzenie dodatkowego szkolenia (w zależności od poziomu i zakresu zmian podstawowych funkcji oprogramowania), w której ujęte i opisane zostają wprowadzone modyfikacje. Czasami, Unowocześnienie ingeruje w strukturę bazy danych , a nawet wymaga zmiany jej wersji na wyższą. Często, w] zapisie formalnym oznaczenia wersji oprogramowania składającym się z ciągu cyfr lub liter, przedzielonych kropkami. Upgrade wiąże się zazwyczaj ze zmianą jednego ze znaków głównych (początkowych).

unowocześnienie systemu odnosi się do zakresu funkcjonalnego systemu bądź aplikacji, do którego Zamawiający uzyskał prawo do eksploatacji na podstawie udzielonej licencji dostarczonej w ramach realizacji przedmiotowego postepowania

1. **Aktualizacja systemu / aplikacji** (ang. Update) – uaktualnienie obejmujące zmiany związane z eliminacją zidentyfikowanych błędów aplikacji, najczęściej nie ingerujące w strukturę bazy danych. W niektórych przypadkach, Update wiąże się ze zmianą interfejsu użytkownika lub usprawnieniem działania funkcji lub procesów, natomiast nie wzbogaca aplikacji o nowe rozwiązania. Aktualizacja zazwyczaj nie wymaga konieczności dostarczenia Zamawiającemu nowej dokumentacji. W zapisie formalnym oznaczenia oprogramowania, Upgrade wiąże się zazwyczaj ze zmianą jednego ze znaków występujących po głównej pozycji (znaki środkowe).
2. **Łata** (ang. Patch) – poprawka wprowadzająca zmiany związane z eliminacją zidentyfikowanych błędów/luk oprogramowania, najczęściej nie ingerujące w strukturę bazy danych. W większości przypadków wiąże z usprawnieniem działania funkcji lub procesów, rzadziej ze zmianą interfejsu. Łaty nie wzbogacają oprogramowania o nowe rozwiązania. W zapisie formalnym oznaczenia oprogramowania, Patch wiąże się zazwyczaj ze zmianą jednego ze znaków występujących na końcu oznaczenia (znaki końcowe).
3. **Dokumentacja** (dot. oprogramowania - systemu lub aplikacji) – zbiór dokumentów dostarczonych przez Wykonawcę w formie tradycyjnej lub elektronicznej (np. plikach doc, pdf). Dokumentacja systemu to ogół dokumentacji technicznej i dokumentacji użytkownika stworzonej dla określonego oprogramowania informatycznego przez jego twórców. W jej skład wchodzą:
	* + dokumentacja użytkownika - opis programu przeznaczony dla jego użytkownika. Składają się na nią np. pliki pomocy, ogólne informacje o programie i jego sposobie obsługi.
		+ dokumentacja techniczna – dokumentacja jest przeznaczona dla osób, które mogą potrzebować modyfikować program (najczęściej są to użytkownicy uprzywilejowani – administratorzy). Zawiera dokładny opis metody działania programu, algorytmów w nim zastosowanych, rozmieszczenia i sposobu działania poszczególnych komponentów, tabel w bazie danych, powiązań logicznych w oprogramowaniu bazodanowym itp.
4. **Sprzęt Komputerowy** – zestaw komputerów (w tym stacje robocze, sprzęt serwerowy, terminale) i oprzyrządowania, na którym pracuje ZSI określony w OPZ.
5. **Stacja Robocza -** oznacza komputer klasy PC lub/i terminal z monitorem, na którym pracuje ZSI określony w OPZ i załączniku do OPZ.
6. **Nośnik** – fizyczny środek (materiał lub urządzenie) przechowujący lub przeznaczony do przechowywania w nim danych: CD, DVD, HDD, Pendrive.
7. **System Komunikacyjny** – infrastruktura telekomunikacyjna, sieciowa, systemy separacji, systemy bezpieczeństwa oraz certyfikaty serwerów WWW, obejmujące elementy lokalnej sieci komputerowej, łącza i urządzenia rozległej sieci transmisji danych oraz urządzenia komutacji pakietów wraz z ich oprogramowaniem, odpowiedzialne za obsługę ZSI.
8. **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;
9. **Analiza Przedwdrożeniowa** – wynik szeregu spotkań Stron, w trakcie których Zespół Konsultantów zapozna się ze strategią Zamawiającego, jego potrzebami, strukturą organizacyjną i przebiegiem procesów biznesowych. Etap ten zakończy się przygotowaniem przez Wykonawcę zbioru dokumentów pt. Analiza Przedwdrożeniowa, który będzie zawierał wynik ustaleń pomiędzy członkami Zespołu Wdrożeniowego oraz Wykonawcą,
10. **Plan Realizacji Projektu** – Dokument określający zasady współpracy pomiędzy Zamawiającym, a Wykonawcą. Zawiera m.in.:
	* strukturę organizacyjną projektu,
	* produkty projektu,
	* zasady komunikacji w projekcie,
	* procedury zarządzania ryzykiem i zmianami w projekcie,
	* metodykę realizacji projektu,
11. **Scenariusz Testów Akceptacyjnych** – spisany i uzgodniony z Zamawiającym zakres czynności operacyjnych, które należy wykonać w celu potwierdzenia, że wskazane wymagane funkcjonalności zostały prawidłowo skonfigurowane i działają zgodnie z opisami procesów,
12. **Testy Akceptacyjne** - proces sprawdzenia działania systemu w odniesieniu do funkcjonalności wymaganej w umowie i uszczegółowionej w dokumencie analizy przedwdrożeniowej,
13. **Szkolenie Administratora(ów)** – szkolenia użytkownika(ów) wskazanych przez Zamawiającego do pełnienia funkcji administratora ZSI,
14. **Systemy Zewnętrzne** – systemy z którymi docelowo współpracować będzie wdrażany system.
15. **Wdrożenie** – etap cyklu życia systemu informatycznego, polegający na instalacji i dostosowaniu oprogramowania do wymagań Zamawiającego 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. **Dokumentacja powdrożeniowa -** przygotowana przez Wykonawcę, w związku z realizacją Umowy, specyfikacja opisująca funkcje wdrożonego Systemu. W szczególności, w zakresie użytkowania Systemu oraz administrowania nim, w języku polskim.
2. **Środowisko Zapasowe** – kopia Środowiska Produkcyjnego lub jego części, służąca do gromadzenia kopii rzeczywistych danych biznesowych Zamawiającego i podjęcia ich przetwarzania w przypadku awarii Środowiska Produkcyjnego lub w celach przeprowadzenia testów wdrożeniowych aktualizacji/nowych funkcjonalności.
3. **Zdalny Dostęp** – analogowe lub cyfrowe łącze wydajnej transmisji danych pomiędzy węzłem infrastruktury siedziby Wykonawcy, a węzłem infrastruktury zapewnianym przez Zamawiającego, umożliwiające realizować usługi serwisowe lub konfiguracyjne.
4. **Szczegółowym Harmonogramem Realizacji Zadania** – szczegółowy terminarz realizacji przedmiotu Umowy wraz z podziałem na Etapy przygotowany przez Wykonawcę w terminie 14 dni roboczych od zawarcia umowy.
5. **Zadanie** – przedmiot zamówienia (przedmiot Umowy) wynikający łącznie z SWZ, Oferty Wykonawcy, Umowy.
6. **Etap** – główny element części Zadania, stanowiący funkcjonalną całość, podlegająca odrębnym odbiorom. Każdy Etap stanowi odrębną część (rozdział) niniejszego OPZ.
7. **Protokół Zdawczo – Odbiorczy** – protokół przygotowany przez Wykonawcę, będący potwierdzeniem przyjęcia przez Zamawiającego wykonanych przez Wykonawcę prac będących przedmiotem poszczególnych Etapów.
8. **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.
9. **Godziny Robocze** – godziny od 8:00 do 16:00 w każdym Dniu Roboczym.
10. **Kierownik Wdrożenia, Kierownik Wdrożenia Zamawiającego** – osoba wyznaczona przez

Zamawiającego, koordynująca całość Wdrożenia, posiadająca odpowiednie pełnomocnictwa. W szczególności odpowiedzialna ze strony Zamawiającego za realizację przedmiotu niniejszego OPZ.

1. **Kierownik Projektu, Kierownik Projektu Wykonawcy** - osoba wyznaczona przez Wykonawcę do koordynacji Wdrożenia oraz wspomagająca Kierownika Wdrożenia w osiąganiu celów Wdrożenia. Upoważniona do podpisywania Dokumentacji Projektu z ramienia Wykonawcy.
2. **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 oraz w okresie jego gwarancji.
3. **Błąd aplikacji** - oznacza działanie powtarzalne, pojawiające się za każdym razem w tym samym miejscu w aplikacji i prowadzące za każdym razem do otrzymywania błędnych wyników jej działania.
4. **Awaria (błąd krytyczny)** – oznacza sytuację, w której nie jest możliwe prawidłowe używanie ZSI z powodu uszkodzenia elementów serwera, uszkodzenia lub utraty kodu programu, struktur danych lub zawartości bazy danych. Awaria jest traktowana priorytetowo i usuwana najszybciej jak to jest możliwe.
5. **Usterka Programistyczna** – błąd aplikacji, mimo identyfikacji którego aplikacja nadal funkcjonuje, natomiast usunięcie którego wymaga ingerencji w kod źródłowy.
6. **Konsultacja** – usługa świadczona przez Wykonawcę polegająca na udzielaniu Zamawiającemu

wyjaśnień w kwestiach dotyczących ZSI.

