*Załącznik nr 5 do SIWZ 20/2020*

|  |  |
| --- | --- |
|  | **Szczegółowy Opis Przedmiotu Zamówienia**Dostawa i uruchomienie sprzętu oraz oprogramowania w ramach projektu pn.: „Wdrożenie e-usług w Szpitalu Powiatowym im. Jana Pawła II w Bartoszycach” |

Spis treści

[Wstęp 3](#_Toc51663559)

[Ogólny zarys projektu 3](#_Toc51663560)

[Wymagania ogólne 3](#_Toc51663561)

[Etap I – Dostawa sprzętu i oprogramowania systemowego 4](#_Toc51663562)

[Serwery 4](#_Toc51663563)

[Macierz dyskowa 7](#_Toc51663564)

[Macierz NAS 13](#_Toc51663565)

[UPS 14](#_Toc51663566)

[Stacje robocze all in one 14](#_Toc51663567)

[Laptopy 17](#_Toc51663568)

[Tablety 20](#_Toc51663569)

[Drukarki 20](#_Toc51663570)

[Modernizacja infrastruktury teleinformatycznej 21](#_Toc51663571)

[Warunki ogólne 21](#_Toc51663572)

[Switch dostępowy 21](#_Toc51663573)

[Switch SAN 23](#_Toc51663574)

[AP 23](#_Toc51663575)

[Szafa 42U 29](#_Toc51663576)

[Firewall / UTM 29](#_Toc51663577)

[System analizy bezpieczeństwa 34](#_Toc51663578)

[Sejf ogniotrwały 36](#_Toc51663579)

[Licencje 36](#_Toc51663580)

[Migracja bazy danych systemu HIS oraz ERP użytkowanego przez Zamawiającego 37](#_Toc51663581)

[Organizacja prac migracyjnych 38](#_Toc51663582)

[Odbiór procesu migracji 46](#_Toc51663583)

[Przygotowanie i dostarczenie dokumentacji projektowej oraz powykonawczej 47](#_Toc51663584)

[Etap II – Adaptacja budowlana serwerowni 48](#_Toc51663585)

[Informacje ogólne 48](#_Toc51663586)

[Instalacja elementów w modernizowanej serwerowni zapasowej 48](#_Toc51663587)

[Etap III – Wdrożenie oprogramowania 54](#_Toc51663588)

[Przeszkolenie pracowników Zamawiającego z dostarczanych rozwiązań 89](#_Toc51663589)

[Gwarancja i wsparcie 89](#_Toc51663590)

# Wstęp

Niniejszy dokument stanowi Szczegółowy Opis Przedmiotu Zamówienia (dalej SzOPZ lub OPZ) w zakresie dostawy i wdrożenia sprzętu oraz oprogramowania służącego uruchomieniu i zabezpieczeniu działania e-Usług w Szpitalu. Wszystkie parametry techniczne określone w niniejszym OPZ określają minimalne lub maksymalne (zgodnie z opisem) wymagania stawiane oferowanym urządzeniom i oprogramowaniu.

## Ogólny zarys projektu

Celem projektu jest wdrożenie nowoczesnych i bezpiecznych e-Usług w Szpitalu. W tym celu wszystkie obecne i nowe systemy oraz usługi muszą zostać uruchomione w trybie wysokiej dostępności (HA). Aby sprostać temu wymogowi w Szpitalu zostaną zainstalowane nowe serwery bazodanowe z zabezpieczeniami.

Aby usługi elektroniczne świadczone były w sposób bezpieczny, serwerownia zostanie wyposażona w urządzenia typu UTM zabezpieczające ruch sieciowy pomiędzy pacjentami i placówką oraz gwarantującymi ciągłość dostępności e-Usług.

## Wymagania ogólne

Zamawiający wymaga, by dostarczone oprogramowanie było oprogramowaniem w wersji aktualnej na dzień jego instalacji (tzn. powinno być dostosowane do zmieniających się powszechnie obowiązujących przepisów prawa lub regulacji wewnętrznych Zamawiającego).

System musi być zbudowany w architekturze wysokiej dostępności (HA).

System musi umożliwiać definiowanie dowolnej ilości użytkowników.

System musi gwarantować integralność danych, bieżącą kontrolę poprawności wprowadzanych danych, spójność danych.

System musi pracować w środowisku sieciowym i posiadać wielodostępność pozwalającą na równoczesne korzystanie z bazy danych przez wielu użytkowników bez ograniczeń na ich liczbę.

System musi posiadać mechanizmy ochrony danych przed niepowołanym dostępem, nadawania uprawnień dla użytkowników do korzystania z modułów jak również do korzystania z wybranych funkcji.

Dla dostarczonego oprogramowania należy dostarczyć: licencje, nośniki instalacyjne, instrukcje użytkownika i administratora (w formie elektronicznej).

Dla dostarczonego oprogramowania należy dostarczyć: bezterminowe licencje użytkowe oraz subskrypcyjne okresowe [np. na aktualizację systemu zabezpieczeń] na min. okres zaoferowanej gwarancji na urządzenie na którym licencje są instalowane; nośniki instalacyjne, instrukcje.

**Minimalny okres gwarancji - 36 msc. - dotyczy wszystkich elementów systemu – o ile w specyfikacji i/lub ofercie nie wyszczególniono inaczej.**

# Etap I – Dostawa sprzętu i oprogramowania systemowego

Poniżej przedstawiono parametry minimalne jaki dostarczany sprzęt musi spełniać. W przypadku gdy w wariancie technologicznym wybranym przez Wykonawcę, do realizacji Przedmiotu Zamówienia wymagany jest sprzęt/oprogramowanie/licencje nieujęte w poniższym zestawieniu Wykonawca musi go dostarczyć i wykazać w wykazie asortymentowo-cenowym.

## Serwery

**Obudowa**

• Typu RACK, wysokość nie więcej niż 2U;

• Szyny umożliwiające wysunięcie serwera z szafy stelażowej;

• Ramię porządkujące ułożenie przewodów z tyłu serwera;

• Możliwość zainstalowania 8 dysków twardych hot plug, rozbudowa do 24 slotów na dyski;

• Zainstalowany wewnętrzy napęd DVD-RW;

• Zainstalowane 2 dyski SSD min. 480GB;

**Płyta główna**

• Dwuprocesorowa;

• Wyprodukowana i zaprojektowana przez producenta serwera

• Możliwość instalacji procesorów 28-rdzeniowych;

• Zainstalowany moduł TPM 2.0

• 6 złącz PCI Express generacji 3w tym:

o 3 fizyczne złącza o prędkości x16;

o 3 fizyczne złącza o prędkości x8;

o Możliwość rozbudowy do 8 aktywnych złącz PCIe

• 24 gniazda pamięci RAM;

• Obsługa minimum 3TB pamięci RAM;

• Wsparcie dla technologii:

o Memory Scrubbing

o SDDC

o Advanced ECC

o Rank Sparing;

• Obsługa pamięci nieulotnej instalowanej w gniazdach pamięci RAM o pojemności sumarycznej minimum 1TB (przez pamięć nieulotną rozumie się moduły pamięci zachowujące swój stan np. w przypadku nagłej awarii zasilania, nie dopuszcza się podtrzymania bateryjnego stanu pamięci)

• Minimum 2 sloty dla dysków M.2 na płycie głównej (lub dedykowanej karcie PCI Express) nie zajmujące klatek dla dysków hot-plug;

**Procesory**

• Jeden procesor min. 8-rdzeniowy[[1]](#footnote-2) w architekturze x86\_64

osiągający w teście SPEC CPU2017 Floating Point wynik SPECrate2017\_fp\_base minimum 93 pkt (wynik osiągnięty dla zainstalowanych dla dwóch procesorów). Wynik musi być opublikowany na stronie https://www.spec.org/cpu2017/results/rfp2017.html

**Pamięć RAM**

• min. 128 GB pamięci RAM

• DDR4 Registered, 2933Mhz

**Kontrolery LAN**

• Trwale zintegrowana karta LAN, nie zajmująca żadnego z dostępnych slotów PCI Express, wyposażona minimum w interfejsy: 2x 1Gbit Base-T ze wsparciem iSCSI oraz PXE boot;

• Zainstalowana karta LAN 2x 10Gbit Base-T, możliwość wymiany zainstalowanych interfejsów LAN na interfejsy 4x 10Gbit SFP+ bez potrzeby wymiany całego układu lub instalacji dodatkowych kart w slotach PCI Express;

**Kontrolery I/O**

• Zainstalowany kontroler RAID obsługujący poziomy 0, 1, 10, 5, 50

• Możliwość zainstalowania kontrolera RAID obsługującego dyski NVMe;

• Możliwość zainstalowania dwóch nośników flash o pojemności 64GB w konfiguracji RAID-1, rozwiązanie dedykowane dla hypervisora oraz niezajmujące zatok dla dysków hot-plug;

• Zainstalowana 2 portowa karta FC 16Gb

**Porty**

• Zintegrowana karta graficzna ze złączem VGA z tyłu i przodu serwera;

• 2 port USB 3.0 na panelu przednim;

• 1 port USB wewnętrzny;

• 2 porty USB 3.0 dostępne z tyłu serwera;

• Możliwość instalacji jednego portu serial, możliwość wykorzystania portu do zarządzania serwerem;

• Ilość dostępnych złącz USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express i/lub USB serwera;

**Zasilanie, chłodzenie**

• Redundantne zasilacze hotplug o sprawności 94% (klasa Platinum) o mocy min. 750W;

• Redundantne wentylatory hotplug;

**Zarządzanie**

• Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera - system przewidywania, rozpoznawania awarii

o informacja o statusie pracy (poprawny, przewidywana usterka lub usterka) następujących komponentów:

* karty rozszerzeń zainstalowane w dowolnym slocie PCI Express
* procesory CPU
* pamięć RAM z dokładnością umożliwiającą jednoznaczną identyfikację uszkodzonego modułu pamięci RAM
* wbudowany na płycie głównej nośnik pamięci M.2 SSD
* status karty zrządzającej serwera
* wentylatory
* bateria podtrzymująca ustawienia BIOS płyty główne
* zasilacze

o system przewidywania/rozpoznawania awarii musi być niezależny i działać w przypadku odłączenia kabli zasilających serwera (podtrzymywany kondensatorowo lub bateryjnie w celu uruchomienia przy odłączonym zasilaniu sieciowym).

Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach:

• Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera;

o Dedykowana karta LAN 1 Gb/s, dedykowane złącze RJ-45 do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym;

o Dostęp poprzez przeglądarkę Web, SSH;

o Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii;

o Zarządzanie alarmami (zdarzenia poprzez SNMP)

o Możliwość przejęcia konsoli tekstowej

o Możliwość zarządzania przez 6 administratorów jednocześnie

o Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (KVM)

o Obsługa serwerów proxy (z autentykacją)

o Obsługa VLAN

o Możliwość konfiguracji parametru Max. Transmission Unit (MTU)

o Wsparcie dla protokołu SSDP

o Obsługa protokołów TLS 1.0, TLS 1.1, TLS 1.2, SSL v3

o Obsługa protokołu LDAP

o Integracja z HP SIM

o Synchronizacja czasu poprzez protokół NTP

o Możliwość backupu i odtworzenia ustawień bios serwera oraz ustawień karty zarządzającej

• Oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (m.in. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna);

• Dedykowana, wbudowana w kartę zarządzającą (lub zainstalowana) pamięć flash o pojemności minimum 16 GB;

• Możliwość zdalnej reinstalacji systemu lub aplikacji z obrazów zainstalowanych w obrębie dedykowanej pamięci flash bez użytkowania zewnętrznych nośników lub kopiowania danych poprzez sieć LAN;

• Serwer posiada możliwość konfiguracji i wykonania aktualizacji BIOS, Firmware, sterowników serwera bezpośrednio z GUI (graficzny interfejs) karty zarządzającej serwera bez pośrednictwa innych nośników zewnętrznych i wewnętrznych poza obrębem karty zarządzającej.

**Wspierane systemy**

• Microsoft Windows Server 2019, 2016

• VMWare vSphere 6.7

• Suse Linux Enterprise Server 12

• Red Hat Enterprise Linux 7, 8

• Hyper-V Server

Zainstalowany system operacyjny wspierany przez producenta systemu bazodanowego Oracle[[2]](#footnote-3) oraz posiadający natywne wsparcie dla wirtualizacji.

**Gwarancja**

• gwarancja producenta serwera w miejscu instalacji z gwarantowaną skuteczną naprawą do końca następnego dnia od zgłoszenia. Naprawa realizowana przez producenta serwera lub autoryzowany serwis.

• Zgłaszanie usterek i awarii sprzętowych poprzez automatyczne założenie zgłoszenia w systemie helpdesk/servicedesk producenta sprzętu;

• Firma serwisująca musi posiadać certyfikat lub inny dokument zezwalający na świadczenie usług serwisowych;

• Bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanego serwera – jeżeli funkcjonalność ta wymaga dodatkowego serwisu lub licencji producenta serwera, takowy element musi być uwzględniona w ofercie;

• Możliwość odpłatnego wydłużenia gwarancji producenta do 7 lat z gwarantowanym skutecznym zakończeniem naprawy serwera najpóźniej w następnym dniu roboczym od zgłoszenia usterki;

**Inne wymagania**

• Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA;

• Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w UE;

• Ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera, w ofercie należy podać link do strony producenta na której znajduje się nr telefonu oraz maila na który można zgłaszać usterki;

• W czasie obowiązywania gwarancji na sprzęt, możliwość po podaniu na infolinii numeru seryjnego urządzenia weryfikacji pierwotnej konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji;

• Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera;

## Macierz dyskowa

System musi być dostarczony ze wszystkimi komponentami do instalacji w standardowej szafie rack 19” z zajętością maks. 2U (na urządzenie) w tej szafie. Każdy skonfigurowany moduł/obudowa musi posiadać układ nadmiarowy zasilania i chłodzenia, zapewniający bezprzerwową pracę macierzy bez ograniczeń czasowych w przypadku utraty redundancji w danym układzie (zasilania lub chłodzenia). Każdy moduł/obudowa powinien posiadać widoczne elementy sygnalizacyjne do informowania o stanie poprawnej pracy lub awarii. Rozbudowa o dodatkowe moduły dla obsługiwanych dysków powinna odbywać się wyłącznie poprzez zakup takich modułów, bez konieczności zakupu dodatkowych licencji lub specjalnego oprogramowania aktywującego proces rozbudowy lub musi być dostarczona licencja na dwukrotność dostarczanej pojemności. Dostarczana macierz musi umożliwiać takie podłączenie półek aby awaria lub/i usunięcie jednej z półek nie powodowało utraty dostępu do danych znajdujących się na pozostałych modułach. Oferowana macierz musi obsługiwać min. 260 dysków wykonanych w technologii hot-plug. Wszystkie zainstalowane dyski hot-plug, z wyłączeniem dysków SSD stosowanych jako rozszerzenie pamięci Cache kontrolerów, muszą być dostępne dla zapisu danych Użytkownika. Macierz musi umożliwiać rozbudowę i jednoczesne podłączenie i używanie modułów (tzw. „półek dyskowych”) w rozmiarze 2U pozwalająca umieścić do 24 dysków 2,5” typu hotplug dla dysków NL-SAS SAS i SSD oraz w rozmiarze 2U dla 12 dysków 3,5” typu hotplug SAS, NL-SAS,SSD oraz 3U/4U dla 60 dysków typu hotplug SAS, NL-SAS, SSD-SAS; Wymaga się aby macierz umożliwiała jednoczesne podłączenie i użycie dowolnego rodzaju i kombinacji wyżej wymienionych półek dyskowych.