# OGÓLNY OPIS PRZEDMIOTU ZAMÓWIENIA

Przedmiot zamówienia składa z następujących elementów:

1. dostawy i konfiguracji systemu bezpieczeństwa, modernizacji istniejącego środowiska sieciowego, dostawa licencji dostępowych do posiadanego środowiska
2. rozbudowy posiadanego przez Zamawiającego systemu ZSI

Wymienione elementy będą tworzyły dwa podstawowe Etapy przedmiotu zamówienia **stanowiące etapy składowe projektu o nazwie: Modernizacja infrastruktury teleinformatycznej oraz rozbudowa ZSI na potrzeby Wojewódzkiego Szpitala Zespolonego im. dr. Romana Ostrzyckiego w Koninie.**

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. 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 niniejszym załączniku i dane identyfikujące produkt.

Wykonawca, który nie oferuje równoważności nie ma obowiązku przedkładania opisów i materiałów jak powyżej.

1. **Dostawa i konfiguracja systemu bezpieczeństwa, modernizacja istniejącego środowiska sieciowego, dostawa licencji dostępowych do posiadanego środowiska**

**Przedmiotem etapu zamówienia jest, w szczególności:**

1. dostawa i konfiguracja systemu bezpieczeństwa,
2. modernizacja istniejącego środowiska sieciowego
3. dostawa licencji dostępowych do posiadanego środowiska
4. wykonanie warsztatów instruktażowych dla administratorów
5. udzielenie wsparcia powdrożeniowego

**Wymagania ogólne**

1. W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Wykonawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.
2. Wykonawca winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.
3. **Dostawa i konfiguracja systemu bezpieczeństwa**

**Wymagania Ogólne**

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się, aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić 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.

System musi wspierać IPv4 oraz IPv6 w zakresie:

* Firewall
* Ochrony w warstwie aplikacji
* Protokołów routingu dynamicznego.

wraz z urządzeniem należy dostarczyć 4 wkładki sfp+ LR dedykowane do dostarczanych urządzeń.

**Redundancja, monitoring i wykrywanie awarii**

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.
2. W ramach postępowania system musi zostać dostarczony w postaci redundantnej.
3. 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.

**Interfejsy, Dysk, Zasilanie:**

1. System realizujący funkcję Firewall musi dysponować minimum:
* 16 portami Gigabit Ethernet RJ-45.
* 8 gniazdami SFP 1 Gbps.
* 2 gniazdami SFP+ 10 Gbps.
1. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
2. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN’y w oparciu o standard 802.1Q.
3. System realizujący funkcję Firewall musi być wyposażony w lokalną przestrzeń dyskową o pojemności minimum 480 GB.
4. System musi być wyposażony w zasilanie AC.

**Parametry wydajnościowe:**

1. W zakresie Firewall’a obsługa nie mniej niż 1.5 mln. jednoczesnych połączeń oraz nie mniej niż 54 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 18 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 2.1 Gbps.
4. Wydajność szyfrowania IPSec VPN nie mniej niż 10 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 2.5 Gbps.
6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 1 Gbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 1 Gbps.

**Funkcje Systemu Bezpieczeństwa:**

W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje.

Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
2. Kontrola Aplikacji.
3. 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 system

**Polityki, Firewall**

1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
* Translację jeden do jeden oraz jeden do wielu.
* Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
1. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
2. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików.
3. 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 VPN**

1. 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.
1. 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 WAN**

1. 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-WAN**

1. 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 pasmem**

1. 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 malware**

1. 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 atakami**

1. 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 1000 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 aplikacji**

1. 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 1000 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 WWW**

1. 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 sesji**

1. 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.
1. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.
2. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.
3. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

**Zarządzanie**

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
3. 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.

**Logowanie**

1. 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.

**Certyfikaty**

Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje ICSA lub EAL4 dla funkcji Firewall.

**Serwisy i licencje**

W ramach zostaną dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Będą one obejmować: Kontrole 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 12 miesięcy.

**Gwarancja oraz wsparcie**

Gwarancja: System jest objęty serwisem gwarancyjnym producenta przez okres wskazany w ofercie Wykonawcy, 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. **Modernizacja istniejącego środowiska sieciowego**

**Opis założeń**

Środowisko Zamawiającego stanową dwie lokalizacje, znajdujące się w Koninie:

1. ul. Szpitalna 45, 62-504 Konin – Budynek główny szpitala lokalizacja serwerowni głównej. W lokalizacji znajduje się:
* 1x GPD ulokowany w serwerowni
* 28x PPD rozlokowane na terenie budynków szpitala
1. ul. Stefana Wyszyńskiego 1 , 62-510 Konin – Budynek Szpitala lokalizacja serwerowni DRC. W lokalizacji znajduje się :
* 1x GPD ulokowany w serwerowni
* 19x PPD rozlokowane na terenie budynków szpitala

Wszelkie połączenia pomiędzy punktami GPD i LPD realizowane są przy użyciu światłowodów jednomodowych.

Połączenie pomiędzy lokalizacjami Szpitalna i Wyszyńskiego musi być realizowane przy pomocy łącza światłowodowego w oparciu o wkładki jedno-włóknowe sfp+ .

**Zakres prac**

Zamawiający wymaga zainstalowania dostarczonego systemu bezpieczeństwa w pomieszczeniach serwerowni, jak i innych wskazanych miejscach w zakresie:

* Wniesienie, ustawienie i fizyczny montaż wszystkich dostarczonych urządzeń w szafach rack w pomieszczeniach (miejscach) wskazanych przez Zamawiającego z uwzględnieniem wszystkich lokalizacji.
* Urządzenia, które nie są montowane w szafach teleinformatycznych, powinny zostać zamontowane w miejscach wskazanych przez Zamawiającego, oraz skonfigurowane i dołączone do infrastruktury Zamawiającego.
* Podłączenie całości rozwiązania do infrastruktury Zamawiającego.
* Wykonanie procedury aktualizacji firmware dostarczonych elementów do najnowszej wersji oferowanej przez producenta.
* Wykonawca musi zapewnić niezbędne okablowanie potrzebne do podłączenia urządzeń aktywnych do sieci elektrycznej (np.: listwy zasilające).

Zamawiający wymaga stworzenia połączeń sieciowych pomiędzy lokalizacjami z wykorzystaniem istniejących połączeń światłowodowych lub innych dostępnych połączeń.

Wymiana infrastruktury musi umożliwiać podłączenie wszystkich dostępnych punktów rj45 w szafach ppd oraz gpd.

Każdy z wymienianych przełączników musi zostać podłączony min 2 linkami światłowodowymi do przełączników rdzenia sieci przy użyciu protokołu LACP. Jeżeli ilość połączeń światłowodowych nie będzie wystraczająca dla uzyskania opisanej funkcjonalności należy użyć wkładek wykorzystujących jedno włókno w celach obustronnej komunikacji.

Parametry minimalne Posiadanych urządzeń szkieletu sieci na urządzenia o parametrach minimalnych:

**Przełącznik Rdzenia Sieci 4 szt.**

|  |  |  |
| --- | --- | --- |
| LP | Nazwa | Parametr |
|  | Rozmiar | 19-inch, 1U |
|  | Interfejsy | • 48 x 1/10GbE SFP/SFP+ ports• 6 x 40/100GbE QSFP+/QSFP28 ports |
|  | Konsola | port konsolowy RJ45 Out-Of-Band |
|  | Port zarzadzania | 10/100/1000 BASE-T RJ-45 Out-Of-Band |
|  | USB | 1x USB 2.0 typ A |
|  | Przełączanie | min 2.16 Tbps |
|  | Stackowanie | Fizyczne: do 12 urządzeń, przepustowość do 1200 Gbps Virtualne: Do 32 urządzeń |
|  | Tablica Mac Address | do 288K |
|  | Spanning Tree | 802.1D STP802.1s MSTP802.1w RSTP  |
|  | Agregacja linków | 802.1AX |
|  | Ochrona ring-u | EPRS |
|  | Vlan | min 4K |
|  | Typ VLAN | GVRPw oparciu o adresację MACw oparciu o portw oparciu o protokół  |
|  | Advanced VLAN  | Double VLAN (Q-in-Q)ISM VLANSuper VLAN  |
|  | Data Center Bridging  | 802.1Qbb |
|  | Tablica Routingu | IPv4 - min 32K |
|  | ACL | EgressIngressVLAN-based  |
|  | Obsługa | IPv6 tunnelingMulticastingRIP v1/v2RIPngOSPFOSPFv3IP-MAC-port binding (IMPB) / Smart BindingARP spoofingBPDU attack protectionKontrola dostępu 802.1XMicrosoft NAP supportUwierzytelnienie RADIUS/TACACS+SNMP (v1/v2c/v3)RMON v1/v2sFlowLLDPLLDP-MED802.3ah802.1agITU-T Y.1731  |

**Przełącznik dostępowy Sieci min 44 szt.**

|  |  |  |
| --- | --- | --- |
| LP | Nazwa | Parametr |
|  | Rozmiar | 19-inch, 1U |
|  | Interfejsy | • min 24 x 10/100/1000Mbps z uwzględnieniem wymaganych portów Lan per LPD• 4 x 10G SFP+ |
|  | Konsola | port konsolowy RJ45 |
|  | Przełączanie | 176 Gbps |
|  | Stackowanie | Fizyczne: do 6 urzadzeńVirtualne: Do 32 urządzeń |
|  | Tablica Mac Address | min 16K |
|  | Spanning Tree | 802.1D STP802.1s MSTP802.1w RSTP  |
|  | Agregacja linków | 802.3ad |
|  | QoS | min 802.1p priority |
|  | Vlan | min 4K |
|  | Typ VLAN | GVRPw oparciu o adresację MACw oparciu o portw oparciu o protokół  |
|  | Routing | ARP-256 Static ARPDefault RoutingStatic Routing |
|  | Bezpieczeństwo | Broadcast/Multicast/Unicast Storm ControlDynamic ARP InspectionD-Link Safeguard EngineDHCP Server Screening |
|  | Tablica Routingu | IPv4 - min 64 wpisów statycznych |
|  | ACL | IngressVLAN-based  |
|  | Obsługa | Loopback Detection MLD Snooping IGMP SnoopingJumbo Frame up to 9,216 BytesFlow ControlCommand Line Interface (CLI)SSHLLDP, LLDP-MED.Web-based GUI |

**Dodatkowe wyposażenie**

Min 180 szt. wkładki SFP+ LR

8 szt. kabel dac sfp+ 0,5m

3 szt. kabel stackowy 100G QSFP28 1m

**Oprogramowanie Zarządzające**

Wraz z przełącznikami musi zostać dostarczone oprogramowanie producenta przełączników do zarzadzania i monitorowania dostarczanej infrastruktury sieciowej. Oprogramowanie powinno obejmować obsługę wszystkich dostarczanych przełączników

**Instalacja i konfiguracja**

Rekonfiguracja urządzeń w zakresie:

* Stworzenia optymalnych połączeń pomiędzy przełącznikami z wykorzystaniem dedykowanych modułów.
* Konfiguracja protokołu STP.
* Konfiguracja sieci wirtualnych VLAN – taka liczba sieci wirtualnych aby odseparować różne typy ruchu, ale nie mniej niż:

• VLAN’y per- jednostka/oddział (odzwierciedlające strukturę organizacyjną), min 47
• VLAN WLAN,
• VLAN drukarki , per- jednostka/oddział (odzwierciedlające strukturę organizacyjną), min 47
• VLAN Serwer, min 2
• VLAN Public,
• VLAN DMZ,
• VLAN MGMT – dla ruchu do systemów zarządzania sprzętem .

* Konfiguracja połączeń pomiędzy przełącznikami sieci LAN z wykorzystaniem połączeń światłowodowych oraz miedzianych.
* Dołączenie i konfiguracja przełączników CORE do dostarczanych urządzeń firewall – klaster
* konfiguracja klastra HA firewall:
* Modernizacja konfiguracja klastra HA firewall w trybie active-active
* Segmentacja sieci w oparciu o protokół 802.1q
* Konfiguracja routingu pomiędzy sieciami VLAN
* Konfiguracja polityk dostępu pomiędzy strefami
* Konfiguracja dostępu zdalnego dla różnych grup użytkowników
* Konfiguracja funkcji bezpieczeństwa w zakresie: skanowanie antywirusowe, moduł IPS, moduł web-filter, inspekcja protokołu https.
* Konfiguracja połączenia pomiędzy lokalizacja główną a punktem DRC.
* Konfiguracja serwerów DHCP na użytek urządzeń końcowych, które zostaną przyłączone do portów w poszczególnych sieciach VLAN
* Implementacja mechanizmów bezpieczeństwa sieci LAN:
* Mechanizm monitorowania przydziału adresów IP przez serwery DHCP, ochrona przed nieautoryzowanymi serwerami DCHP.
* Mechanizm monitorowania prawidłowego użycia protokołu ARP przez stacje końcowe w celu zapobieżenia nadużyciom oraz atakom typu „man in the middle”.
* Implementacja mechanizmów Quality of Service:
* Konfiguracja w miarę możliwości środowiska kolejkowania traktującego ruch pochodzący od serwerów oraz ruch zarządzający jako priorytetowy.
* Implementacja w miarę możliwości środowiska mechanizmów zapobiegających wysycaniu pasma na łączach pomiędzy przełącznikami, routerami oraz firewall’em poprzez niepożądany ruch sieciowy np. ruch generowany przez stacje zainfekowane wirusem (Scaveger QoS).
* Przepięcie obecnej infrastruktury serwerowo-macierzowej szpitala pod zrekonfigurowaną sieć LAN.
* Przepięcie i rekonfiguracja infrastruktury serwerowej w tym środowiska klastra bazodanowego, środowiska wirtualizacji oraz środowiska serwera diagnostyki obrazowej.
* Przygotowanie Środowiska DRC w oparciu o posiadany sprzęt umiejscowiony w serwerowni w lokalizacji Wyszyńskiego, w szczególności przygotowanie środowiska do awaryjnego odtworzenia bazy danych oraz środowiska wirtualizacji wraz z przygotowaniem instrukcji wykonania odtworzenia, określeniem czasu odtworzenia i przeprowadzeniem szkolenia.
* Migracja obecnie posiadanego środowiska Active Directory do wersji 2022 w tym:
* Migracja 2 Kontrolerów domeny z wersji 2008 R2
* Migracja Klastra Microsoft z uwzględnieniem replikacji danych pomiędzy 2-ma macierzami ( na poziomie usługi klastrowej) – do zmigrowania 2TB danych użytkowników – profile mobilne z 2008 R2
* Migracja Serwerów Certyfikatów z 2008 R2
* Migracja Serwerów Terminali – 4 serwery usług terminalowych wraz z konfiguracją środowiska do pracy z brokerem sesji usług terminalowych umożliwiających prace w posiadanym systemie medycznym Eskulap.
* Konfiguracja serwerów usług opartych obecnie o Microsoft Windows 2008 R2
* W tym usług medycznych : EskulapNT, serwer EDM, eRejestracja , HL7
* W tym usług części szarej : Simple

W celu realizacji prac Zamawiający dopuszcza wykorzystanie istniejącej infrastruktury sieciowej lub dostarczenie alternatywnej o parametrach zapewniających optymalną pracę całości sieci Zamawiającego.

1. **Dostawa licencji dostępowych zgodnych z posiadanym środowiskiem**

Zamawiający posiada obecnie środowisko Active Directory, w ramach postępowania należy zmigrować obecnie posiadaną infrastrukturę z posiadanego 2008 R2 na 2022 . Szpital posiada licencje systemów operacyjnych w wersji 2022 , migracja wymaga zakupienia poniższych licencji:

|  |  |
| --- | --- |
| Cecha | Wymagania minimalne |
| Oprogramowanie | MS Windows 2022 Device CAL lub równoważne  |
| Kompatybilność | Zamawiający wymaga, aby licencja była kompatybilna z Serwerowym Systemem Operacyjnym SSO opisanym powyżej. |
| Ilość | 600 szt. |

|  |  |
| --- | --- |
| Cecha | Wymagania minimalne |
| Oprogramowanie | MS Windows 2022 Remote Desktop Device CAL lub równoważne  |
| Kompatybilność | Zamawiający wymaga, aby licencja była kompatybilna z Serwerowym Systemem Operacyjnym SSO opisanym powyżej. |
| Ilość | 1. szt.
 |

**Dokumentacja**

Zamawiający wymaga opracowania dokumentacji technicznej użytkownika (w formie elektronicznej) obejmującej opis konfiguracji wdrożonego systemu. Wykonawca przenosi na Zamawiającego na zasadach regulowanych umową prawa autorskie majątkowe do wszelkiej dokumentacji, w tym również dokumentacji technicznej, jaką przekaże Zamawiającemu w ramach wykonania umowy, oraz własność nośników egzemplarzy takiej dokumentacji, w ramach wynagrodzenia umownego, z chwilą podpisania przez Wykonawcę i Zamawiającego końcowego protokołu odbioru.

Konfiguracje urządzeń (lub opisy konfiguracji w przypadku sprzętu lub oprogramowania nieumożliwiającego eksportu konfiguracji do pliku tekstowego bądź posiadające rozproszoną konfigurację).

Dyski instalacyjne dostarczonego oprogramowania, jeżeli takowe występowały.

Kody dostępowe oraz klucze licencyjne, jeżeli takowe występowały.

Opis typowych czynności, prac administracyjnych, które pozwalają na codzienną obsługę dostarczonego i zmodernizowanego sprzętu oraz systemów.