**Pojemność macierzy:**

Pojemność użyteczna, dostępna dla hostów:

22 TB realizowana na dyskach SAS 10 000 rpm 12G (minimum 2 x RAID-5 + Hot-spare)

**Kontrolery**

* Kontrolery macierzy muszą obsługiwać tryb pracy w układzie active-active lub mesh-active, macierz musi być dostarczona z zainstalowanymi minimum 2 kontrolerami;
* Każdy z kontrolerów macierzy musi posiadać po minimum 64 GB pamięci podręcznej Cache – kontrolery muszą obsługiwać między sobą mechanizm lustrzanej kopii danych (cache mirror) przeznaczonych do zapisu;
* Macierz musi obsługiwać rozbudowę pamięci podręcznej cache dla operacji odczytu o minimum 800GB poprzez instalację dodatkowych modułów pamięci w kontrolerach lub wykorzystanie pojemności zainstalowanych dysków SSD,
* W przypadku awarii zasilania dane nie zapisane na dyski, przechowywane w pamięci podręcznej Cache dla zapisów muszą być zabezpieczone metodą trwałego zapisu na dysk.
* Kontrolery muszą posiadać możliwość ich wymiany bez konieczności wyłączania zasilania całego urządzenia;
* Kontrolery macierzy obsługują funkcjonalność kompresji danych.
* Kontrolery macierzy obsługują funkcjonalność deduplikacji w trybie in-line.
* Macierz musi obsługiwać wymianę kontrolera RAID bez utraty danych zapisanych na dyskach.
* Każdy z kontrolerów RAID powinien posiadać dedykowany minimum 2 interfejsy RJ-45 Ethernet obsługujący połączenia z prędkością minimum 1Gb/s dla zdalnej komunikacji z oprogramowaniem zarządzającym i konfiguracyjnym macierzy.
* Kontrolery macierzy muszą być oparte o procesor wykonany w technologii wielordzeniowej z minimum 4 rdzeniami,
* Kontrolery macierzy muszą obsługiwać do 130 grup dyskowych w całym rozwiązaniu, bez konieczności wymiany dostarczonych kontrolerów
* Oferowana macierz musi mieć wyprowadzone 2 porty FC 16Gb/s do dołączenia serwerów bezpośrednio lub do dołączenia do sieci SAN, na każdy kontroler RAID.
* Macierz musi umożliwiać dołożenie dodatkowych portów do transmisji danych:
	+ 4 x FC 16Gb/s,
	+ 2 x FC 16Gb/s,
	+ 2 x FC 32Gb/s,
	+ 2 x iSCSI 1Gb/s,
	+ 2 x iSCSI 10Gb/s,
	+ 2 x SAS 12GB/s
* Dołożenie portów jw. nie może powodować wymiany samych kontrolerów RAID w oferowanym rozwiązaniu a w przypadku konieczność licencjonowania tej funkcjonalności macierz ma być dostarczona z aktywną licencja na instalację i obsługę każdego z wymienionych protokołów transmisji danych
* Macierz musi umożliwiać wymianę portów do transmisji danych obsługujących protokoły: FC 32Gb/s, iSCSI 1Gb/s, iSCSI 10Gb/s, SAS 12GB/s
* Wymiana portów jw. nie może powodować wymiany samych kontrolerów RAID w oferowanym rozwiązaniu a w przypadku konieczność licencjonowania tej funkcjonalności macierz ma być dostarczona z aktywną licencja na instalację i obsługę każdego z wymienionych protokołów transmisji danych
* Macierz posiada obsługę operacji plikowych I/O w sieci NAS w obrębie zainstalowanych kontrolerów. Protokoły dostępu: CIFS, NFS. W przypadku obsługi protokołów CIFS i NFS wymagana jest funkcjonalność agregacji przepustowości dla interfejsów dedykowanych do obsługi tych protokołów. Obsługa protokołów CIFS i NFS musi odbywać się jednocześnie . – nie jest wymagane dostarczenie tej funkcjonalności – opcja rozbudowy

**Poziomy RAID**

* Macierz musi zapewniać poziom zabezpieczenia danych na dyskach definiowany poziomami RAID: 0, 1, 10, 5, 50, 6.

**Dyski**

* Oferowana macierz musi wspierać dyski hot-plug:
	+ dyski elektroniczne SSD i mechaniczne HDD z interfejsami SAS12Gb/s
	+ dyski mechaniczne HDD o prędkości obrotowej 7,2k rpm, 10k rpm oraz 15k rpm,
* Macierz musi obsługiwać mieszaną konfigurację dysków hot-plug SSD i HDD w rozmiarach 2,5” i 3,5” zainstalowanych w dowolnym module rozwiązania;
* Wszystkie dyski wspierane przez oferowany model macierzy muszą być wykonane w technologii hot-plug i posiadać podwójne porty SAS obsługujące tryb pracy full-duplex
* Macierz musi obsługiwać min. 260 dysków SAS SSD w całym rozwiązaniu, bez konieczności dokupowania/wymiany żadnych innych elementów sprzętowych czy licencyjnych innych niż same półki dyskowe wraz z dyskami;
* Możliwość rozbudowy oferowanego modelu macierzy do minimum 520 dysków bez migracji i przenoszenia danych - jedynie poprzez wymianę modułu kontrolerów macierzy (bez konieczności wymiany posiadanych dysków, półek dyskowych, bez konieczności przenoszenia danych/ istniejącej struktury grup dyskowych/LUN, jak również z zachowaniem istniejącej gwarancji producenta na półki dyskowe i dyski;
* Macierz musi umożliwiać skonfigurowanie każdego zainstalowanego dysku hot-plug jako dysk hot-spare (dysk zapasowy)
	+ Macierz posiada możliwość konfiguracji dysku hot-spare dla zabezpieczenia dowolnej grupy dyskowej RAID
	+ Macierz posiada możliwość konfiguracji dysku hot-spare dedykowanego dla zabezpieczenia tylko wybranej grupy dyskowej RAID
* W przypadku awarii dysku fizycznego i wykorzystania wcześniej skonfigurowanego dysku zapasowego wymiana uszkodzonego dysku na sprawny nie może powodować powrotnego kopiowania danych z dysku hot-spare na wymieniony dysk (tzw. CopyBackLess).
* Macierz musi pozwalać na zaszyfrowanie danych zapisanych na wszystkich obsługiwanych dyskach SSD-SAS i HDD-SAS/NL-SAS minimum kluczem AES256-bit – jeżeli w tym celu niezbędne jest zakupienie dodatkowych licencji bądź komponentów sprzętowych to należy je dostarczyć wraz z macierzą.

**Opcje programowe**

* Macierz musi być wyposażona w system kopii migawkowych umożliwiających wykonanie minimum 2000 kopii migawkowych
* Macierz musi umożliwiać zdefiniowanie min. 5000 woluminów (LUN)
* Macierz powinna umożliwiać podłączenie logiczne z serwerami i stacjami poprzez min. 1024 ścieżek logicznych FC
* Macierz musi umożliwiać aktualizację oprogramowania wewnętrznego kontrolerów RAID i dysków bez konieczności wyłączania macierzy oraz bez konieczności wyłączania ścieżek logicznych FC/iSCSI dla podłączonych stacji/serwerów
* Macierz musi umożliwiać dokonywanie w trybie on-line (tj. bez wyłączania zasilania i bez przerywania przetwarzania danych w macierzy) operacje: powiększanie grup dyskowych, zwiększanie rozmiaru woluminu, migrowanie woluminu na inną grupę dyskową
* Macierz musi posiadać wsparcie dla systemów operacyjnych : Microsoft Windows Server 2012R2, 2016, 2019, SuSE Linux Enterprise Server, Red Hat Linux Enterprise Server, HP-UNIX, IBM AIX, SUN Solaris, Vmware Vsphere;
* Macierz musi być dostarczona z licencją na oprogramowanie wspierające technologię typu multipath (obsługa nadmiarowości dla ścieżek transmisji danych pomiędzy macierzą i serwerem) dla połączeń FC i iSCSI.
* Macierz musi posiadać możliwość uruchamiania mechanizmów zdalnej replikacji danych, w trybie synchronicznym i asynchronicznym, po protokołach FC oraz iSCSI, bez konieczności stosowania zewnętrznych urządzeń konwersji wymienionych protokołów transmisji. Funkcjonalność replikacji danych musi być zapewniona z poziomu oprogramowania wewnętrznego macierzy, jako tzw. storage-based data replication. Replikacja danych musi być obsługiwana w połączeniu z każdą macierzą z tej samej rodziny urządzeń wspierającą obsługę zdalnej replikacji danych.
* Macierz musi posiadać możliwość tworzenia lokalnych tj. w obrębie zasobów macierzy, pełnych kopii danych (tzw. klony danych), kopii przyrostowych oraz kopii lustrzanych (mirror) – nie jest wymagane dostarczenie tej funkcjonalności – opcja rozbudowy;
* Macierz musi obsługiwać mechanizm ochrony priorytetów obsługi wybranych zasobów – za taki mechanizm uznaje się funkcję typu ‘cache partitioning’ lub ‘storage partitioning’.
* Macierz musi obsługiwać adresację IP v.4 i IP v.6
* Wraz z macierzą należy dostarczyć oprogramowanie lub moduły programowe typu plug-in pozwalające na integracje macierzy w środowiskach Vmware w zakresie obsługi mechanizmów: Vmware VAAI, Vmware VVOL, Vmware MultiPath IO – z subskrypcją do bezpłatnej aktualizacji w całym okresie obowiązywania gwarancji
* Macierz musi obsługiwać mechanizmy Thin Provisioning, czyli przydziału dla obsługiwanych środowisk woluminów logicznych o sumarycznej pojemności większej od sumy pojemności dysków fizycznych zainstalowanych w macierzy.
* Macierz musi obsługiwać mechanizmy typu AST (Automated Storage Tiering) tj. automatycznego migrowania i realokacji bloków danych pomiędzy różnymi technologiami dyskowymi na podstawie analizy częstotliwości operacji I/O dla tych bloków oraz wg potrzeb wydajnościowych serwerów, środowisk i aplikacji korzystających z zasobów macierzy. Mechanizm AST musi być obsługiwany przy korzystaniu zarówno z trzech jak z dwóch dostarczonych technologii dyskowych: SSD, SSAS, NLSAS. Macierz musi pozwalać na definiowanie różnych polityk i zasad migrowania danych w obrębie tej samej macierzy. Mechanizm AST musi być obsługiwać funkcję Quality-of-Services pozwalająca na zagwarantowaniu wydajności dla wybranych zasobów macierzy (woluminów) mierzonej jako maksymalny czas opóźnień operacji I/O wykonywanych przez serwer/środowisko/aplikację. Mechanizm AST musi pozwalać na definiowanie okna czasowego dla zbierania pomiarów wydajności operacji I/O oraz okna czasowego dla migrowania danych wg ustalonych zasad i polityk – minimalny definiowany czas trwania w/w operacji (długość okna czasowego) nie może być dłuższy niż 4 godziny. Mechanizm AST musi pozwalać na wykluczanie wybranych godzin i dni z pomiarów wydajności operacji I/O. – nie jest wymagane dostarczenie tej funkcjonalności – opcja rozbudowy
* Macierz musi wspierać usługi VSS (Volume ShadowCopy Services) w systemach klasy Microsoft Windows Sever – wymagane jest dostarczenie niezbędnego oprogramowania / sterowników VSS pozwalających na obsługę VSS przy maksymalnej pojemności i liczbie dysków obsługiwanych przez oferowaną. W czasie trwania gwarancji wymaga się bezpłatnego dostępu do nowych wersji oprogramowania i sterowników
* Macierz musi obsługiwać mechanizmy migracji danych w trybie online z innej macierzy tej klasy, z zachowaniem obsługi operacji I/O dla serwerów podłączonych do migrowanej macierzy tj. do migrowanych zasobów LUN
* Macierz musi wspierać rozwiązania klasy ‘klastra macierzowego’ tj. zapewnienia wysokiej dostępności zasobów dyskowych macierzy dla podłączonych platform software’owych i sprzętowych z wykorzystaniem synchronicznej replikacji danych pomiędzy minimum 2 macierzami protokołami FC oraz iSCSI. Mechanizm klastra macierzowego musi być obsługiwany dla protokołów FC oraz iSCSI, zarówno w zakresie replikacji danych jak i w zakresie sposobu podłączenia serwerów do zasobów macierzy. Pod użytym pojęciem ‘wysoka dostępność zasobów dyskowych’ należy rozumieć zapewnienie bezprzerwowego działania środowiska (aplikacja/ system operacyjny/ serwer) podłączonego do macierzy (macierz podstawowa) w przypadku wystąpienia awarii logicznego połączenia z tą macierzy bądź awarii samej macierzą, powodujących dla danego środowiska brak dostępu do zasobów macierzy podstawowej. Funkcjonalność ‘klastra macierzowego’ musi pozwalać na automatyczne i ręczne przełączanie obsługi środowisk produkcyjnych z macierzy podstawowej na zapasową w przypadku awarii macierzy podstawowej (tzw. Automated/manual failover). – nie jest wymagane dostarczenie tej funkcjonalności – opcja rozbudowy
* Macierz w dostarczonej konfiguracji musi obsługiwać deduplikację i kompresję danych na dyskach wbudowanych w macierzy (nie dopuszcza się główek, kompresji zewnętrznej, programowej itp.) w następujących trybach równocześnie oraz niezależnie na poziomie każdego LUN:
	+ Sama deduplikacja wybranego LUN;
	+ Sama kompresja wybranego LUN;
	+ Kombinacja technologii kompresji i deduplikacji wybranego LUN;
	+ Brak użycia technologii kompresji i deduplikacji dla wybranego LUN;