1. **Warsztaty instruktażowe**

Warsztaty instruktażowe mają obejmować zakres dostarczonego/zmodernizowanego sprzętu. Całość powinna zostać zrealizowana w ciągu 2 dni zgodnie z przekazanym Zamawiającemu przez Wykonawcę szczegółowym harmonogramem realizacji zadania i dotyczyć będzie autorskiego rozwiązania zrealizowanego w ramach podmiotowego wdrożenia. Warsztaty instruktażowe będą przeznaczone dla 3 osób i będą odbywały się w siedzibie Szpitala w pomieszczeniu wskazanym przez Zamawiającego. Sprzęt do obsługi warsztatów instruktażowych zapewni Wykonawca.

Zakres warsztatów instruktażowych:

* Architektura sieci LAN – przełączniki sieciowe.
* Punkt styku z Internetem – firewall.
1. **Asysta powdrożeniowa**

Zamawiający wymaga świadczenia asysty powdrożeniowej przez okres minimum 1 miesiąca od dnia podpisania protokołu odbioru końcowego (telefoniczna, zdalna, mailowa, na miejscu u klienta) z czasem reakcji następnego dnia roboczego dla problemów istotnych.

Czas reakcji jest rozumiany jako podjęcie działań mających na celu wsparcie w rozwiązywaniu problemów technicznych.

Wykonawca zapewni przyjmowanie zgłoszeń w Godzinach Roboczych, przez które rozumie się godziny od 08.00 do 16.00 w Dni Robocze.

###

1. **Rozbudowa posiadanego przez Zamawiającego systemu ZSI**
2. Wykonawca zobowiązuje się dostarczyć Zamawiającemu wymagane funkcjonalności ZSI 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 zachowanie pełnej wzajemnej interoperacyjności nowo wdrażanych modułów/grup funkcjonalności, a także w przypadku rozbudowy, pełnej interoperacyjności z modułami/grupami /systemami funkcjonalności już funkcjonującymi u Zamawiającego.
3. Zarówno w przypadku rozbudowy i zmodernizowania istniejącego systemu jak i dostawy nowego rozwiązania, 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.
4. 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.
5. 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 do migracji danych z istniejącego systemu klasy HIS (Eskulap firmy Nexus Polska Sp z o.o.).
6. Szpitalny System Informatyczny musi spełniać wymogi i zalecenia im stawiane, takie jak:
* Zapewnienie pełnej zgodności na dzień odbioru z opracowaniami publikowanymi przez CeZ
* Rozporządzenie Ministra Zdrowia z dnia 6 kwietnia 2020 r. w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania ( tj. z 22 czerwca 2022 r., Dz.U. 2022 poz. 1304 )
* Ustawa z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia (tj. z dnia 26 lipca 2022 r. Dz. U.
z 2022 r. poz. 1555 z późn. zm.)
* Efektywną interoperacyjność z platformami P1 i P2 oraz z platformą regionalną, od momentu produkcyjnego ich uruchomienia, zgodnie z rekomendacjami publikowanymi przez CeZ.
* Wymianę dokumentacji w ramach systemu informacji medycznej bezpośrednio pomiędzy jednostkami ochrony zdrowia, a także za pośrednictwem systemów regionalnych i z wykorzystaniem platformy P1
* Wymianę dokumentacji zarówno pacjentom, jak i ich opiekunom, a także podmiotom do tego uprawnionym, np. prokuraturze oraz udostępni dokumentacje w celu realizacji procesów diagnostyczno-terapeutycznych
1. Stan bieżący posiadanego systemu HIS.

Obecnie Zamawiający posiada w ramach HIS system Eskulap (Nexus Polska Sp. z o.o.)

Zamawiający wskazuje, że jest licencjobiorcą modułów medycznego oprogramowania aplikacyjnego przedstawionych w poniższej Tabeli 1 kolumna LP.1. Realizacja przez Wykonawcę przedmiotu zamówienia określonego w niniejszym OPZ winna nastąpić w sposób gwarantujący Zamawiającemu dalsze poprawne i właściwe funkcjonowanie oraz użytkowanie posiadanego medycznego oprogramowania aplikacyjnego.

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.

1. Stan obecny i docelowy modułów systemu HIS.

Zamawiający wymaga by Wykonawca dostarczył dodatkowe bezterminowe licencje modułów posiadanego medycznego oprogramowania aplikacyjnego oraz licencje nowych modułów ZSI 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.

|  |  |  |  |
| --- | --- | --- | --- |
| **Tabela 1** | **LP.1** | **LP.2** | **Lp.3** |
| **Licencja na moduł** | **Posiadane** | **Rozbudowa** | **Łącznie po rozbudowie** |
| Eskulap - Administrator | 3 RU |  | 3 RU |
| Eskulap - Apteczka Oddziałowa | 26 RU |  | 26 RU |
| Eskulap - Apteka | 5 RU |  | 5 RU |
| Eskulap - Bakteriologia | 5 RU |  | 5 RU |
| Eskulap - Biuro Przyjęć, Statystyka | 6 RU |  | 6 RU |
| Eskulap - Blok Operacyjny | 5 RU |  | 5 RU |
| Eskulap – Blok Porodowy | 5 RU |  | 5 RU |
| Eskulap - DICOM | 24 URZ |  | 24 URZ |
| Eskulap - Dokumentacja Medyczna | OPEN |  | OPEN |
| Eskulap - Dyrekcja | 3 RU |  | 3 RU |
| Eskulap - eRejestracja | 2 SRW |  | 2 SRW |
| Eskulap - eWyniki | 2 SRW |  | 2 SRW |
| Eskulap - Gabinet | 25 RU |  | 25 RU |
| Eskulap - Gruper | 1 SRW |  | 1 SRW |
| Eskulap - HL7 | 3 SYS |  | 3 SYS |
| Eskulap - Integrator | 1 SYS |  | 1 SYS |
| Eskulap - Izba Przyjęć | 7 RU |  | 7 RU |
| Eskulap - Kalkulacja Kosztów Procedur | 4 RU |  | 4 RU |
| Eskulap - Kolejki Oczekujących | 1 SRW |  | 1 SRW |
| Eskulap - Laboratorium | 14 RU |  | 14 RU |
| Eskulap - Lekarz Zakładowy | 4 RU |  | 4 RU |
| Eskulap - Magazyn | 2 RU |  | 2 RU |
| Eskulap - mApteka | 6 URZ |  | 6 URZ |
| Eskulap - mObchód | OPEN |  | OPEN |
| Eskulap - Oddział | OPEN |  | OPEN |
| Eskulap - PACS | 1 SRW |  | 1 SRW |
| Eskulap - Podpis elektroniczny z archiwum dokumentów cyfrowych (Archiwum dokumentów cyfrowych) | 1 SRW |  | 1 SRW |
| Eskulap - Poradnia | 30 RU |  | 30 RU |
| Eskulap – Pracownia Diagnostyczna | 20 RU |  | 20 RU |
| Eskulap - Pracownia Cytostatyków | 2 RU |  | 2 RU |
| Eskulap - Pracownia Cytostatyków - Loża | 1 URZ |  | 1 URZ |
| Eskulap - Pracownia Diagnostyczna | 20 RU |  | 20 RU |
| Eskulap - Rachunek Kosztów Leczenia | 4 RU |  | 4 RU |
| Eskulap - Rehabilitacja | 6 RU |  | 6 RU |
| Eskulap - Rejestracja Poradni | 10 RU |  | 10 RU |
| Eskulap - Replikator Danych | 2 URZ |  | 2 URZ |
| Eskulap - Rozliczenia z Płatnikami | 4 RU |  | 4 RU |
| Eskulap - Sterownik Analizatora | 20 URZ |  | 20 URZ |
| Eskulap - Zakażenia Szpitalne | 3 RU |  | 3 RU |
| Eskulap - Zakład Histopatologii | 5 RU |  | 5 RU |
| Eskulap - Zlecenia Medyczne | OPEN |  | OPEN |
| Eskulap - Zlecenia Medyczne (Diagnostyka Ogólna) | OPEN |  | OPEN |
| Eskulap - Zlecenia Medyczne (Pracownia Cytostatyków) | 5 RU |  | 5 RU |
| Eskulap - Żywienie | 4 RU |  | 4 RU |
| Eskulap - eZLA | 1 SRW |  | 1 SRW |
| Eskulap - APKOLCE | 1 SRW |  | 1 SRW |
| Rejestr Zdarzeń Medycznych | 1 SRW |  | 1 SRW |
| Interfejs TOPSOR | 1 SRW |  | 1 SRW |
| Ordynacja Lekarska  | OPEN |  | OPEN |
| Pulpit Lekarski  | OPEN |  | OPEN |
| Bank krwi | 2 RU |  | 2 RU |
| Lokalne Oprogramowanie Komunikacyjne | 1 SRW |  | 1 SRW |
| NT | 1 SRW |  | 1 SRW |
| Transport Medyczny |  | 10 RU | 10 RU |
| eZWM |  | 1 SRW | 1 SRW |
| Powiadomienia |  | 1 SRW | 1 SRW |
| Interfejs NFZ AP-DILO |  | 1 SRW | 1 SRW |
| Interfejs KRN |  | 1 SRW | 1 SRW |
| Poczta |  | 1 SRW | 1 SRW |
| mPracownik |  | powyżej 1000 ST | powyżej 1000 ST |