**Zarządzanie**

* Oprogramowanie do zarządzania musi być zintegrowane z systemem operacyjnym systemu pamięci masowej
* Komunikacja z wbudowanym oprogramowaniem zarządzającym macierzą musi być możliwa w trybie graficznym np. poprzez przeglądarkę WWW oraz w trybie tekstowym.
* Musi być możliwe zdalne zarządzanie macierzą z wykorzystaniem standardowej przeglądarki internetowej (np. Internet Explorer, Google Chrome, Mozilla Firefox) bez konieczności instalacji żadnych dodatkowych aplikacji na stacji administratora
* Wbudowane oprogramowanie macierzy musi obsługiwać połączenia z modułem zarządzania macierzy poprzez szyfrowanie komunikacji protokołami: SSL dla komunikacji poprzez przeglądarkę WWW i protokołem SSH dla komunikacji poprzez CLI

**Gwarancja i serwis**

* Całe rozwiązanie musi być objęte zaoferowanym okresem gwarancji z naprawą w miejscu instalacji urządzenia i z gwarantowanym czasem skutecznego zakończenia naprawy najpóźniej w ciągu następnego dnia roboczego od dnia zgłoszenia awarii do organizacji serwisowej producenta macierzy.
* Dyski twarde nie podlegają zwrotowi organizacji serwisowej;
* Serwis gwarancyjny musi obejmować dostęp do poprawek i nowych wersji oprogramowania wbudowanego, które są elementem zamówienia.
* Po zakończeniu okresu gwarancji musi być zapewniony przez producenta rozwiązania bezpłatny dostęp do aktualizacji oprogramowania wewnętrznego oferowanej macierzy oraz do kolejnych wersji oprogramowania zarządzającego w okresie minimum 2 lat.
* System musi zapewniać możliwość samodzielnego i automatycznego powiadamiania producenta i administratorów Zamawiającego o usterkach za pomocą wiadomości wysyłanych poprzez szyfrowany protokół. Funkcjonalność musi pozwalać na automatyczne otwarcie zgłoszenia serwisowego w bazie serwisowej producenta macierzy zgodnie z wymaganym w specyfikacji poziomem SLA; Opcja ta musi być dostępna bezpłatnie w trakcie całego okresu gwarancji producenta macierzy. Oferowana funkcjonalność musi również umożliwiać konfigurację i uruchomienie zdalnego dostępu do macierzy bezpośrednio przez Producenta – musi być do tego wykorzystany dedykowany system serwisowy macierzy.
* Macierz musi pochodzić z oficjalnego kanału sprzedaży producenta w UE. Nie dopuszcza się użycia macierzy odnawianych, demonstracyjnych lub powystawowych
* Urządzenie musi być wykonane zgodnie z europejskimi dyrektywami RoHS i WEEE stanowiącymi o unikaniu i ograniczaniu stosowania substancji szkodliwych dla zdrowia
* Możliwość odpłatnego wydłużenia gwarancji producenta do 7 lat w trybie onsite z gwarantowanym skutecznym zakończeniem naprawy serwera najpóźniej w następnym dniu roboczym od zgłoszenia usterki (podać koszt na dzień składania oferty);

Producent oferowanej macierzy musi posiadać dedykowaną, ogólnie dostępną stronę internetową, gdzie po wpisaniu numeru seryjnego macierzy można zweryfikować co najmniej: czas i poziom oferowanego serwisu gwarancyjnego producenta zarówno dla macierzy jak i dowolnej z półek dyskowych, datę zakończenia wsparcia gwarancyjnego, datę zakończenia wsparcia producenta dla oferowanego urządzenia.

## Macierz NAS

|  |  |
| --- | --- |
| Parametr | Wymagania minimalne |
| Procesor | Min. 4 rdzeniowy |
| Obudowa | Rack max. 2U |
| Pamięć RAM | 4 GB RAM – możliwość rozszerzenia do 16 GB |
| Ilość obsługiwanych dysków | 4 dyski SATA III o maksymalnej pojemności 16TB każdy,Zamontowane dyski o łącznej pojemności 20TB |
| Interfejsy sieciowe | 4 x Gigabit (10/100/1000)1 x 10Gb RJ45 (10G/5G/2.5G/1G/100M) |
| Porty | 2 x USB 3.0, 3 x USB 2.0, gniazdo PCIe 2.0 x4 (preinstalowana karta 10G) |
| Obsługa RAID | Pojedynczy dysk, JBOD, RAID 0,1,5,5+Spare,6,6+Spare,10,10+Spare. Obsługa BITMAP w celu przyspieszenia odbudowy. Możliwość skonfigurowania Global Spare Disk. |
| Funkcje RAID | Możliwość zwiększania pojemności i migracja między poziomami RAID online. |
| System Operacyjny | Windows 10, Server 2016, Apple Mac OS X, Linux |
| Stacja monitoringu | Obsługa kamer IP min. 4 licencje w zestawie z urządzeniem |
| Protokoły | CIFS, NFS, FTP, WebDAV, iSCSI, SSH, SNMP |
| Usługi | Serwer pocztowy, Stacja monitoringu, Windows ACL, Integracja w Windows ADS, Serwer wydruku, Serwer WWW, Serwer plików, Manager plików przez WWW, Obsługa paczek QPKG, Montowanie obrazów ISO, Replikacja w czasie rzeczywistym, Serwer RADIUS, Klient LDAP, Serwer Syslog, Serwer Proxy, Serwer VPN |
| Wirtualizacja | Możliwość podłączenia do Vmware, Citrix lub Hyper-V, możliwość uruchomienia maszyn wirtualnych bezpośrednio na macierzy bez konieczność posiadania zewnętrznych wirtualizatorów |
| Szyfrowanie | Szyfrowanie ze wsparciem sprzętowym AES-NI całych woluminów lub tylko wybranych udziałów sieciowych |
| iSCSI | Wbudowany inicjator i target iSCSI |
| Replikacja | Replikacja między urządzeniami w czasie rzeczywistym |
| Kontroler domeny | Możliwość podłączenia do kontrolera domeny Microsoft lub uruchomienie kontrolera domeny na bazie SAMBA 4  |
| Liczba iSCSI Target/LUN | Do 256 |
| Liczba udziałów | 512 |
| Liczba jednoczesnych połączeń | Min. 500 |
| Zasilanie | 250W +/- 10% |
| UPS  | Obsługa sieciowych awaryjnych zasilaczy UPS. |

## UPS

Zasilacz UPS do serwerowni - wraz z wymaganymi bateriami i osprzętem:

* elementy umożliwiające montaż w szafie RACK
* zajętość w szafie RACK nie więcej niż 3U
* moc pozorna 3kVA
* moc rzeczywista 2,7 kW
* technologia on-line
* podtrzymanie min. 3 minuty przy 100% obciążeniu; 11 minut przy 50% obciążeniu
* wyjścia: 8x IEC 320 C13 (10A)
* 1x RJ45
* aplikacja do automatycznego zamykania wspieranych systemów operacyjnych w przypadku braku zasilania
* wspierane i certyfikowane systemy operacyjne: Microsoft Windows Server, SUSE Linux Enterprise Server, Red Hat Enterprise Linux, VMware Infrastructure
* zarządzanie przez SNMP
* automatyczny wewnętrzny bypass
* bezprzerwowa wymiana baterii
* możliwość dołączenia baterii wydłużających czas podtrzymania zasilania
* wyświetlacz LCD na froncie urządzenia, umożliwiający zarządzanie i monitoring urządzenia
* certyfikaty: CE, CB
* gwarancja „door-to-door.

## Stacje robocze all in one

* Typ: Komputer AIO. W ofercie wymagane jest podanie modelu, symbolu oraz producenta
* Zastosowanie: Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do Internetu oraz poczty elektronicznej,
* Wydajność obliczeniowa: Procesor, który powinien osiągać w teście wydajności PassMark PerformanceTest (wynik dostępny: http://www.passmark.com/products/pt.htm) co najmniej wynik 10000 punktów Passmark CPU Mark.
* Pamięć operacyjna: 8GB 2933 MHz
* Parametry pamięci masowej: Min. 512 GB SSD NVMe zawierający partycję RECOVERY umożliwiającą odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii bez dodatkowych nośników.
* Zintegrowana karta graficzna wykorzystująca pamięć RAM systemu dynamicznie przydzielaną na potrzeby grafiki w trybie UMA. Obsługująca funkcje:

- 4K przy 60Hz

- DirectX

- Częstotliwość podstawowa układu graficznego 350 MHz (+/- 10%)

* Sprzętowe wsparcie technologii wirtualizacji procesorów, pamięci i urządzeń I/O realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji.
* Wyposażenie multimedialne: Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition Audio. Obudowa wyposażona we wbudowane głośniki stereo.
* Obudowa
	+ Typu AIO wyposażona w min. 1x kieszeń 2,5 cala na dyski SATA .
	+ Wbudowany zasilacz o mocy 190 W (+/- 10%) pracujący w sieci 230V 50/60Hz prądu zmiennego i efektywności min. 93%.
	+ Obudowa musi mieć możliwość zabezpieczenia wnętrza komputera oraz wszystkich slotów znajdujących się z tyłu obudowy przed niepowołanym odstępem za pomocą kłódki lub linki typu Kensington.
* Ergonomia:
	+ Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej, która może blokować również dostęp do wnętrza komputera poprzez blokowanie klap serwisowych.
	+ Ciężar komputera nie powinien przekraczać 12 kg.
* Wymagania dodatkowe
	+ Licencja na zainstalowany system operacyjny 64 bit niewymagający aktywacji za pomocą telefonu lub Internetu u producenta. Graficzny system operacyjny umożliwiający uruchomienie systemów Zamawiającego (m.in.:CGM Clininet, CGM ERP, Płatnik) bez użycia wirtualizacji w wersji pozwalającej na zarządzanie systemem za pomocą systemu domeny i przeznaczonej do zastosowań biznesowych.
	+ Dodatkowe oprogramowanie:
		- darmowy program pozwalający na w pełni automatyczną instalację sterowników urządzeń opartą o automatyczną detekcję posiadanego sprzętu;
		- rozszerzenie licencji na posiadany przez Zamawiającego program antywirusowy Nod32
	+ Wbudowane porty minimalnie:
	- 1 x Display Port 1.2

- 2x PS/2

- 1 x RJ-45
- 1 x Audio: line-in/microphone
- 1 x Audio: line-out/headphone

- 1 x Audio front
- 2x USB 3 oraz USB-C z przodu obudowy

- 3x USB 2 oraz 1x USB 3 z tyłu obudowy
Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp.

* + Port sieci LAN 10/100/1000 Ethernet RJ 45 zintegrowany z płytą główną.
	+ Zintegrowany z płytą główną dedykowany układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego.
	+ Minimum 2 złącza DIMM z obsługą do 64 GB DDR4 pamięci RAM.
	+ Min. 2 złącza SATA NCQ AHCI w tym minimum 1 złącze SATA III 6 Gb/s.
	+ Minimum dwa złącza M.2 w tym co najmniej jedno umożliwiające instalację dysków M.2 PCIe NVMe;
	+ Minimum jednak zatoka 5,25 cala (dopuszcza się zatokę na napędy typu SLIM) umożliwiająca instalację napędu optycznego. Zainstalowany napęd DVD-RW.
	+ Specyfikacja wbudowanego ekranu::
		- Typ ekranu: Panoramiczny, matryca o rozmiarze 23,8 cala
		- Jasność: 250 cd/m2
		- Kąty widzenia: 178°/178° CR10:1
		- Czas reakcji matrycy: maks. 14 ms
		- Rozdzielczość maksymalna: 1920 x 1080
		- Możliwość co najmniej 4-stopniowej regulacji wysokości ekranu w zakresie co najmniej 110 mm;
		- Możliwość obracania ekranu na boki w zakresie co najmniej 340°
		- Zakres pochylenia monitora: Od 0° do +20°
		- Konstrukcja komputera powinna umożliwić demontaż stopy ekranu i powieszenie komputera np. za pomocą standardowego złącza VESA
	+ Klawiatura i mysz wyprodukowana przez producenta komputera
	+ Zintegrowana z obudową monitora kamera
	+ Zintegrowany mikrofon stereo cyfrowy
* Normy i standardy
	+ Komputery mają spełniać normy i posiadać deklaracje zgodności (lub inne dokumenty potwierdzające spełnienie norm) w zakresie:
		- Deklaracja zgodności CE
		- Być wykonane/wyprodukowane w systemie zapewnienia jakości ISO 9001 lub innym równoważnym systemie jakości.
* Gwarancja producenta:
	+ świadczona w siedzibie Zamawiającego, przyjazd certyfikowanego przez producenta serwisanta do końca następnego dnia roboczego, chyba że niezbędne będzie naprawa sprzętu w siedzibie producenta ,lub autoryzowanym przez niego punkcie serwisowym - wówczas koszt transportu do i z naprawy pokrywa Wykonawca,
	+ Naprawy gwarancyjne urządzeń musi być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta,
* Wsparcie techniczne producenta
	+ Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej komputera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.
	+ Dostęp do najnowszych sterowników i uaktualnień na stronie producenta zestawu realizowany poprzez podanie na dedykowanej stronie internetowej producenta numeru seryjnego lub modelu komputera.