Wyjaśnienie do powyższej tabeli

1. Moduły mają być zainstalowane w systemie z określeniem uprawnień do ich wykorzystywania na stacjach roboczych wskazanych przez Zamawiającego.
2. Zamawiający ma prawo tylko do takich kopii Oprogramowania Aplikacyjnego, które są niezbędne do zapewnienia bezpieczeństwa ich działania.
3. Zamawiający nie ma prawa do sprzedaży, wypożyczania, powielania, odstępowania, lub rozpowszechniania w innej formie, zmienienia, dekompilacji, tłumaczenia Oprogramowania Aplikacyjnego.
4. Zamawiający nie ma prawa do usuwania bądź zmiany znaków handlowych i informacji o Wykonawcy, bądź producencie podanych w Oprogramowaniu Aplikacyjnym i materiałach towarzyszących.
5. Zamawiający ma prawo do rozpowszechniania bez ograniczeń danych i zestawień utworzonych za pomocą Oprogramowania Aplikacyjnego.
6. Akty prawne
7. Ustawa z dnia 15 kwietnia 2011r. o działalności leczniczej (Dz. U. 2022 poz. 633 z późn. zm.),
8. Ustawa z dnia 5 grudnia 2008r. o zapobieganiu oraz zwalczaniu zakażeń i chorób zakaźnych u ludzi (Dz.U. 2021 poz. 2069 z późn. zm– dotyczy Systemu medycznego HIS - Monitorowanie zakażeń zakładowych.
9. Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. 2019 poz. 1781 z późn. zm.),
10. Rozporządzenie Ministra Zdrowia z dnia 20 września 2012 r. w sprawie warunków, sposobu i trybu zaopatrywania pacjentów szpitala w znaki identyfikacyjne oraz sposobu postępowania w razie stwierdzenia ich braku (Dz. U. 2012 poz. 1098) – dotyczy Systemu medycznego HIS),
11. Rozporządzenie Ministra Zdrowia z dnia 10 sierpnia 2021 r. w sprawie rodzajów i zakresu dokumentacji medycznej oraz sposobu jej przetwarzania (Dz.U. 2021 poz. 1468 z późn. zm.),
12. Ustawa z dnia 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych (Dz.U. 2021 poz. 1285 z późn. zm.),
13. Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. 2017 poz. 2247 z późn. zm.).
14. Ustawa z dnia 11 września 2019 r. - Prawo zamówień publicznych (Dz.U. 2021 poz. 1129 z późn. zm. ) wraz z delegowanymi aktami wykonawczymi.
15. Rozporządzenie Ministra Zdrowia z dnia 08 maja 2018 r. w sprawie rodzajów elektronicznej dokumentacji medycznej (Dz.U.2021 r. poz. 1153)
16. Rozporządzenie Ministra Zdrowia z dnia 21 grudnia 2018 r. w sprawie przyjęcia oraz wypisania ze szpitala psychiatrycznego (Dz.U. z 2018 roku, poz. 2475),
17. Rozporządzenie Ministra Zdrowia z dnia 26 czerwca 2020 r. w sprawie szczegółowego zakresu danych zdarzenia medycznego przetwarzanego w systemie informacji oraz sposobu i terminów przekazywania tych danych do Systemu Informacji Medycznej (Dz. U. z 2020 roku, pozycja 1253),
18. Rozporządzenie Ministra Zdrowia z dnia marca 2021 r. w sprawie wzorów oświadczeń o przysługującym świadczeniobiorcy prawie do świadczeń opieki zdrowotnej (Dz.U.2021, pozycja 475),
19. Ustawa z dnia 19 sierpnia 1994 r. o ochronie zdrowia psychicznego (Dz.U. 2020 poz. 685 z późniejszymi zmianami),
20. Rozporządzenie Ministra Zdrowia z dnia 18 kwietnia 2013 r. w sprawie zakresu niezbędnych informacji gromadzonych przez świadczeniodawców posiadających umowę z Narodowym Funduszem Zdrowia o udzielanie całodobowych lub całodziennych świadczeń zdrowotnych związanych z nabywaniem leków, środków spożywczych specjalnego przeznaczenia żywieniowego oraz wyrobów medycznych (Dz.U. z 2013 roku, pozycja 489),
21. Rozporządzenie Ministra Zdrowia z dnia 30 lipca 2009 r. sprawie prowadzenia depozytu w stacjonarnym zakładzie opieki zdrowotnej (Dz.U z 2021 r., poz. 200),
22. Ustawa z dnia 29 lipca 2005 r. o przeciwdziałaniu narkomanii (Dz.U. 2020 poz. 2050)
23. Rozporządzenie Ministra Zdrowia z dnia 8 kwietnia 2014 r. w sprawie zajęć rehabilitacyjnych organizowanych w szpitalach psychiatrycznych (Dz.U. 2014 poz. 522)
24. Dostarczone i wdrożone Oprogramowanie ma spełniać wszystkie przepisy powszechnie obowiązującego prawa polskiego i europejskiego.
25. Wymagania dotyczące wdrożenia modułów licencji
26. W ramach usług wdrożeniowych wchodzić będzie w szczególności:
27. Instalacja, konfiguracja oraz parametryzacja modułów ZSI na serwerze oraz na stacjach roboczych w miejscach wskazanych przez Zamawiającego,
28. Integracja dostarczanego systemu z systemami posiadanymi przez Zamawiającego.
29. Zamawiający wymaga by moduły ZSI wdrożone przez Wykonawcę w ramach realizacji przedmiotu zamówienia były wdrożone w pełnej ich funkcjonalności opisanej w dalszej części dokumentu.
30. 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.
31. Po dokonaniu instalacji i wdrożenia docelowo Zintegrowany System Informatyczny powinien:
32. spełniać wymagania określone niniejszym dokumentem,
33. spełniać wymagania obowiązujących przepisów prawa i uwzględniać charakter prowadzonej przez Zamawiającego działalności.
34. Po zakończeniu realizacji przedmiotu zamówienia oraz po stwierdzeniu poprawności funkcjonowania wdrożonych modułów zintegrowanych z systemem działającym u Zamawiającego, podpisany zostanie przez Zamawiającego i Wykonawcę Końcowy Protokół Odbioru – bezusterkowy.
35. Po zakończeniu realizacji przedmiotu zamówienia Wykonawca wykona i przekaże Zamawiającemu dokumentację powykonawczą dla administratorów zawierającą dokładny opis funkcjonalny dostarczanych modułów ZSI.
36. Zamawiający wymaga by docelowo wdrożone moduły systemu medycznego zintegrowane z systemem medycznym, z którego korzystał dotychczas Zamawiający, korzystały z jednorodnej bazy danych - ze względu na konieczność zapewnienia jednolicie wysokiego bezpieczeństwa gromadzonych wrażliwych danych medycznych oraz ich spójności.
37. Zamawiający wymaga by docelowo wdrożone moduły systemu medycznego zintegrowane z systemem medycznym, z którego korzystał dotychczas Zamawiający spełniały następujące warunki:
38. zapewnienie jednolitego sposobu wprowadzania danych za pomocą jednego interfejsu,
39. zapewnienie pełnego wykorzystania i dostępu do danych zgromadzonych w obecnie funkcjonującym u Zamawiającego systemie medycznym,
40. zachowanie ciągłości obecnie stosowanej przez Zamawiającego numeracji dokumentacji medycznej,
41. zapewnienie jednego modułu/ aplikacji systemu medycznego do prowadzenia sprawozdawczości i rozliczeń z NFZ,
42. zapewnienie możliwości wykonywania archiwalnych statystyk i raportów,
43. 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);
44. muszą pozwalać na wykonywanie kopii zapasowych struktur danych w trakcie ich pracy;
45. 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;
46. muszą współpracować z aplikacjami typu MS Word, MS Excel w zakresie eksportu danych;
47. muszą zapewniać aktualizację informacji w bazach danych podczas rutynowych czynności wykonywanych na stanowiskach pracy;
48. winny być w języku polskim i komunikować się z użytkownikiem w języku polskim, udostępniając mu możliwość korzystania z rozbudowanych podpowiedzi;
49. 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.
50. Zamawiający oświadcza, że nie jest w posiadaniu kodów źródłowych modułów posiadanego systemu medycznego, a w związku z powyższym Zamawiający przewiduje – na podstawie art.75 ust.2 pkt 3 ustawy z dnia 04 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz.U. 2021, nr 90, poz. 1062) - konieczność dokonania przez Wykonawcę dekompilacji modułów systemu medycznego, dotychczas wykorzystywanego przez Zamawiającego, poprzez zwielokrotnienie kodu lub tłumaczenie jego formy w rozumieniu art.74 ust.4 pkt 1 i 2 ustawy o prawie autorskim i prawach pokrewnych (Dz.U. 2021, nr 90, poz. 1062), jeżeli będzie to niezbędne do uzyskania informacji koniecznych do osiągnięcia współdziałania modułów posiadanego systemu z modułami systemu medycznego dostarczonymi w ramach realizacji zamówienia. Wykonawca będzie zobowiązany wykonać czynności dekompilacyjne na własny koszt i ryzyko, w pełnym koniecznym zakresie z zastrzeżeniem, że czynności te będą odnosiły się tylko do tych części modułów posiadanego systemu medycznego, które będą niezbędne do osiągnięcia współdziałania tych modułów z modułami systemu medycznego dostarczonymi przez Wykonawcę.
51. Zamawiający wymaga, aby moduł/y był/y zainstalowany/wdrożony/zintegrowany w ramach istniejącej instalacji ZSI z uwzględnieniem posiadanej konfiguracji, oraz zapewni ciągłość pracy systemów.
52. Oprogramowanie powinno posiadać interfejs w języku polskim.
53. Wymagane jest, aby uruchomienie zakończyło się instruktażem z zakresu obsługi dla Użytkownika.
54. Wykonawca musi być producentem lub posiadać aktualną autoryzację producenta oprogramowania uprawniającą do świadczenia usług wdrożeniowych oraz serwisowych
55. Dostawa, instalacja, konfiguracja i wdrożenie ZSI:
56. Zadanie dostawy, instalacji, konfiguracji i wdrożenia Oprogramowania aplikacyjnego obejmuje dostarczany w ramach realizacji zamówienia system ZSI
57. Dostawa i instalacja mają być wykonana w lokalizacji Zamawiającego.
58. 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.
59. 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 Zamawiającego.
60. ZSI musi zostać zainstalowany 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.
61. Instruktaż stanowiskowe
62. Wykonawca zaplanuje w uzgodnieniu z Przedstawicielem Zamawiającego Instruktaże stanowiskowe. Instruktaże stanowiskowe zostaną przeprowadzone w miejscach instalacji Oprogramowania z zakresu obsługi, administracji i utrzymania.
63. Instruktaże stanowiskowe będą prowadzone w języku polskim i obejmą w szczególności:
64. pomoc użytkownikom w korzystaniu z Oprogramowania w miejscu instalacji,
65. pomoc w administracji i konfiguracji Systemu,
66. wykonywanie dodatkowych prac konfiguracyjnych,
67. konsultacje.
68. Instruktaże stanowiskowe będą prowadzone w dwóch kategoriach:
69. dla użytkowników Oprogramowania aplikacyjnego,
70. dla administratorów technicznych - wyznaczonych spośród pracowników Zamawiających, obejmujących zakres konfiguracji i użytkowania ZSI oraz nadzoru nad użytkownikami oraz wydawania uprawnień (poświadczeń/certyfikatów),
71. Szacowana liczba pracowników Zamawiającego planowanych do instruktaży stanowiskowych - 500 osób
72. Wykonawca winien w ramach oferty uwzględnić poniższą ilość godzin szkoleniowych:
73. dla użytkowników oprogramowania aplikacyjnego, szacowana liczba godzin szkoleniowych dla wszystkich dostarczanych modułów/systemów: do 200 godz.
74. dla administratorów technicznych szacowana liczba godzin szkoleniowych dla wszystkich dostarczanych modułów/systemów: do 100 godz.
75. Wykonawca wykona i uzgodni z Zamawiającymi plan instruktaży stanowiskowych w etapie wykonania Dokumentacji Analizy Przedwdrożeniowej.
76. 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.
77. 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.
78. Wykonawca nie ponosi odpowiedzialności za brak uczestnictwa użytkowników w szkoleniach. Za skuteczne przeprowadzenie szkolenia uważa się dostępność w ustalonym miejscu i terminie przedstawicieli Wykonawcy, gotowych przeprowadzić szkolenia zgodnie z ustalonym harmonogramem.
79. 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.
80. Testy
81. 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.
82. Pozytywne zakończenie testów wraz z usunięciem wskazanych Błędów Aplikacji jest niezbędne, aby dla poszczególnych Komponentów oraz całego Przedmiotu Zamówienia dokonać odbiorów w ramach poszczególnych Etapów Odbioru Końcowego.
83. Scenariusz testów akceptacyjnych zostanie złożony Zamawiającemu na minimum 7 dni przed planowaną datą przeprowadzenia Testów Akceptacyjnych. Zamawiający dokona akceptacji lub wniesie uwagi do scenariusza testów do 3 dni od ich otrzymania.
84. Dodatkowe zobowiązania Wykonawcy
85. Oferowane rozwiązanie ma być rozwiązaniem działającym, gotowym do wdrożenia i zapewniającym realizację wszystkich wymaganych w SWZ, OPZ funkcjonalności na dzień składania ofert. Rozwiązanie nie może być w fazie budowy, testów, projektowania itp.
86. Wykonanie Przedmiotu Zamówienia z efektywnością oraz zgodnie z praktyką i wiedzą zawodową.
87. Wykonanie w całości Przedmiotu Zamówienia w zakresie określonym w Umowie i SWZ.
88. Dokonanie z Zamawiającym wszelkich koniecznych ustaleń mogących wpływać na zakres i sposób realizacji Przedmiotu Zamówienia oraz ciągła współpraca z Zamawiającym na każdym etapie realizacji.
89. Stosowanie się do wytycznych i polityk bezpieczeństwa informacji u Zamawiającego.
90. Udzielanie na każde żądanie Zamawiającego pełnej informacji na temat stanu realizacji Przedmiotu Zamówienia.
91. Współdziałanie z osobami wskazanymi przez Zamawiającego.
92. Oprogramowanie aplikacyjne – Wymagania ogólne
93. Wykonawca zobowiązuje się dostarczyć Zamawiającemu określone funkcjonalności systemu ZSI, 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.
94. 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.
95. Dane zaimportowane do Systemu ZSI z aktualnie użytkowanego oprogramowania muszą być spójne z nowo wprowadzanymi, edytowalne, podlegające analizie i spełniające warunki walidacji dla określonych typów pól.
96. Pełną odpowiedzialność za przeniesienie danych ponosi Wykonawca.
97. Zamawiający wymaga także, aby wszystkie posiadane lub dostarczane systemy zewnętrzne integrowały się z modernizowanym lub oferowanym systemem informatycznym. Pełną odpowiedzialność za integracje z systemami zewnętrznymi ponosi Wykonawca.
98. Wykonawca w przypadku rozbudowy lub wymiany ZSI obecnie użytkowanego przez Zamawiającego zobowiązany jest zapewnić wzajemną integrację wszystkich dostarczanych modułów ZSI, oraz systemów, w zakresie funkcjonalnie nie mniejszym niż obecnie istniejący.
99. Szczegółowy zakres wymaganych funkcjonalności systemu, został opisany poniżej.
100. Warunki usług opieki serwisowej i aktualizacyjnej:

Wykonawca ma obowiązek świadczyć usługi opieki serwisowej i aktualizacyjnej dla dostarczonego ZSI przez okres zadeklarowany w ofercie.

W obrębie usługi opieki serwisowej Zamawiający nabywa prawo do dowolnego wykorzystania 10 godzin opieki serwisowej w każdym miesiącu w okresie obowiązywania Umowy. Łączna liczba godzin serwisowych w okresie obowiązywania umowy stanowi iloczyn liczby miesięcy gwarancji zaproponowanej przez Wykonawcę w ramach kryterium oceny oferty oraz 10 godzin.

W ramach usług opieki serwisowej i aktualizacyjnej 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 wysłania zgłoszenia do momentu podjęcia 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 ZSI (tj. czas od momentu wysłania zgłoszenia, do momentu usunięcia przez Wykonawcę nieprawidłowości, przywrócenia Systemu do stanu sprzed zgłoszenia ) wynosi do 48 godzin;
* w przypadku zastosowania przez Wykonawcę rozwiązania zastępczego dalsza obsługa usunięcia dotychczasowego błędu krytycznego będzie traktowana jako błąd zwykły, tj. zgodnie z procedurą opisaną pod lit. b) poniżej ;
1. w pozostałych przypadkach:
* czas reakcji Wykonawcy na zgłoszenie Zamawiającego (tj. czas od momentu wysłania zgłoszenia do momentu podjęcia 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 ZSI, (tj. czas od momentu wysłania zgłoszenia, do momentu usunięcia przez Wykonawcę nieprawidłowości, przywrócenia Systemu do stanu sprzed zgłoszenia), wyniesie do 7 dni roboczych;

c) ewentualne przekwalifikowanie błędu zgłoszonego przez Zamawiającego jako zwykły, na Awarię, wymagać będzie osobnego zgłoszenia i oznaczać będzie uruchomienie procedury opisanej w pkt. a).

d) 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 wolnym od pracy - traktowany jest jak przyjęty o godz. 8.00 najbliższego dnia roboczego;
* wyjątkiem od reguł opisanych w tiret 1-3, będą formularze zgłoszenia Awarii (błędu krytycznego), które traktowane będą jako przyjęte odpowiednio w chwili zarejestrowania zgłoszenia przez Zamawiającego w ww. aplikacji lub dokonania zgłoszenia telefonicznie lub wysłania zgłoszenia za pomocą poczty elektronicznej na wskazany adres e-mail, 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. Zapewnienie w ramach serwisu oprogramowania (w limicie dni serwisowych):
* dostarczenia i wdrożenia nowych wersji (Unowocześnienia lub Aktualizacji) Szpitalnego Systemu Informatycznego (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 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 08:00 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.
4. **Wymagane funkcjonalności dostarczanego oprogramowania**