**UWAGA: Wykonawca zainstaluje komputery zgodnie z załącznikiem nr 1 do OPZ. Jeśli Wykonawca oceni, że w wyznaczonych miejscach infrastruktura sieciowa jest nie wystarczająca, należy dokonać modyfikacji sieci LAN poprzez instalację dodatkowych gniazdek sieciowych i przyłączenie ich do najbliższego punktu dystrybucyjnego.**

## Laptopy

**Zastosowanie**

Komputer przenośny, który będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do Internetu oraz poczty elektronicznej.

**Ekran**

o przekątnej 14" o rozdzielczości FHD WLED, matryca matowa AG o podwyższonej trwałości, kontrast 700:1, jasność 220cd/m2.

**Wydajność**

• Procesor klasy x86 ze zintegrowaną grafiką,

• Wydajność obliczeniowa: Procesor powinien osiągać w teście wydajności PassMark PerformanceTest (wynik dostępny: http://www.passmark.com/products/pt.htm) co najmniej wynik 4000 punktów Passmark CPU Mark

**Pamięć RAM**

Pamięć operacyjna: 8GB DDR4 2666 MHz możliwość rozbudowy do min 64 GB

**Pamięć masowa**

256GB SSD NVMe, zawierający partycję RECOVERY umożliwiającą odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii bez dodatkowych nośników.

Karta graficzna Wydajność grafiki: Zintegrowana karta graficzna wykorzystująca pamięć RAM systemu dynamicznie przydzielaną na potrzeby grafiki w trybie UMA (Unified Memory Access). Obsługująca funkcje: DirectX 12, OpenGL 4.4

**Bezpieczeństwo**

Sprzętowe wsparcie technologii weryfikacji poprawności podpisu cyfrowego wykonywanego kodu oprogramowania, oraz sprzętowa izolacja segmentów pamięci dla kodu wykonywanego w trybie zaufanym wbudowane w procesor, kontroler pamięci, chipset I/O.

Złącze typu Kensington Lock lub równoważne,

Zintegrowany z płytą główną dedykowany układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego. Co najmniej TPM 2.0.

Czytnik linii papilarnych wraz z oprogramowaniem

**Multimedia**

Karta dźwiękowa zintegrowana, zgodna z High Definition, wbudowane głośniki stereo.

Dwa cyfrowe mikrofony wbudowane w obudowie matrycy

Kamera internetowa HD trwale zainstalowana w obudowie matrycy oraz dioda LED.

**Klawiatura**

wyspowa układ US–QWERTY odporna na zachlapanie z wydzielonym blokiem klawiatury numerycznej, podświetlenie klawiatury.

Touchpad wyposażony w dwa niezależne klawisze funkcyjne ze wsparciem dla technologii multitouch. Musi pozwalać na obsługę gestów dla minimum trzech niezależnych punktów dotyku.

**Bateria i zasilanie**

Min. 4-cell, 50 Wh, Li-Po Czas pracy na baterii minimum 10 godzin według dokumentacji producenta laptopa. Szybkie ładowanie baterii do 80% w czasie nie dłuższym niż 60 minut. Możliwość beznarzędziowej wymiany baterii. Zabezpieczenie przed przypadkowym wypadnięciem baterii. Zasilacz o mocy min. 60 W.

**Waga**

nie więcej niż: 2 kg

Grubość laptopa po złożeniu powinna być mniejsza niż 25 mm.

**Obudowa**

Szkielet i zawiasy notebooka wykonane z wzmacnianego metalu. Obudowa laptopa powinna umożliwiać łatwą wymianę dysku oraz pamięci RAM przez użytkownika bez potrzeby interwencji serwisu - po demontażu klapy serwisowej.

**Certyfikaty**

Oferowane modele komputerów muszą posiadać certyfikat potwierdzający poprawną współpracę oferowanych modeli komputerów z oferowanym systemem operacyjnym.

Deklaracja zgodności CE lub równoważne

Norma EnergyStar 7.1 - komputer musi znajdować się na liście zgodności dostępnej na stronie www.energystar.gov oraz http://www.eu-energystar.org

Zgodność z normą TCO 8.0

Oferowane laptopy muszą być wykonane/wyprodukowane w systemie zapewnienia jakości ISO 9001 i ISO 14001 lub równoważnych systemach jakości. Wylot powietrza chłodzącego notebooka z tyłu obudowy.

**Inne**

Notebook musi być zgodny z następującymi technologiami:

• WMI (Windows Management Instrumentation)

• PXE (Preboot Execution Environment)

• DMI (Desktop Management Interface)

• SMBIOS (System Management BIOS)

• CIM (Common Information Model)

**BIOS**

Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o:

• Modelu komputera.

• Nr seryjnego komputera.

• Wersji BIOS (z datą).

• Modelu procesora wraz z informacjami o prędkości taktowania

• Informacji o ilości, typie i obsadzeniu pamięci RAM.

• Informacji o dysku twardym: model oraz pojemność

• MAC adresie zintegrowanej karty sieciowej

• Numerze matrycy

Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z USB

Możliwość - bez potrzeby uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych - ustawienia hasła na poziomie systemu, administratora i dysku twardego.

Możliwość autoryzacji użytkownika za pomocą technologii biometrycznej z poziomu BIOS przed uruchomieniem systemu operacyjnego

**Dodatkowe oprogramowanie**

Oprogramowanie dostarczone przez producenta komputera pozwalające na zdalną inwentaryzację komputerów w sieci, lokalną i zdalną inwentaryzację komponentów komputera, umożliwiające co najmniej:

* Informowanie administratora o otwarciu obudowy
* Zdalne wyłączanie, restart oraz hibernacje komputera w sieci,
* Otrzymywanie informacji WMI – Windows Management Interface,
* Tworzenie raportów stanu jednostki,
* Monitorowanie stanu komponentów: CPU, Pamięć RAM, HDD, wersje BIOS,
* Aktualizację BIOS do najnowszej wersji zarówno dla pojedynczej maszyny jak i grupy,
* Tworzenie kopii zapasowych BIOS wraz z ustawieniami
* Tworzenie indywidualnych numerów dla poszczególnych użytkowników,
* Włączenie lub wyłączanie BOOTowania portów USB

Oprogramowanie umożliwiające w pełni automatyczną instalację sterowników urządzeń opartą o automatyczną detekcję posiadanego sprzętu.

Rozszerzenie licencji na posiadany przez Zamawiającego program antywirusowy Nod32.

**System operacyjny**

Licencja na zainstalowany system operacyjny 64 bit niewymagający aktywacji za pomocą telefonu lub Internetu u producenta. Graficzny system operacyjny umożliwiający uruchomienie systemów Zamawiającego (m.in.:CGM Clininet, CGM ERP, Płatnik) bez użycia wirtualizacji w wersji pozwalającej na zarządzanie systemem za pomocą systemu domeny i przeznaczonej do zastosowań biznesowych.

**Porty i złącza**

* Min. 1 x USB 3.2 Gen2 z możliwością ładowania baterii laptopa (USB-C)
* Min. 2 x USB 3.2 Gen1 (przynajmniej jedno z możliwością ładowania zewnętrznych urządzeń bezpośrednio z portu USB komputera).
* VGA / HDMI
* Czytnik kart multimedialnych (SD, SDHC do 32 GB, SDXC do 128 GB)
* Audio: line-in/mikrofon; Audio: line-out/słuchawki; lub combo.
* Karta sieciowa LAN 10/100/1000 Ethernet RJ 45 zintegrowana z płytą główną z diodami sygnalizującymi status
* Zintegrowana w postaci wewnętrznego modułu karta WiFi 6, 802.11ax
* Bluetooth v 5.0,
* Dedykowane złącze do stacji dokującej (nie dopuszcza się USB – nawet dedykowanego)

**Gwarancja**

o świadczona w siedzibie Zamawiającego, przyjazd certyfikowanego przez producenta serwisanta do końca następnego dnia roboczego, chyba że niezbędne będzie naprawa sprzętu w siedzibie producenta ,lub autoryzowanym przez niego punkcie serwisowym - wówczas koszt transportu do i z naprawy pokrywa Wykonawca,

o Naprawy gwarancyjne urządzeń musi być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta,

o Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej komputera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela

o Dostęp do najnowszych sterowników i uaktualnień na stronie producenta zestawu realizowany poprzez podanie na dedykowanej stronie internetowej producenta numeru seryjnego lub modelu komputera – do oferty należy dołączyć link strony.

## Tablety

Procesor umożliwiający płynną pracę w zaoferowanym systemie.

Pamięć RAM: min. 4 GB DDR3

Pamięć trwałą wbudowana: min. 64 GB

Przekątna ekranu: około 10" (+/- 0,5”)

Minimalna rozdzielczość ekranu: 2560 x 1600

Łączność: Wi-Fi 5 (802.11 a/b/g/n/ac), Bluetooth

Aparaty, min.: 8.0 Mpix – przód, 13.0 Mpix - tył

Dodatkowe informacje: Funkcja szybkiego ładowania, Aluminiowa obudowa

Dołączony zasilacz oraz kabel USB Type-C

## Drukarki

|  |
| --- |
| Typ drukarki: Monochromatyczna - A4 |
| Technologia: Laserowa |
| Szybkość: min. 40 stron na minutę |
| Funkcja automatycznego duplexu w standardzie. |
| Rozdzielczość: min. 1200 dpi |
| Wymiary maksymalne: (Szer. x Głęb. x Wys.) 370 × 300 × 300 mm |
| Pobór mocy: max 620 W |
| Napięcie zasilania: AC 220 ~ 240 V, 50/60 Hz |
| Hałas: max. 63 dB(A) |
| Pamięć: min. 128 MB RAM |
| Pojemność wejściowa: kaseta na min. 200 arkuszy A4, podajnik ręczny na min: 20 arkuszy |
| Pojemność wyjściowa: min. 100 arkuszy A4 |
| Obsługiwane Systemy Operacyjne: min. Windows 7/10/Server 2012 oraz nowsze |
| Standardowe interfejsy: min. USB 2.0, FastEthernet (10/100BaseTX) |
| Sterowniki w formacie plików PPD |

## Modernizacja infrastruktury teleinformatycznej

### Warunki ogólne

Wykonawca połączy dostarczane przełączniki sieciowe oraz punkty dostępowe z pozostałymi segmentami sieci. Zamawiający wymaga aby wszystkie dostarczane Access pointy zostały podłączone do sieci LAN w punktach wyznaczonych w załączniku 1 do niniejszego OPZ. Za podłączenie Access pointów do sieci odpowiedzialny jest Wykonawca. W celu prawidłowego oszacowania oferty w zakresie wymaganej modernizacji sieci zaleca się wykonać wizję lokalną.

Wszystkie zmodernizowane punkty muszą przejść testy: Wire Map, Lenght, Propagation delay, Delay Skew, Resistance, Insertion Loss, Return Loss, NVP, NEXT, PS NEXT, ACR.

Wykonawca dostarczy Zamawiającemu odpowiednie patchcordy światłowodowe oraz miedziane [min. cat. 6] w ilościach pozwalających na podłączenie wszystkich zainstalowanych w szafkach portów, oraz niezbędnych do podłączenia urządzeń sieciowych do każdego gniazda abonenckiego.

Wykonawca musi skonfigurować prawidłowe tabele routingu z użyciem odpowiednich poziomów dostępu wskazanych przez ASI [np. przy pomocy ACL] dla wszystkich sieci vLan na dostarczanych urządzeniach.

**Wszystkie urządzenia muszą zostać zainstalowane zgodnie z wytycznymi producenta sprzętu.**

**Wszystkie dostępne porty SFP/SFP+ muszą zostać obsadzone odpowiednimi wkładkami kompatybilnymi z zainstalowaną infrastrukturą światłowodową.**

W ramach projektu Wykonawca dostarczy, zainstaluje i skonfiguruje urządzenia sieciowe:

### Switch dostępowy

1. Przełącznik posiadający 48 porty 10/100/1000BASE-T
2. Przełącznik posiadający 4 porty 1GbE SFP (z wkładkami)
3. Wysokość urządzenia 1U
4. Nieblokująca architektura o wydajności przełączania min.104 Gb/s
5. Szybkość przełączania min. 77 Milionów pakietów na sekundę
6. Tablica MAC adresów min. 16k
7. Wsparcie dla ramek Jumbo Frames
8. Obsługa Quality of Service, IEEE 802.1p
9. Obsługa Link Layer Discovery Protocol LLDP IEEE 802.1AB
10. Obsługa LLDP Media Endpoint Discovery (LLDP-MED)
11. Obsługa CDPv2
12. Wbudowany dodatkowy port Fast Ethernet do zarządzania poza pasmem - out of band management.
13. Wbudowany port pozwalający na podłączenie zewnętrznego redundantnego zasilacza RPS.
14. Możliwość monitoringu pakietów
15. Obsługa TACACS+ (RFC 1492)
16. Obsługa klienta RADIUS RFC 2865
17. Obsługa RADIUS Accounting RFC 2866
18. Obsługa ACL (Access Control List) – minimum 100
19. Obsługa RSPAN
20. Obsługa Internal 802.1X Authentication Server, 802.1X Monitor Mode, 802.1X Client Scaling
21. Obsługa SSH 2
	1. RFC 4252: SSH authentication protocol
	2. RFC 4253: SSH transport layer protocol
	3. RFC 4254: SSH connection protocol
	4. RFC 4251: SSH protocol architecture
	5. RFC 4716: SECSH public key file format
	6. RFC 4419: Diffie-Hellman group exchange for the SSH transport layer protocol
22. Obsługa routingu statycznego
23. Obsługa IEEE 802.3x —Flow control
24. Obsługa Multicast VLAN Registration (MVR)
25. Obsługa Independent VLAN Learning (IVL)
26. Obsługa RFC 4541 (IGMP)
27. Obsługa minimum 4 instancji MSTP
28. Obsługa mechanizmu S-Flow
29. Obsługa dynamicznego routing IPv4 (RFC 2453 RIP v2)
30. Obsługa Authentication, Authorization and Accounting (AAA)
31. Obsługa list kontroli dostępu dla ruchu przychodzącego na podstawie:
	1. Czasu
	2. Źródłowego i docelowego adresu IP
	3. TCP/UDP źródłowy i docelowy
	4. Rodzaju protokołu IP
	5. EtherType
	6. IEE 802.1p
	7. Źródłowy i docelowy adres MAC
	8. Vlan id
32. Zakres temperatury pracy 0-50 °C
33. Możliwość zarzadzania przełącznikiem z dedykowanej aplikacji zarządzającej
34. Możliwość zarzadzania przełącznikiem z poziomu wbudowanej przeglądarki
35. Możliwość zarzadzania przełącznikiem z poziomu CLI
36. Wsparcie dla Zero-touch provisioning
37. Obsługa skryptów CLI
38. Gwarancja Lifetime realizowana przez min. pięć lat po zakończeniu produkcji urządzenia