Dostawa i wdrożenie ZSI obejmuje dostawę licencji oprogramowania w zakresie poniższych modułów i funkcjonalności, bądź w odniesieniu do aplikacji obecnie eksploatowanych rozszerzenie przedmiotu/ilości licencji. Wszystkie wymienione w niniejszym punkcie moduły i ich funkcjonalności oraz te które zostaną zaktualizowane do najnowszej wersji oprogramowania muszą zostać objęte usługami wdrożeniowymi oraz opieką serwisową.

|  |  |
| --- | --- |
| **Lp.** | **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:  |
|  | * eksportowanie, importowanie, przenoszenie, duplikowanie schematów uprawnień
 |
|  | * kopiowanie schematów uprawnień z jednego pracownika na innego pracownika
 |
|  | * raportowanie różnic pomiędzy poszczególnymi schematami
 |
|  | * ręczne zablokowanie konta użytkownika przez administratora
 |
|  | * ewidencję daty zablokowania konta w przyszłości, z zapewnieniem automatycznego zablokowania kontra przez system po upływie wprowadzonej daty
 |
|  | * 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. |
|  | 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. |

|  |
| --- |
| 1. **Transport Medyczny**
 |
| **Lp.** | **Opis wymagań** |
| **Wymagania ogólne** |
|  | Możliwość rejestracji zleceń transportu medycznego pacjentów.  |
|  | Zarządzanie listą zleceń na transport medyczny.  |
|  | Posiada możliwość wywołania formularzy pozwalających określić stopień niepełnosprawności pacjenta, pozycję przewozu, adresy, personel zaangażowany w transport.  |
|  | Integracja z pozostałymi modułami systemu medycznego.  |
| **Wymagania szczegółowe - słowniki** |
| 5. | Cele przewozu: 1. konieczność podjęcia natychmiastowego leczenia w innej placówce medycznej w trakcie hospitalizacji – transport bezpłatny,
2. potrzeba kontynuacji leczenia w trakcie hospitalizacji pacjenta przyjętego na leczenie szpitalne– transport bezpłatny,
3. dysfunkcja narządu ruchu uniemożliwiająca korzystanie ze środków transportu publicznego w celu przejazdu na leczenie, lub do miejsca pobytu np. pacjent lezący (nosze) – transport bezpłatny,
4. inne wyżej nie wymienione za zgodą Koordynatora/Ordynatora oddziału– transport bezpłatny; - transport krwi i jej składników– transport bezpłatny,
5. dysfunkcja narządu ruchu umożliwiająca samodzielne poruszanie się bez stałej pomocy innej osoby, ale wymaga przy korzystaniu ze środków transportu publicznego pomocy innej osoby lub środka transportu dostosowanego do potrzeb osób niepełnosprawnych, np. pacjent siedzący (wózek inwalidzki) – transport częściowo płatny 60%,
6. inne wyżej nie wymienione – pełnopłatne.
 |
| 6. | Podmiot zlecający: 1. jednostki medyczne Szpitala (wraz z właściwymi kodami MPK),
2. podmioty zewnętrzne (słownik do samodzielnej modyfikacji i uzupełniania).
 |
| 7. | Lekarz zlecający. |
| 8. | Pozycja transportu: 1. siedząca,
2. leżąca,
3. półleżąca,
4. chodząca.
 |
| 9. | Środki transportu: - typ pojazdu 1. marka pojazdu,
2. numer rejestracyjny,
3. typ ambulansu (T, P, N, S).
 |
| 10. | Kierowca: 1. imię i nazwisko,
2. numer telefonu.
 |
| 11. | Zespół wyjazdowy: 1. imię i nazwisko,
2. funkcja/rola.
 |
| 12. | Rozpoznanie ICD-10.  |
| 13. | Firma transportowa. |
| 14. | Pacjent: 1. imię i nazwisko,
2. PESEL,
3. adres zamieszkania.
 |
| 15. | Data i godzina realizacji transportu.  |
| 16. | Skąd.  |
| 17. | Dokąd.  |
| 18. | Numer zlecenia (numeracja wewnętrzna zleceń transportu w skali roku).  |
| 19. | Wydruk: 1. numer zlecenia,
2. dane pacjenta,
3. data i godzina realizacji transportu – skąd,
4. dokąd,
5. zespół medyczny,
6. rodzaj pojazdu,
7. typ,
8. cel przewozu (pola wyboru),
9. uwagi,
10. dane rozliczeniowe (pola wyboru).
 |
| 20. | Raporty:1. zliczające liczbę poszczególnych rodzajów transportu,
2. generowanie raportu wg rodzaju transportu,
3. generowanie raportu wg wybranego ambulansu,
4. generowanie raportu wg zespołu medycznego,
5. generowanie raportu zrealizowanych przewozów, wg MPK,
6. filtrowanie i sortowanie list wg daty realizacji, oddziałów zlecających, etc.
 |
| 21. | Monitorowanie realizacji: 1. stan realizacji,
2. etapy (zgłoszony, w trakcie realizacji, zrealizowany, zatwierdzony).
 |

|  |
| --- |
| 1. **eZWM**
 |
| **Lp.** | **Opis wymagań** |
|  | Możliwość wystawienia elektronicznego zapotrzebowania na wyrobu medyczne  |
|  | Możliwość anulowania elektronicznego zapotrzebowania na wyrobu medyczne |
|  | Możliwość otrzymania potwierdzenia on-line |
|  | Możliwość otrzymywania podpowiedzi dotyczącej dofinansowania przysługującego pacjentowi z powodu minimum wiek, niepełnosprawność |

|  |
| --- |
| 1. **Powiadomienia**
 |
| **Lp.** | **Opis wymagań** |
|  | Wysyłanie wiadomości testowych o dowolnej treści przez e-mail lub SMS. |
|  | Możliwość konfiguracji wiadomości o dowolnej treści z możliwością wykorzystania dowolnych informacji w bazie danych systemu HIS. |
|  | Możliwość konfiguracji dowolnych zdarzeń powodujących wysłanie wskazanych wiadomości (np. zdarzenie czasowe, akcja użytkownika, zdarzenie bazy danych). |
|  | Określanie terminu ważności wiadomości, po którym niewysłana wiadomość staje się nieważna. |
|  | Określanie zalecanego czasu wysłania wiadomości w postaci przedziału godzinowego. |
|  | Powiadomienia e-mail: |
|  | Obsługa wysyłania wiadomości e-mail przez wskazane konto i serwer SMTP. |
|  | Możliwość wysyłania plików jako załączniki do wiadomości e-mail. |
|  | Powiadomienia SMS: |
|  | Obsługa wysyłania wiadomości SMS z wykorzystaniem wybranego, internetowego dostawcy usług (np. Redlink, SMS Api, PLUS/Polkomtel). |
|  | Możliwość wysyłania wiadomości SMS z ustawianiem pola Sender ID (nazwa nadawcy zamiast numeru telefonu). |

|  |
| --- |
| 1. **APDILO**
 |
| **Lp.** | **Opis wymagań** |
| 1. | Moduł umożliwia przekazywanie danych o kartach onkologicznych do systemu AP-DILO prowadzonego przez Narodowy Fundusz Zdrowia. |
| 2. | Moduł umożliwia wyszukiwanie kart onkologicznych pacjenta w systemie AP-DILO i pobieranie informacji o tych kartach (w szczególności ich numery i etapy). |
| 3. | Moduł umożliwia zakładanie w systemie AP-DILO nowych kart onkologicznych wraz z pobraniem ich numerów. |
| 4. | Moduł pozwala na otwieranie i zamykanie etapów dla danych kart onkologicznych w systemie AP-DILO.  |
| 5. | Moduł pozwala na zamykanie karty onkologicznej w systemie AP-DILO. |
| 6. | Moduł pozwala na anulowanie karty onkologicznej w systemie AP-DILO. |
| 7. | Dane do systemu AP-DILO wysyłane są automatycznie w momencie wykonywania przez użytkownika odpowiednich czynności w systemie. |
| 8. | Przekazywanie informacji do systemu AP-DILO jest możliwe również jeżeli operacje są wykonywane przez użytkownika na komputerze, który nie ma dostępu do internetu. |
| 9. | Moduł zapewnia weryfikację kompletności danych przed wysłaniem do systemu AP-DILO. |
| 10. | Moduł zapewnia obsługę błędów podczas wysyłania informacji do systemu AP-DILO poprzez ponowienie próby wysłania i informowanie administratorów i/lub użytkowników o powtarzających się nieudanych próbach. |
| 11. | Moduł zapewnia komunikację z interfejsami AP-DILO w sposób bezpieczny i szyfrowany. |
| 12. | Moduł zarządza hasłami dostępu do systemu AP-DILO – pozwala na przesyłanie informacji za pomocą loginu i hasła użytkownika, który wykonał operację w systemie. |