### Switch SAN

* Wysokość przełącznika 1U w systemie montażu w szafie typu rack 19”
* Ilość portów SFP: 24 szt. porty uniwersalne o maksymalnej przepustowości 32GB/s, z obsługą przepustowości 16Gbit/s, 8Gbit/s i 4Gbit/s z automatycznym wyborem przepustowości (auto-sensing), obsługa trybu full-duplex
* 8 portów aktywnych
* Dostarczone moduły optyczne 8 szt. SFP 16Gbit/s, Short Wave Length (SWL), Multi Mode Fibre (MMF)
* Obsługa trybów pracy portów FC: D\_port, F\_port, E\_port, M-Port
* Obsługa funkcji POD (Ports on Demand) przydziału licencji dla aktywnych portów FC
* Możliwość aktualizacji firmware’u switcha
* Aktywne funkcje: Active Gateway, Webtools, Advanced Zoning, FullFabric (z obsługą do min. 64 przełączników FC)
* Możliwość obsługi funkcjonalności (przez zakupienie odpowiednich licencji): Trunking, Extended Fabric, Fabric Vision
* Zarządzanie
	+ RJ-45 min 10/100 Mb/s do zarządzania poprzez sieć Ethernet
	+ RJ-45 lub DB9 do zarządzania poprzez interfejs RS232
	+ USB
	+ In-band over FC
* Sygnalizacja aktywnych i podłączonych portów na panelu przednim urządzenia
* Zarządzanie poprzez przeglądarkę WWW z obsługą połączeń szyfrowanych 128-bit SSL oraz poprzez usługę SSH
* Wsparcie dla protokołu SNMP v.3

Gwarancja: producenta w miejscu instalacji urządzenia z gwarantowaną skuteczną naprawą do końca następnego dnia od zgłoszenia. Naprawa realizowana przez certyfikowanego przez producenta serwisanta.

### AP

* Punkt dostępowy z dwoma wbudowanymi, niezależnymi od siebie, modułami radiowymi dla komunikacji IEEE 802.11a/b/g/n/ac
* Obsługa 802.11ac Wave 2
* Dwu zakresowe moduły radiowe; 2x2:2 MIMO
* Zysk z anten 4dBi - pasmo 2.4 GHz; 6 dBi - pasmo 5GHz
* Obsługa trybu MU MIMO
* Obsługa 16 SSID oraz minimum 250 użytkowników
* Punkt dostępowy musi wspierać standard Bluetooth Low Enegry (BLE) w wersji 4.2
* Punk dostępowy posiada wbudowany port USB 2.0
* Punkt dostępowy zasilany poprzez POE zgodnie ze standardem IEEE 802.11af
* Port 10/100/1000BaseT Ethernet z automatycznym wykrywaniem parametrów transmisji
* Punkt dostępowy musi oferować obsługę następujących mechanizmów warstwy L2 i L3:
* Routing warstwy L3, 802.1q, DynDNS, DHCP serwer/klient, klient BOOTP, PPPoE oraz CDP, LLDP, L2TPv3 Client, L2TPv3 Tunnel Establishment Criteria, L2TPv3 Broadcast Optimization, L2TPv3 over IPsec, L2TPv3 Client, L2TPv3 Fast Failover
* Punkt dostępowy musi obsługiwać następujące mechanizmy bezpieczeństwa:

Firewall typu stateful, filtrowanie IP, NAT, 802.1x, 802.11i, WPA2, WPA, metoda wykrywania fałszywych urządzeń: 24x7 dwuzakresowy sensor WIPS, wbudowany IDS oraz bezpieczny dostęp gości (hotspot) wraz z portalem rejestracyjnym (captive portal), IPSec, wudowany Radius Server

* Obsługa następujących mechanizmów QoS:

Quality of Service (QoS) WMM, WMM-UAPSD, 802.1p, Diffserv i TOS

* Obsługa mechanizmu Smart Load Balancing polegającą na: Równomiernym dystrybuowaniu klientów na punkty dostępowe i pasma częstotliwości.
* Wsparcie dla Network Access Control oraz mechanizmów analizy anomalii w ruchu sieciowym Deep Packet Inspection
* Zintegrowana funkcjonalność widoczności i kontroli aplikacji (Layer 7) bezpośrednio na punkcie dostępowym bez zewnętrznego kontrolera
* Temperatura pracy urządzenia od 0° C do 40° C
* Interfejs konsoli RJ45 lub RS232
* Współdzielenie modułów radiowych oraz skanowanie poza kanałem transmisji umożliwiające pełnienia dwóch funkcji – punktu dostępowego i sensora
* 802.11r Fast Roaming: szybki roaming
* Mechanizm typu Smart Rf pozwalający urządzeniom na automatyczne i inteligentne dostosowanie się do zmian w środowisku radiowym w celu eliminacji niespodziewanych luk w zasięgu. Wykrywanie zakłóceń pochodzące od urządzeń Wi-Fi i pozostałych (np. uszkodzone anteny, sąsiednie punkty dostępu) oraz automatycznie dostosowanie w razie potrzeby, kanału i mocy sygnału.
* Wsparcie dla usług lokalizacyjnych
* Wsparcie dla usług WIPS co najmniej w zakresie: 32 WIPS Events, Customized WIPS Signatures, Device Categorization, Rogue AP Detection, Rogue AP Termination (Manual / Automatic)
* Wsparcie DLA ACL bazujących na DNS co najmniej w zakresie:

Per IP Interface, Per Port, Per User, Per Wireless LAN

* Firewall bazujący na Rolach, przypisywanie Ról na podstawie parametrów:

Role Assignment by AP Location,Default Role, Role Assignment by Active Directory Attributes,Role Assignment by OpenLDAP Attributes,Role Assignment by Authentication State,Role Assignment by Authentication Type Role Assignment by DHCP Fingerprint, Role Assignment by Encryption Type, Role Assignment by Group Membership,Role Assignment by MAC Address,Role Assignment by SSID Name,Role Based VLANs,Role Assignment User Defined LDAP Attributes

* Wsparcie dla EAP-MD5
* Obsługa DHCP Finderprinting
* Wsparcie dla certyfikatów RSA: Certificate Management Protcol (CMPv2)
* Obsługa WIPS Sernsor: Dedicated Sensor Radio, On-Channel Scanning, Off-Channel Scanning, Sensor Radio Lock
* Zaawansowane zarządzanie plikami: IPv4 FTP Client,IPv6 FTP Client, IPv4 SFTP Client, IPv6 SFTP Client, IPv4 TFTP Client, IPv6 TFTP Client
* Obsługa logowania: Email Notifications,IPv4 Syslog Event Logging, IPv6 Syslog Event Logging, Syslog Event Policy, SNMP Traps
* Zarządzanie, wsparcia dla ACL: IPv4 Host Address, IPv4 Access Control List, IPv4Source Subnet, IPv6 Host Address, IPv6 Access Control List, IPv6 Source Subnet
* Zarządzanie, wsparcia dla: IPv4 HTTP / HTTPS, IPv6 HTTP / HTTPS, Serial Console, IPv4 SSHv2, IPv6 SSHv2, IPv4 Telnet, IPv6 Telnet
* Zarządzanie użytkownikami AAA: Idle Session Timeout, Local Management Authentication, RADIUS Management Authentication, RADIUS Management Authorization, TACACS+ Authentication, TACACS+ Authorization, TACACS+ Accounting, Management Authentication Fallback
* Obsługa SNMP: SNMPv2c, SNMPv3, SNMP Traps, Disable export of sensitive information over SNMP
* Zarządzanie poprzez Web interfejs, dosępne conajmniej opcje: Device Status, Floor Plans, Heat Maps (Signal, Interference, Noise), Mesh Topology View, Mesh Visualization, Network Topology View, Mesh Topology View, Mesh Visualization, RF Quality, System Dashboard, System Configuration, System Diagnostics, System Inventory, System Operations, System Security Status, System Statistics, Traffic Utilization
* Wsparcie dla topologii MESH
* Obsługa rozszerzeń 802.11:

IEEE 802.11a, IEEE 802.11b, IEEE 802.11d, IEEE 802.11g,IEEE 802.11e, IEEE 802.11h, IEEE 802.11i, IEEE 802.11k, IEEE 802.11n, IEEE 802.11r, IEEE 802.11v, IEEE 802.11w, IEEE 802.11ac

* Automatyczny provisioning AP bazujący na: Automatic Re-provisioning for Existing Devices, Re-run Automatic Provisioning for each Adoption, CDP Match, DHCP Option Match, DNS Suffix Match, Hostname Match, LLDP Match, MAC Address Match, Model Number Match, Serial Number Match, VLAN ID Match, Wildcard Match
* Wsparcie dla debuggingu: Telnet/SSH/Serial, Syslog, Web-UI
* Lokalizacja AP poprzez: wyłączenie LED, sekwencja LED
* Packet Capture wsparcie dla: Telnet/SSH/Serial, FTP / TFTP Server,Tasman Sniffer Protocol (TZSP)
* Obsługa: IEEE 802.1s Multiple Spanning Tree Protocol, IGMPv1, v2, v3 Snooping, Multicast Listener Discovery Protocol (MLDv2)
* Wsparcie dla Bonjour Gateway w zakresie: Bonjour Service Discovery, Bonjour Service Filtering (SVI), Bonjour Service Filtering (User Role), Bonjour Service Filtering (Wireless LAN), Bonjour Service Forwarding (Inter VLAN)
* Wsparcie dla IPv6
* Wsparcie dla IP Routing V4/V6
* Obsługa NAT: Dynamic NAT, Port Address Translation (PAT), NAT Load Balancing / Failover, NAT Precedence, Static NAT, Layer 2 NAT (Split Tunneling for Tunneled VLANs)
* Wsparcie dla rate limiting
* Obsługa funkcji mobilności:

Controller Assisted Mobility, Credential Caching, IEEE 802.11r Fast BSS Transition (FT), IEEE 802.11i OPMK Caching, IEEE 802.11i PMK Caching, IEEE 802.11i Pre-Authentication, Layer 2 Mobility, Layer 3 Mobility (Extended VLANs), Proxy ARP, Proxy Neighbor Discovery (ND)

* Obsługa enkrypcji:

CCMP (WPA2), TKIP (WPA/WPA2), KeyGuard, WEP 128

* Wsparcie dla EAP:

Cisco Protected EAP (EAP-MSCHAPv2), Cisco Protected EAP (EAP-GTC), Cisco LEAP, EAP-AKA, EAP-FAST, EAP-SIM, EAP-TLS, EAP-TTLS (PAP), EAP-TTLS (CHAP),EAP-TTLS (MS-CHAP),

EAP-TTLS (MSCHAPv2), EAP-TTLS (EAP-MD5), EAP-TTLS (EAP-GTC), EAP-TTLS (EAP-TLS), Microsoft Protected EAP (MSCHAPv2), Microsoft Protected EAP (EAP-TLS)

* Punkt dostępowy musi mieć możliwość pracy w trybie autonomicznym (bez kontrolera) lub w trybie „lekkiego AP” pod kontrolą kontrolera bezprzewodowego
* Punk dostępowy musi mieć możliwość pracy jako witrualny kontroler (musi obsługiwać w tym trybie minimum 64 punkty dostępowe

**UWAGA: Wykonawca wykona infrastrukturę Ethernet do podłączenia Access Pointów zgodnie z załącznikiem nr 1 do OPZ. Infrastruktura musi zostać wykonana zgodnie z wymaganiami producenta Access Pointów (min. zgodnie z cat. 6).**

Kontroler AP

* Kontroler sieci bezprzewodowej w formie fizycznej
* Port - Gigabit SFP interface
* 5 portów 10/100/1000 Ethernet Ports, 802.3af and, 802.3at Draft
* 1 port USB 2.0 Host
* 1 Serial Port (RJ45)
* Zakres temperatury pracy 0-40 ° C
* Możliwość obsługi do min. 128 jednocześnie podpiętych punktów dostępowych
* W momencie dostarczenie ma mieć możliwość podpięcia min. 12 punktów dostępowych wyspecyfikowanych w specyfikacji Access Points
* Wbudowana zapora ogniowa zarówno dla sieci przewodowej i bezprzewodowej z funkcjonalnością Role Based Firewall
* Wbudowany mechanizm Wireless Intrusion Protection System (WIPS)
* Obsługa IPSec VPN gateway
* Obsługa AAA radius Server oraz zabezpieczonego dostępu gościnnego za pośrednictwem Captive Portal.
* Obsługa Captive Portal
* Uwierzytelnianie w oparciu o adresy MAC
* Wsparcie dla standardu 802.11w Secure Management Frames
* Wsparcie dla Network Access Control oraz mechanizmów analizy anomalii w ruchu sieciowym Deep Packet Inspection
* Dystrybucja licencji bazująca na aktualnym obciążeniu w poszczególnych lokalizacjach – brak konieczności stosowania licencji, dotyczących ilości obsługiwanych punktów dostępowych, jednocześnie w lokalizacjach zdalnych i w punkcie centralnym.
* Wsparcie dla NAC (Network Access Control)
* Obsługa: Routing warstwy L3, 802.1q, DynDNS, DHCP serwer/klient, klient BOOTP, PPPoE oraz CDP, LLDP, L2TPv3 Fast Failover
* Wsparcie dla: Firewall typu stateful, filtrowanie IP, NAT, 802.1x, 802.11i, WPA2, WPA, metoda wykrywania fałszywych urządzeń: 24x7 dwuzakresowy sensor WIPS, wbudowany IDS oraz bezpieczny dostęp gości (hotspot) wraz z portalem rejestracyjnym (captive portal), IPSec, wudowany Radius Server
* Możliwość klastrowania kontrolerów oraz opcji HA: Automatic Synchronized Configuration, Active / Active, Active / Standby, Access Point Load Balancing, Access Point Steering (Controller Groups), License Pooling
* Zintegrowana funkcjonalność widoczności i kontroli aplikacji
* Wsparcie dla analityki: Captive Portal Analytics, Client Analytics, Device Analytics, User Walk-in Analytics, User Analytics, ApplicationTraffic Analytics (24 hours), Client Walk-in, AP Utilization, Client Utilization, Device Details, ApplicationTraffic
* Wsparcie dla usług WIPS co najmniej w zakresie: 32 WIPS Events, Customized WIPS Signatures, Device Categorization, Rogue AP Detection, Rogue AP Termination (Manual / Automatic)
* Obsługa Web Filtering
* Wsparcie DLA ACL bazujących na DNS co najmniej w zakresie:

Per IP Interface, Per Port, Per User, Per Wireless LAN

* Firewall bazujący na Rolach, przypisywanie Ról na podstawie parametrów:

Role Assignment by AP Location,Default Role, Role Assignment by Active Directory Attributes,Role Assignment by OpenLDAP Attributes,Role Assignment by Authentication State,Role Assignment by Authentication Type Role Assignment by DHCP Fingerprint, Role Assignment by Encryption Type, Role Assignment by Group Membership,Role Assignment by MAC Address,Role Assignment by SSID Name, Role Based VLANs,Role Assignment User Defined LDAP Attributes

* Wsparcie dla certyfikatów RSA: Certificate Management Protcol (CMPv2)
* Zaawansowane zarządzanie plikami: IPv4 FTP Server, IPv6 FTP Server, IPv4 FTP Client,IPv6 FTP Client, IPv4 SFTP Client, IPv6 SFTP Client, IPv4 TFTP Client, IPv6 TFTP Client
* Obsługa logowania: Email Notifications,IPv4 Syslog Event Logging, IPv6 Syslog Event Logging, Syslog Event Policy, SNMP Traps
* Zarządzanie, wsparcia dla ACL: IPv4 Host Address, IPv4 Access Control List, IPv4Source Subnet, IPv6 Host Address, IPv6 Access Control List, IPv6 Source Subnet
* Zarządzanie, wsparcia dla: IPv4 HTTP / HTTPS, IPv6 HTTP / HTTPS, Serial Console, IPv4 SSHv2, IPv6 SSHv2, IPv4 Telnet, IPv6 Telnet
* Zarządzanie użytkownikami AAA: Idle Session Timeout, Local Management Authentication, RADIUS Management Authentication, RADIUS Management Authorization, TACACS+ Authentication, TACACS+ Authorization, TACACS+ Accounting, Management Authentication Fallback
* Obsługa SNMP: SNMPv2c, SNMPv3, SNMP Traps, Disable export of sensitive information over SNMP
* Zarządzanie poprzez Web interfejs, dosępne conajmniej opcje: Device Status, Floor Plans, Heat Maps (Signal, Interference, Noise), Mesh Topology View, Mesh Visualization, Network Topology View, Mesh Topology View, Mesh Visualization, RF Quality,System Dashboard, System Configuration, System Diagnostics, System Inventory, System Operations, System Security Status, System Statistics, Traffic Utilization
* Wsparcie dla REST API
* Automatyczny provisioning AP bazujący na: Automatic Re-provisioning for Existing Devices, Re-run Automatic Provisioning for each Adoption, CDP Match, DHCP Option Match, DNS Suffix Match, Hostname Match, LLDP Match, MAC Address Match, Model Number Match, Serial Number Match, VLAN ID Match, Wildcard Match
* Wsparcie dla debuggingu: Telnet/SSH/Serial, Syslog, Web-UI
* Packet Capture wsparcie dla: Telnet/SSH/Serial, FTP/TFTP Server, Tasman Sniffer Protocol (TZSP)
* Wsparcie dla Bonjour Gateway w zakresie: Bonjour Service Discovery, Bonjour Service Filtering (SVI), Bonjour Service Filtering (User Role), Bonjour Service Filtering (Wireless LAN), Bonjour Service Forwarding (Inter VLAN)
* Wsparcie dla IPv6
* Wsparcie dla IP Routing v4/v6
* Obsługa NAT: Dynamic NAT, Port Address Translation (PAT), NAT Load Balancing / Failover, NAT Precedence, Static NAT, Layer 2 NAT (Split Tunneling for Tunneled VLANs)
* Analiza spektrum
* Raporty conajmniej w zakresie: Device Inventory, RF Health, Utilization, Security, Compliance
* Obsługa funkcji mobilności:

Controller Assisted Mobility, Proxy ARP, Proxy Neighbor Discovery (ND)

* Obsługa enkrypcji: CCMP (WPA2), TKIP (WPA/WPA2), WEP 64, WEP 128
* Wsparcie dla EAP: Cisco Protected EAP (EAP-MSCHAPv2), Cisco Protected EAP (EAP-GTC), Cisco LEAP, EAP-AKA, EAP-FAST, EAP-SIM, EAP-TLS, EAP-TTLS (PAP), EAP-TTLS (CHAP),EAP-TTLS (MS-CHAP), EAP-TTLS (MSCHAPv2), EAP-TTLS (EAP-MD5), EAP-TTLS (EAP-GTC), EAP-TTLS (EAP-TLS), Microsoft Protected EAP (MSCHAPv2), Microsoft Protected EAP (EAP-TLS)

### Szafa 42U

|  |  |
| --- | --- |
| Parametr | Wymagania minimalne |
| Wysokość | Min. 42U |
| Szerokość całkowita | Min. 600 mm |
| Głębokość całkowita | 1200 mm |
| Szerokość szyn montażowych | Standard 19 cali |
| Ilość belek nośnych | Dwie pary belek nośnych 19 cali o płynnej regulacji położenia |
| Wykonanie drzwi przednich | Blaszane, jednoskrzydłowe, perforowane (prześwit ok. 80%) z zamkiem z klamką, możliwość zmiany kierunku otwierania drzwi |
| Wykonanie drzwi tylnych | Perforowane, dwuskrzydłowe dla ograniczenia przestrzeni serwisowej, zamykane na zamek z kluczem wspólny z zamkiem przednim, możliwość zdjęcia bez użycia narzędzi |
| Ściągane panele boczne | dwie osłony boczne, pełne z zamkami  |
| Chłodzenie | przystosowana do chłodzenia horyzontalnego przód-tył, pasywna – bez wentylatorów wspomagających |
| Otwory kablowe | w płycie dolnej i górnej  |
| Obciążenie dopuszczalne | Min. 1000 kg |
| Wykończenie powierzchni: szkielet, osłony, drzwi | Malowane farbą proszkową o grubej strukturze |
| Klasa ochrony | IP 20 zgodnie z normą PN-EN 60529 lub równoważną |
| Wyposażenie dodatkowe | Wszystkie wolne „U” zaślepione zaślepkami, zainstalowane dwa zestawy 3-fazowych listew zasilających z 8 szt. gniazd. Stopki poziomujące, opcjonalne fabryczne zabezpieczenie teleskopowe przeciwko wywróceniu szafy do przodu Zestaw przewodów uziemiających, certyfikat CE |

Szafę należy zainstalować, zgodnie z zaleceniami producenta, w serwerowni.

### Firewall / UTM

Platforma służąca zabezpieczeniu dostępu do systemów szpitalnych oraz do innych usług zainstalowanych u Zamawiającego, pozwalająca na filtrowanie ruchu z/do internetu do/z sieci LAN. Platforma musi umożliwiać kontrolę w warstwie aplikacji oraz umożliwiać zdalny dostęp do sieci LAN zamawiającego. W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca 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.

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje bezpieczeństwa oraz funkcjonalności dodatkowe. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

Dla elementów systemu bezpieczeństwa wykonawca musi zapewnić wszystkie poniższe funkcjonalności:

1. Zapora sieciowa typu Next Generation Firewall (NGFW)
2. Mechanizm pozwalający na dwustronną analizę ruchu bez proxy oraz ograniczeń na rozmiar skanowanego pliku.
3. Minimalna ilość interfejsów:
	1. 4 interfejsy 2.5 Gb SFP
	2. 4 interfejsy 2.5 GbE
	3. 12 interfejsów RJ-45 Ethernet 10/100/1000 – każdy z interfejsów musi mieć możliwość konfiguracji osobnej podsieci i strefy bezpieczeństwa.
	4. 2 interfejsy USB dla przyszłych potrzeb i do podłączenia modemu 3G
	5. 1 interfejs konsoli do zarządzania zaporą
	6. 1 interfejs RJ-45 Ethernet 10/100/1000 do zarządzania zaporą
4. Zapora powinna posiadać dysk SSD o pojemności przynajmniej 16 GB z możliwością wymiany na większy.
5. Możliwość przypisania wielu interfejsów fizycznych do pojedynczej strefy bezpieczeństwa
6. Możliwość powiązania wielu interfejsów fizycznych w jeden port logiczny (agregacja portów) celem podniesienia wydajności połączeń oraz zapewnienia redundancji
7. Możliwość utworzenia przynajmniej 256 interfejsów logicznych VLAN, wsparcie dla standardu 802.1q
8. Obsługa nielimitowanej ilości hostów podłączonych w sieci chronionej
9. Minimalna ilość jednocześnie obsługiwanych połączeń: 1 000 000
10. Możliwość obsłużenia przynajmniej 14 000 nowych połączeń w ciągu 1 sekundy.
11. Przepustowość urządzenia pracującego w trybie stateful firewall: 3 Gbps – dla ramki 1518B zgodnie z RFC 2544
12. Przepustowość urządzenia pracującego z włączonym mechanizmem IPS: 1.4 Gbps
13. Przepustowość urządzenia pracującego jako koncentrator VPN: 1.45 Gbps dla szyfrowania AES bez aktywnych usług UTM, zgodnie z RFC 2544
14. Przepustowość urządzenia DPI/NGFW (z włączonymi wszystkimi usługami bezpieczeństwa – antivirus, antyspyware, IPS, bez buforowania, proxy oraz bez ograniczeń jeśli chodzi o wielkość skanowanych plików) – 1500 Mbps
15. Minimalna ilość jednocześnie zestawionych tuneli site-site VPN (urządzenie – urządzenie): 1 000
16. Minimalna ilość licencji umożliwiających zestawienie połączeń client-site IPSec VPN (komputer – urządzenie), dostępnych w pakiecie z urządzeniem: 50 z możliwością rozszerzenia do przynajmniej 1 000.
17. Urządzenie powinno umożliwiać poddanie inspekcji zawartości ruchu szyfrowanego SSL/TLS poprzez jego odszyfrowanie i ponowne zaszyfrowanie zmienionym certyfikatem. Administrator powinien mieć możliwość tworzenia wyjątków do inspekcji ruchu SSL poprzez wykorzystanie kategorii stron np. wyłączenie z inspekcji kategorii zawierających strony bankowe i medyczne.
18. Wydajnośc urządzenia z włączoną funkcją inspekcji ruchu SSL/TLS powinna wynosić minimum 300 Mbps oraz obsłużyć pow. 60 000 połączeń.
19. Obsługa IPSec, ISAKMP/IKE, Radius, L2TP, PPPoE, PPTP
20. Zintegrowany serwer DHCP, umożliwiający przydzielanie adresów IP dla hostów znajdujących się w sieci chronionej, a także dla hostów połączonych poprzez VPN (dla tuneli nawiązanych w trybie site-site oraz client-site)
21. Wsparcie funkcjonalności IP Helper, lub IP Relay (przekazywanie komunikacji DHCP pomiędzy strefami bezpieczeństwa)
22. Uwierzytelnianie użytkowników w oparciu o wewnętrzną bazę użytkowników, oraz z wykorzystaniem zewnętrznych mechanizmów RADIUS/XAUTH, Active Directory, SSO, LDAP
23. Wsparcie dla Dynamicznego DNS tzw. DDNS
24. Zintegrowany mechanizm kontroli zawartości witryn pogrupowanych na kategorie tematyczne.
25. Mechanizm kontroli treści powinien mieć możliwość filtrowania stron tłumaczonych przez google translate (strony takie również powinny być poddane inpekcji, na takich samych zasadach jak strony na które użytkownik wchodzi bezpośrednio).
26. Administrator powinien mieć możliwośc tworzenia róznych akcji dla stron które zostały wychwycone przez filtr treści. Powinny być dostępne takie akcje jak:
	1. wyświetlenie strony blokady (z możliwością tworzenia kilku róznych stron)
	2. wyświetlenie strony blokady z możliwością podania hasła odblokowującego dostęp do zablokowanej strony
	3. wyświetlenie informacji z polityką bezpieczeństwa organizacji podczas wchodzenia na strony z danj kategorii. Używtkonik może wejść na stronę po akceptacji polityki.
27. Administrator powinien mieć możliwośc stworzenia polityki kontroli treści obejmującego np. strony z kategorii Multimedia i przydzielenia ograniczonego pasma dla stron w tej kategorii np. 5 Mbps
28. Zintegrowany mechanizm kontroli transmisji poczty elektronicznej w oparciu o zewnętrzne serwery RBL.
29. Zintegrowany mechanizm zabezpieczający bezprzewodową sieć LAN, umożliwiający szyfrowanie transmisji w połączeniach bezprzewodowych realizowanych pomiędzy dodatkowymi urządzeniami Access Point a stacjami roboczymi za pomocą IPSec VPN. System wspomagania uwierzytelniania bezprzewodowych stacji roboczych, oraz użytkowników, pozwalający na wdrożenie polityki dostępowej dla sieci.
30. Możliwość uruchomienia minimum dwóch łączy WAN - Zintegrowane funkcje Load-Balancing, oraz Failover. Funkcja Failover oparta o badanie stanu łącza i badanie dostępności hosta zewnętrznego.
31. Możliwość ograniczenia ruchu na zewnętrznej stacji roboczej podczas pracy zdalnej VPN (dostęp tylko do udostępnionych zasobów lub dostęp do udostępnionych zasobów oraz zasobów sieci Internet z uwzględnieniem filtrowania treści, mechanizmu IPS oraz ochrony przed wirusami i wszelkim innym oprogramowaniem złośliwym dla komputerów połączonych przez VPN)
32. Kontrola dostępności zestawionych tuneli VPN
33. Możliwość zarządzania urządzeniem z wykorzystaniem protokołów http, https, SSH i SNMP.
34. Konfiguracja oparta na pracy grupowej/obiektowej. Polityka bezpieczeństwa pozwalająca na całkowitą kontrolę nad dostępem do Internetu powinna być tworzona według reguł opartych o grupy i obiekty.
35. Przy tworzeniu reguł dostępowych zapewniona możliwość konfiguracji trzech typów reakcji: allow, deny, discard (zezwolić, zabronić, odrzucić)
36. Funkcja NAT oparta o reguły bezpieczeństwa.
37. NAT w wersji jeden-do-jeden, jeden-do-wielu, PAT, wiele-do-wielu, wiele-do-jednego. Funkcje oparte o zaawansowaną konfigurację według reguł bezpieczeństwa (m.in. możliwość ograniczenia działania funkcji do niektórych hostów, możliwość translacji portów wyjściowych na inne docelowe)
38. Zintegrowany system skanowania antywirusowego na poziomie bramy internetowej – skanowanie protokołów http, ftp, pop3, smtp, imap4, tcp stream. Możliwość filtrowania załączników poczty. Skanowanie również plików skompresowanych.
39. Zintegrowany system skanowania antyspyware
40. Zintegrowany system IPS (system wykrywania i blokowania wtargnięć) oparty o sygnatury ataków uwzględniające zagrożenia typu worm, Trojan, dziury systemowe, peer-to-peer, buffer overflow, komunikatory, niebezpieczne kody zawarte na stronach www.
41. System IPS musi używać algorytmu szeregowego przetwarzania.
42. Zintegrowany system zapory działającej w warstwie aplikacji, umożliwiający definiowanie własnych sygnatur aplikacji z wykorzystaniem ciągu znaków lub wyrażeń regularnych (regex).
43. Systemy skanowania IPS/Antywirus/Antyspyware muszą umożliwiać skanowanie ruchu w warstwie aplikacji
	1. Bazy w/w systemów muszą być aktualizowane co najmniej raz dziennie.
	2. Administrator systemu musi mieć możliwość ręcznej aktualizacji sygnatur (online lub offline poprzez manualne importowanie sygnatur
	3. Administrator systemu musi mieć możliwość skonfigurowania, którym portem i łączem urządzenie będzie się kontaktowało z serwerami backend w celu aktualizacji sygnatur.
44. System IPS/Antywirus/Antyspyware nie może posiadać ograniczeń związanych z rozmiarem skanowanych plików.
45. Skanowanie IPS/Antywirus/Antyspyware musi być możliwe między strefami bezpieczeństwa
46. Możliwość pełnej kontroli nad programami typu P2P, IM oraz aplikacjami multimedialnymi
47. Wsparcie mechanizmów QoS – Priorytet pasma, maksymalizacja pasma, gwarancja pasma, DSCP, 802.1p
48. Wsparcie dla komunikacji VoIP - Pełne wsparcie dla SIP, H323v.1-5, zarządzanie pasmem (ruch wychodzący), VoIP over WLAN, śledzenie i monitorowanie połączeń
49. Urządzenie powinno mieć możliwość analizy behawioralnej (sandbox) minimum plików wykonywalnych PE, PDF, Office i aplikacji mobilnych. Sandbox powinien działać z wykorzystaniem minimum 4 silników pochodzących od różnych producentów w celu zwiększenia skuteczności analizy sandbox. Analiza powinna być wykonywana równolegle na wszystkich silnikach.
50. Wymagane jest dostarczenie dodatkowego urządzenia pełniące funkcję standby w klastrze wysokiej dostępności (HA) z urządzeniem podstawowym. Urządzenie standby powinno mieć identyczne parametry wydajnościowe jak podstawowa jednostka.
51. System w postaci maszyny wirtualnej powinien wspierać platformy ESX/ESXi/Hyper-V
52. System posiadać wsparcie dla IPv6.
53. System posiada wbudowany Load Balancing dla http/https.
54. System musi wspierać następujące protokoły szyfrujące:

ARC4 (128), MD5, SHA-1, SHA-256, SHA-384, SSLv3, TLSv1, TLS 1.1, TLS 1.2, TLS 1.3, 3DES (168, 256), AES (256), RSA, DHE.

1. System musi umożliwiać: 2 składnikową autentykację, wspierać One-time Passwords, umożliwiać uwierzytelnianie na podstawie własnej bazy danych użytkowników, RADIUS, LDAP, Microsoft Active Directory i Single Sign On (SSO), wsparcie dla SAML 2.0 Identity Provider (IdP)
2. System musi umożliwiać wsparcie zapytań dla kilku domen AD
3. System musi umożliwiać zmianę haseł dla podłączonych baz danych użytkowników.
4. System musi posiadać technologie „cache cleaner” umożliwiającą wykasowanie po zakończonej sesji m. in. cookies, wykorzystywanych URL.
5. System musi zawierać mechanizm uniemożliwiający wykorzystanie nieaktywnych sesji.
6. System musi umożliwiać granularne nakładanie uprawnień.
7. System musi umożliwiać dostęp do aplikacji za pomocą portalu wspierającego HTML 5.
8. Portal powinien wspierać następujące przeglądarki: Internet Explorer, Mozilla, Chrome, Opera, Safari.
9. System powinien wspierać następujące protokoły aplikacyjne: http, https, ftp, ssh, telnet, VNC, SMB/CIFS, OWA 2003/2007/2010, Citrix (ICA), RDP.
10. Zarządzanie systemem odbywa się za pomocą wbudowanego portalu web.
11. System musi mieć możliwość przywrócenie po awarii do ostatnio zapisanej konfiguracji.
12. Dla ułatwienia zarządzania certyfikatami, system powinien natywnie wspierać urząd certyfikacji min. Let’s Encrypt.
13. System umożliwia sprawdzanie urządzenia z którego wywoływane jest żądanie połączenia pod kątem uruchomienia parametrów zdefiniowanych przez administratora, np. odpowiednia wersja programu antywirusowego, wpis w rejestrze, weryfikacja istnienia wskazanego pliku na dysku.
14. Administrator może w systemie ręcznie zatwierdzać albo blokować urządzenia które chcą się podłączyć do systemu.
15. Rozwiązanie wymusza dostęp do systemu logowania za pomocą captcha dla osób które łączą się ze zdefiniowanych przez administratora krajów.
16. System musi umożliwiać graficzne przedstawienie na mapie lokalizacji podłączonego klienta na po nawiązaniu przez niego połączenia.
17. Subskrypcje pozwalające na aktualizację sygnatur aplikacji, IPS i wirusów oraz dostęp do bazy URL dla modułu kontroli aplikacji oraz zapewnienie wsparcia technicznego 24x7.
18. Licencja na oprogramowanie służące do przechowywania logów z systemu firewall i genrowania na ich podstawie raportów. W celach zapewnienia kompatybilności oprogramowanie powinno pochodzić od tego samego producenta co system firewall.

### System analizy bezpieczeństwa

**Podstawowe funkcje**

Proponowane rozwiązanie w zakresie monitorowania powinno być w stanie natychmiast wykryć nieprawidłowości w sieci, analizując dane z milionów plików i zdarzeń.

Powinno wykonywać proaktywną analizę logów i korelację zdarzeń w czasie rzeczywistym w całej infrastrukturze, aby szybko zidentyfikować ataki i wykryć naruszenia zasad.

Powinno być w stanie skorelować miliony zdarzeń z sieci, systemów, aplikacji, maszyn wirtualnych i infrastruktury pamięci masowej przy użyciu funkcji korelacji w czasie rzeczywistym.

Powinno przechowywać terabajty danych, logów bez konieczności zakupu dodatkowej pamięci masowej przy użyciu wysokowydajnego modelu danych o wysokiej kompresji, który powinien kompresować dane w stosunku co najmniej 60:1

Powinno monitorować zarówno urządzenia, jak i systemy. Na przykład, monitorowanie kontrolerów domen Windows pod kątem prób włamania, monitorowanie firewalli pod kątem skanowania portów, monitorowanie oprogramowania antywirusowego pod kątem nieoczyszczonych wirusów, monitorowanie serwerów proxy pod kątem podejrzanego dostępu do adresów URL, monitorowanie bazy danych SQL pod kątem zmian w tabelach itp.

Proponowane rozwiązanie powinno umożliwiać uwierzytelnianie i szyfrowanie połączenia między komponentami systemu.

Powinno pomóc w tworzeniu raportów bezpieczeństwa poprzez monitorowanie naruszeń bezpieczeństwa.

**Zgodność**

Proponowane rozwiązanie do monitorowania powinno zapewniać zgodność z PCI, HIPAA, NCUA, GLBA, NERC-CIP, FISMA, SOX.

**Alarmowanie i aktywne reagowanie**

Proponowane rozwiązanie monitorujące powinno być w stanie wykrywać zagrożenia dzięki aktywnemu reagowaniu na informacje pochodzące z urządzeń i systemów.

Powinno mieć wiele wbudowanych reguł do natychmiastowego użycia i dostosowania do indywidualnych potrzeb.

Powinno automatycznie i interaktywnie podejmować działania w celu ochrony infrastruktury poprzez kwarantannę, blokowanie, routing i kontrolowanie usług, procesów, kont i uprawnień.

**Graficzny interfejs użytkownika**

Proponowane rozwiązanie do zarządzania powinno zapewniać wysokiej jakości graficzny interfejs użytkownika dostępny za pośrednictwem standardowych przeglądarek.

Powinno posiadać konsolę do monitorowania zdarzeń w czasie rzeczywistym.

Powinno posiadać opcje "przeciągnij i upuść" do tworzenia filtrów i reguł.

Powinno ułatwić wyszukiwanie reguł, najlepiej przy użyciu tagów lub kategorii.

Powinno mieć możliwość wyświetlania zarówno oryginalnych, jak i znormalizowanych logów w tym samym interfejsie wyszukiwania.

Powinno mieć widoki „Top 10” dla różnych występujących problemów.

Konsola do zarządzania powinna być dostępna lokalnie lub zdalnie.

Konsola do zarządzania powinna zezwalać wielu użytkownikom na logowanie się w tym samym czasie.

Proponowane rozwiązanie powinno integrować się z Active Directory w celu logowania użytkownika.

Powinien szybko wskazać nieprawidłowości w sieci.

Proponowane rozwiązanie powinno być łatwe w użyciu i intuicyjne dzięki funkcjom typu „drill-down”.

**Raportowanie**

Proponowane rozwiązanie w zakresie monitorowania powinno być w stanie szybko wygenerować raporty dotyczące zgodności.

Powinno mieć wiele wbudowanych raportów (min. 300) i gotowych pakietów zgodności z normami, które pomogłyby w celach audytowych.

Proponowane rozwiązanie powinno umożliwiać dostosowywanie raportów przez dodawanie / usuwanie kolumn, ustawianie filtrów, określanie ram czasowych itp.

Powinno mieć raporty, które pokazują informacje dotyczące wykorzystania bazy danych.

**Wsparcie dla wielu producentów**

Proponowane rozwiązanie monitorujące nie powinno być specyficzne dla producenta.

Proponowane rozwiązanie powinno umożliwiać tworzenie nowych alarmów od zera a także definiowanie wartości progowych.

**Wdrożenie**

Powinno umożliwiać szybkie wdrożenie, tak jak w przypadku urządzenia wirtualnego, na popularnych hiperwizorach, takich jak VMware lub Hyper-V.

**Dodatkowe komponenty**

Proponowane rozwiązanie w zakresie monitorowania powinno chronić wrażliwe dane poprzez wykrywanie w czasie rzeczywistym i blokowanie dysków USB.

**Integracja**

Proponowane rozwiązanie monitorujące powinno współdzielić i korelować logi i zdarzenia z rozwiązań do monitorowania sieci, rozwiązań do monitorowania aplikacji i rozwiązań do monitorowania wirtualizacji poprzez integrację współdzielenia danych.

Powinno być w stanie przyjmować trapy z monitoringu sieci, monitoringu aplikacji i innych rozwiązań do monitoringu.

**Skalowanie**

Proponowane rozwiązanie w zakresie monitorowania powinno zapewniać możliwość długoterminowego przechowywania i wyszukiwania oryginalnych logów.

Proponowane rozwiązanie powinno obsługiwać opcje wielu wdrożeń - scentralizowane, rozproszone i hybrydowe wdrożenia, z opcją scentralizowanego widoku w jednej konsoli.

**Częstotliwość aktualizacji**

Wydawane aktualizacje produktu, min. dwa razy w roku.

**Wsparcie produktu**

Wykonawca lub producent zapewni wsparcie 24x7x365.

## Sejf ogniotrwały

Sejf do przechowywania nośników kopii zapasowych

|  |  |
| --- | --- |
| Przeznaczenie | przeznaczony do mocnej ochrony przed włamaniem oraz ogniem |
| Klasa odporności | klasa II |
| Wymiary maksymalne | Wysokość – 100 mmSzerokość – 550 mmGłębokość – 450 mm |
| Ochrona antywłamaniowa | wg EN 1143-1 |
| Odporność ogniowa | 60 min LFS 60P (E-CBS) wg EN 15569 |
| Drzwi i korpus sejfu | - drzwi i korpus wzmocnione ognioodpornymwypełnieniem - wielopłaszczowa schodkowa konstrukcja drzwii korpusu - „sejf w sejfie”- grubość drzwi - 110 mm, grubość ścian - 90 mm- blokada termiczna zabezpieczająca szczelinę pomiędzy obudową i drzwiami przed ogniem i wysoką temperaturą |
| Zamek | - zamek kluczowy klasy A- zamek zabezpieczony przed rozwierceniem- certyfikaty IMP, VdSm ECB-S- możliwość kombinacji klucza 25.000 - 1.000.000- dwa klucze w zestawie |
| Inne | - 4-stronne ryglowanie, podwójne rygle pionowe- blokada rygli w przypadku próby sforsowania sejfu |

## Licencje

W ramach postępowania należy dostarczyć wszystkie licencje wymagane do uruchomienia oraz użytkowania dostarczanych urządzeń i serwerów zgodnie z ich przeznaczeniem i niniejszym SIWZ. Licencje terminowe, subskrypcje, abonamenty, itp. muszą pozwalać na użytkowanie każdego elementu Systemu przez okres udzielonej gwarancji od dnia podpisania protokołu odbioru – jeśli dotyczy. Całe oprogramowanie oraz wszystkie licencje muszą być dostarczone w wersjach aktualnych na dzień składania ofert lub nowszych.