|  |
| --- |
| 1. **KRN**
 |
| **Lp.** | **Opis wymagań** |
|  | Moduł musi umożliwiać definiowanie kart nowotworowych dla pacjentów przebywających na oddziałach i w poradniach. |
| 2. | Karty nowotworowe zapisane w module muszą zawierać wszystkie informacje wymagane przez Krajowy Rejestr Nowotworów. |
| 3. | Dane demograficzne pacjentów muszą być automatycznie przepisywane do karty nowotworowej bez potrzeby ich ponownego wprowadzania w systemie. |
| 4. | Moduł musi umożliwiać zlecenie przez użytkownika przesłania karty nowotworowej do Krajowego Rejestru Nowotworów za pomocą udostępnionych przez tę jednostkę interfejsów (webservice’ów). |
| 5. | Moduł musi sprawdzać kompletność wypełnionej karty oraz jej poprawność merytoryczną przed wysłaniem do Krajowego Rejestru Nowotworów. |
| 6. | Moduł musi zapewniać obsługę błędów podczas wysyłania karty nowotworowej do Krajowego Rejestru Nowotworów, w szczególności informowanie o nich administratorów systemu i/lub użytkowników zlecających wysłanie karty. |
| 7. | Moduł musi automatycznie odczytywać z Krajowego Rejestru Nowotworów za pomocą interfejsów informacje zwrotne (w szczególności status karty oraz jej numer) i udostępnia te dane w karcie nowotworowej w module. |
| 8. | Moduł musi pozwalać na zlecanie przesłania karty nowotworowej również na komputerach, które nie mają dostępu do Internetu. |
| 9. | Moduł musi zapewniać komunikację z interfejsem Krajowego Rejestru Nowotworów w sposób bezpieczny i szyfrowany. |
| 10. | Moduł musi zarządzać hasłami dostępu do interfejsu Krajowego Rejestru Nowotworów – pozwala na przesyłanie informacji za pomocą loginu i hasła lekarza, który zlecił wysłanie karty. |

|  |
| --- |
| 1. **Poczta**
 |
| **Lp.** | **Opis wymagań** |
| 1. | Wysyłanie i odbiór poczty wewnętrznej przez użytkowników systemu. |
|  | Możliwość wysyłania powiadomień do wielu odbiorców wybieranych wg: |
| 2. | * Modułu systemu,
 |
| 3. | * Jednostki organizacyjnej,
 |
| 4. | * Typu pracownika.
 |
|  | Ustawiany konfiguracyjnie sposób powiadomienia adresata o poczcie do odebrania : |
| 5. | * Komunikat ekranowy,
 |
| 6. | * komunikat w pasku statusu formularza,
 |
| 7. | * sygnał dźwiękowy,
 |
| 8. | * komunikat z możliwością bezpośredniego wejścia do skrzynki pocztowej.
 |
|  | Dodatkowe opcje dotyczące wysyłania wiadomości dla użytkowników administracyjnych: |
| 9. | * wymuszanie sposobu powiadomienia adresata,
 |
| 10. | * data aktywacji oraz termin ważności wiadomości,
 |
| 11. | * wymuszenia zamknięcia aplikacji na stacji odbiorcy.
 |
| 12. | Mechanizm automatycznego (jedno- lub wielokrotnego) generowania powiadomień wskutek modyfikacji określonych danych w bazie. |
| 13. | Możliwość umieszczania w wiadomościach systemowych, wysyłanych do użytkowników, przycisków prowadzących do wskazanych konfiguracyjnie formularzy. |
| 14. | Możliwość zastosowania jednej konfiguracji wiadomości automatycznej do generowania powiadomień różnych użytkowników przy różnych warunkach (np. zależnie od zmiany w danych bazowych). |
|  | Opcja zapisu konfiguracji wiadomości automatycznej: |
| 15. | * do pliku na dysku lokalnym,
 |
| 16. | * bezpośrednio do bazy.
 |
| 17. | Konfigurowalne treści powiadomień. |
| 18. | Mechanizmpowiadomieńsystemowychgenerowanychcykliczniezmożliwościąustaleniadowolnej częstotliwości sprawdzenia warunków wysłania wiadomości. |

**Rozbudowa posiadanego przez Zamawiającego systemu ERP:**

|  |
| --- |
| 1. **mPracownik**
 |
| **Lp.** | **Opis wymagań** |
| 1. | Aplikacja musi być wyposażona w dedykowany pulpit pracownika, dzięki któremu od razu po zalogowaniu ma on szybki dostęp do najważniejszych informacji o ostatnim wynagrodzeniu, wykorzystanych urlopach oraz wnioskach o absencję. |
| 2. | W obszarze kadr pracownik musi mieć wgląd do swoich pełnych danych, zdefiniowanych w systemie ERP. Dane dotyczyć mogą dowolnego, definiowalnego zakresu udostępnianych formatek danych z poziomu systemu ERP z obszaru zarządzania personelem. Mogą być to na przykład dane o zatrudnieniu, stażach, badaniach, czy dane płacowe. |
| 3. | Aplikacja musi umożliwiać podgląd dokumentów płacowych pracownika z możliwością przeglądania ich na liście z filtrowaniem wg przedziału czasu i wyszukiwaniem wg informacji nagłówkowych. Kliknięcie na dokumencie powinna otwierać jego szczegóły, czyli wykaz obliczonych składników płacowych. Ilość widocznych składników jest możliwa do skonfigurowania przez użytkownika w systemie ERP w obszarze zarządzanie personelem. |
| 4. | Aplikacja musi posiadać możliwość przekazania pracownikowi rocznego rozliczenia PIT i deklaracji IMIR w wersji PDF, wprost na urządzenie mobilne. Dostępna musi być również operacja potwierdzania odbioru przez pracownika i zapisywana tego faktu w systemie ERP. |
| 5. | Aplikacja musi mieć możliwość prezentacji bilansów urlopowych w aplikacji. Zakres rodzajów urlopów dostępnych w aplikacji musi być konfigurowalny przez pracowników Wykonawcy. |
| 6. | Aplikacja musi mieć możliwość wystawienia wniosku o absencję wg rodzajów zdefiniowanych w obszarze zarządzania personelem. Dokument taki musi trafić do jego przełożonego wg struktury organizacyjnej lub do osób uprawnionych do akceptacji według ustalonej przy pracowniku ścieżce w systemie ERP. W aplikacji muszą być obsługiwane wnioski rozliczane godzinowo. Aplikacja musi umożliwiać pracownikowi przegląd kalendarz swoich nieobecności. Aplikacja musi wyświetlać także historię obiegu każdego wniosku oraz umożliwiać wpisywanie komentarzy na każdym etapie akceptacji. |
| 7. | Aplikacja musi zapewnić wywiązanie się z jednego z podstawowych wymagań narzuconych przez nowe przepisy, mówiącego o dostępnie pracownika do jego danych osobowych przetwarzanych przez firmę oraz zgód i celów przetwarzania tych danych. Funkcjonalność musi pozwalać pracownik w czytelny sposób widzieć jego udzielone zgody wg określonych celów i czynności zgodnie z RODO.  |
| 8. | Aplikacja musi umożliwiać każdemu z pracowników, którzy otrzymali uprawnienia do akceptacji wniosków o absencję, oprócz standardowego, wyświetlać dodatkowy zestaw narzędzi pozwalających na obsługę procesu akceptacji wniosków. Przełożony musi mieć możliwość filtrowania listy oczekujących i obsłużonych wniosków swoich podwładnych oraz przeglądać szczegóły tych wniosków. Każdy wniosek oczekujący może zaakceptować, odrzucić lub zwrócić do pracownika w celu zmodyfikowania. Aplikacja musi mieć możliwość podglądu kalendarza z naniesionymi absencjami wszystkich podwładnych z możliwością przejścia do bilansu urlopowego danego pracownika. |
| 9. | Użytkownicy aplikacji musza mieć możliwość włączenia powiadomień push przekazywanych bezpośrednio na urządzenie mobilne oraz dodatkowo powiadomień e-mail, które informują użytkowników już w chwili zaistnienia zdarzenia, np. wprowadzenia czy zmiany stanu akceptacji wniosku. |
| 10. | Aplikacja musi umożliwiać swobodny dostęp do niej na osobistych urządzeniach mobilnych typu smartfon czy tablet (iOS, Android) lub komputerach i laptopach z systemem Windows 10\*, jednocześnie musi mieć możliwości uruchomienia na ogólnodostępnych kioskach (w postaci tabletów czy modułowych komputerów). Aplikacja działająca w trybie kiosku musi mieć możliwość włączenia mechanizmów dbających o prywatność, w tym niepozwalających na zapamiętywanie danych logowania i automatycznie wylogowywanie się użytkownika po ustalonym i widocznym dla pracownika czasie. |
| 11. | Bezpieczeństwo danych w aplikacji musi być zapewniony przez szereg mechanizmów ograniczających dostęp do aplikacji i danych w niej zawartych, w tym logowanie na indywidualne konta pracowników zabezpieczone hasłami, możliwość wykorzystania do logowania parametrów biometrycznych (odcisk palca lub skan twarzy) a także przekazywanie danych wyłącznie szyfrowanymi kanałami. |