Ponadto, aby uruchomić wszystkie funkcjonalności e-Usług, Zamawiający wymaga dostarczenia licencji na użytkowanie silnika bazodanowego Oracle[[3]](#footnote-4) w wersji zgodnej z użytkowanym systemem HIS – CGM Clininet oraz CGM-ERP [*możliwe wykorzystanie licencji typu ASFU*]. Dodatkowo Wykonawca zobowiązany jest do dokonania migracji danych z obecnie używanego silnika bazodanowego - Sybase – do nowej bazy danych opartej o silnik Oracle. Wykonawca określi i dostarczy ilości i rodzaje licencji wymaganych do realizacji Projektu inne niż wymagane w SIWZ.

## Migracja bazy danych systemu HIS oraz ERP użytkowanego przez Zamawiającego

Przedmiotem zadania jest migracja z użytkowanych systemów CGM CLININET oraz CGM-ERP firmy CGM na dostarczony silnik bazy danych Oracle, celem podniesienia wydajności i skalowalności systemu. Proces migracji musi odbywać się ze szczególnym uwzględnieniem zachowania ciągłości pracy Zamawiającego i w ramach tego procesu wszelkie przestoje systemu muszą być zaplanowane i uzgodnione z Zamawiającym. W ramach procesu migracji Wykonawca jest zobowiązany do przeniesienia danych z użytkowanych instancji systemu na nowy dostarczany w ramach zamówienia silnik bazy danych, podłączenia systemu HIS oraz ERP w konfiguracji funkcjonalnej jaka istniała u Zamawiającego oraz uruchomienia systemu we wszystkich użytkowanych obecnie przez Zamawiającego aspektach to jest:

1. System musi być uruchomiony w zakresie wszystkich modułów.
2. Musi mieć możliwość zachowania ciągłości pracy wszystkich użytkowników. Jeżeli elementy interfejsu graficznego systemu i/lub przebiegu procesu ulegną zmianie w wyniku migracji Wykonawca jest zobowiązany w tych obszarach przeszkolić wszystkich użytkowników systemu.
3. Wykonawca jest zobowiązany do uruchomienia pełnego zakresu integracji z systemami obecnie zintegrowanymi z systemami HIS oraz ERP. Koszt ewentualnej modyfikacji integrowanych systemów stanowi koszt Wykonawcy i jest on w pełni odpowiedzialny za uruchomienie pełnych funkcjonalności integracji po wykonaniu migracji.

W ramach procesu migracji Wykonawca jest zobowiązany do wykonania następujących zadań:

1. Dostarczenia i instalacji systemów operacyjnych dla serwerów, biorąc pod uwagę specyfikę konfiguracyjną aktualnie funkcjonującego systemu i ustaloną na etapie analizy przedwdrożeniowej.
2. Dostarczenia i instalacji silnika bazy danych.
3. Wykonania audytu bieżącej instalacji systemu celem określenia szczegółowej listy elementów niestandardowych, które będą podlegały odtworzeniu na nowym środowisku bazy danych w szczególności raportów i wydruków używanych przez Zamawiającego,
4. Przedstawienia planu, harmonogramu migracji i projektu technicznego migracji do akceptacji Zamawiającego,
5. Wykonania zaakceptowanego planu migracji w szczególności zainstalowania, uruchomienia i wdrożenia systemu na nowej wydajnej bazie danych wraz ze wszystkimi elementami niezbędnymi do jego poprawnego funkcjonowania takimi jak: systemy operacyjne, serwery aplikacyjne, konfiguracja bazy danych.
6. Przeszkolenia administratorów Zamawiającego z nowej konfiguracji systemu oraz struktury bazy danych.
7. Przeniesienia wszystkich danych z użytkowanych systemów CGM CLININET oraz CGM-ERP na nową instancję bazy danych.
8. Wykonania testów potwierdzających poprawne funkcjonowanie wszystkich modułów aplikacji oraz potwierdzającymi prawidłowość działania raportów, wydruków i integracji z innymi systemami.
9. Przeszkolenia użytkowników w zakresie w jakim uległ modyfikacji interfejs graficzny użytkownika i/lub przebieg procesów w systemie.
10. Przedstawienie raportu z migracji zawierającego raporty z testów oraz potwierdzenie kompletnego przeniesienia danych pomiędzy systemami bazodanowymi (użytkowanym i zaoferowanym).
11. Uruchomienia i wdrożenia systemów Clininet oraz CGM-ERP na nowej wydajnej bazie danych wraz z asystą uruchomieniową w zakresie w jakim modyfikacji uległ interfejs graficzny użytkownika i/lub przebieg procesów w systemie.
12. Dołączenia dotychczas używanych serwerów (Sybase, MySQL) do posiadanej infrastruktury serwerów wirtualnych. Należy zapewnić wsparcie dla wspomnianej licencji na okres trwania projektu.

### Organizacja prac migracyjnych

W celu efektywnego prowadzenia prac projektowych w ramach migracji bazy HIS oraz CGM-ERP muszą zostać powołane odpowiednie struktury projektowe, zarówno po stronie Wykonawcy, jak również po stronie Zamawiającego, w skład której wejdą:

1. Kierownik Procesu migracji
2. Kierownik Zespołu ds. migracji danych
3. Kierownik Zespołu ds. testów

#### Kierownictwo Procesu migracji

W skład kierownictwa wchodzi Kierownik Procesu migracji ze strony Zamawiającego oraz Kierownik Procesu migracji ze strony Wykonawcy. Wykonawca i Zamawiający są zobowiązani do wskazania osób pełniących role Kierownika Procesu migracji.

Obowiązki Kierownika Procesu migracji ze strony Wykonawcy:

1. Wyznaczenie osób upoważnionych do realizacji przedmiotu umowy.
2. Lista osób upoważnionych zostanie przekazana Kierownikowi Procesu migracji ze strony Zamawiającego bezzwłocznie po podpisaniu umowy oraz bezzwłocznie po każdej zmianie osób upoważnionych.
3. Nadzór nad czynnościami realizowanymi, w ramach realizacji przedmiotu umowy, przez osoby upoważnione o których mowa w pkt. 1, w szczególności w zakresie zgodności z postanowieniami umowy.
4. Przygotowywanie planów etapów i ewentualnych planów awaryjnych dla Procesu migracji.
5. Przygotowywanie harmonogramu realizacji.
6. Zgłaszanie, zatwierdzanie gotowości do odbioru usług Kierownikowi Procesu migracji ze strony Zamawiającego.
7. Zgłaszanie potrzeby konsultacji i doradztwa w zakresie realizacji.
8. Nadzór i kontrola realizacji prac i zobowiązań zgodnie z uzgodnionymi terminami.
9. Prowadzenie i archiwizowanie dokumentacji zdarzeń i czynności wykonanych w ramach realizacji umowy, pozwalających na ustalenie faktów związanych m.in. ze zlecaniem, odbiorem i rozliczeniem usługi migracji.
10. Zapewnienie odpowiedniego zastępstwa na czas swojej nieobecności z poinformowaniem Kierownika Procesu migracji ze strony Zamawiającego.
11. Przedkładanie informacji Kierownikowi Procesu migracji ze strony Zamawiającego zgodnie z jego potrzebami.
12. Przedkładanie wniosków, sugestii i propozycji Kierownikowi Procesu migracji ze strony Zamawiającego zgodnie z potrzebami.
13. Realizowanie we współpracy z Kierownikiem ze strony Zamawiającego wszystkich zadań związanych z procesem zarządzania migracją.
14. Kontrola zakresu Procesu migracji.
15. Zarządzanie ryzykiem.
16. Wspólna z Kierownikiem Procesu migracji ze strony Zamawiającego kontrola realizacji Procesu migracji, w szczególności w obszarach prac wykonywanych przez pracowników Wykonawcy.
17. Wspólne z Kierownikiem Procesu migracji ze strony Zamawiającego rozwiązywane istotnych kwestii pojawiających się podczas prac procesowych; nadzór nad Liderami Zespołów Procesu migracji.
18. Koordynacja przeprowadzenia odbioru prac w Procesie migracji. W przypadku powstania kwestii spornych między stronami zaangażowanymi w realizację Procesu migracji Kierownik powinien być stroną rozstrzygającą o najlepszym rozwiązaniu.

Obowiązki Kierownika Procesu migracji ze strony Zamawiającego:

1. Współpraca z Wykonawcą w realizacji przedmiotu umowy.
2. Bezzwłoczne rozstrzyganie spraw spornych pomiędzy zespołami ze strony Zamawiającego oraz Wykonawcą.
3. Określenie formy sprawozdań przedstawianych przez Kierownika Projektu migracji ze strony Wykonawcy.
4. Zatwierdzanie planów etapów i ewentualnych planów awaryjnych.
5. Zatwierdzanie harmonogramu Procesu migracji.
6. Przyjmowanie i akceptacja protokołów odbioru z realizacji etapów migracji.
7. Prawo i obowiązek formalnego zgłoszenia żądania zmiany jeżeli uzna, że dla zapewnienia prawidłowej realizacji migracji konieczne jest podjęcie działań mających wpływ na ustalony zakres prac.
8. Przegląd, zgłaszanie uwag, akceptacja oraz odbiór poszczególnych etapów migracji.
9. Zarządzanie i kontrola zakresu Procesu migracji - wspólne z Kierownikiem Procesu migracji ze strony Wykonawcy zarządzanie zakresem prac realizowanych w ramach Procesu migracji.
10. Zarządzanie jakością - w rozumieniu jakości realizacji Procesu migracji oraz jakości dostarczanych produktów prac, w ścisłej współpracy z Kierownikiem Procesu migracji ze strony Wykonawcy
11. Nadzór nad pracownikami Zamawiającego.
12. Zarządzanie komunikacją - zapewnienie odpowiedniego procesu informacyjnego dotyczącego prowadzonych prac i ich wyników oraz wspólnego z Kierownikiem ze strony Wykonawcy.
13. Zarządzanie ryzykiem - w ścisłej współpracy z Zespołami Procesu migracji Zamawiającego i Kierownikiem Procesu migracji ze strony Wykonawcy.
14. Zapewnienie zasobów ze strony Zamawiającego koniecznych do terminowego i zgodnego z założeniami wykonania prac.

Do obowiązków Lidera Zespołu Procesu migracji należy koordynowanie prac w ramach zadań Zespołu zgodnie z przyjętym zakresem i harmonogramem zdefiniowanym dla danego obszaru prac. W szczególności do obowiązków Lidera należy:

1. Zarządzanie pracą specjalistów pracujących w ramach danego Zespołu poprzez precyzyjne wyznaczanie celów i zadań.
2. Informowanie Kierownictwa Procesu migracji o postępie prac oraz ewentualnych ryzykach związanych z ich realizacją w części, za którą odpowiada.
3. Opiniowanie i podejmowanie decyzji w zakresie założeń oraz koncepcji przedstawianych przez Zespół.
4. Ocena jakości realizowanych prac.
5. Operacyjne zarządzanie czasem pracy specjalistów Zespołu.
6. Zarządzanie harmonogramem pracy danego Zespołu.
7. Przekazywanie produktów do akceptacji Kierownictwa Procesu migracji.
8. Opiniowanie prac z zakresu pracy Zespołu wykonanych przez Wykonawcę.

#### Opis sposobu zarządzania ryzykiem w procesie migracji

Kierownik procesu migracji ze strony Wykonawcy musi opracować i przedstawić Kierownikowi Procesu migracji ze strony Zamawiającego do akceptacji rejestr zagrożeń i środków zaradczych, gdzie identyfikowane i kategoryzowane są poszczególne czynniki ryzyka za pomocą poziomu wpływu na proces migracji, prawdopodobieństwa wystąpienia, priorytetu, daty powstania i zamknięcia, właściciela ryzyka, opisu ryzyka, kategorii, wymaganych środków zaradczych, statusu. Rejestr ten musi być na bieżąco w ramach potrzeb aktualizowany.

#### Opis sposobu komunikacji Wykonawcy z Zamawiającym

Podczas przeprowadzenia migracji bazy danych systemu HIS oraz ERP muszą obowiązywać następujące założenia dotyczące wzajemnej współpracy Zamawiającego i Wykonawcy:

1. Komunikacja między uczestnikami Procesu migracji po stronie Wykonawcy i Zamawiającego musi odbywać się na poziomie Kierowników Procesu migracji obu stron oraz Liderów Zespołów i wyznaczonych osób po stronie Zamawiającego.
2. Przewiduje się wykorzystanie różnych mediów komunikacyjnych uzależnionych od poziomu oraz wagi uzgodnień. Podstawowym środkiem komunikacji w ramach prac roboczych uczestników Procesu migracji musi być poczta elektroniczna, kontakt telefoniczny i telekonferencje, z zastrzeżeniem że jeżeli podczas rozmowy podjęte zostaną istotne ustalenia muszą one zostać potwierdzone poprzez e-mail.
3. Prace wspólne specjalistów po obu stronach (spotkania w ramach analizy przedwdrożeniowej, testy odbiorcze, szkolenia) muszą być każdorazowo potwierdzone przedstawioną przez Wykonawcę i podpisaną przez obie strony, notatką ze spotkania, zawierającą: listę uczestników, wykonanych zadań, opisem poruszanych zagadnień, czy ustaleniami.
4. Spotkania poświęcone kontroli realizacji wdrożenia muszą być organizowane w miarę bieżących potrzeb na życzenie Zamawiającego. Wykonawca będzie odpowiedzialny za przedstawienie raportu o bieżącym zaawansowaniu prac i informacji o zagrożeniach w realizacji procesu migracji oraz sposobach rozwiązywania tych problemów. Spotkania dotyczące kontroli realizacji Procesu migracji również muszą być potwierdzone notatką ze spotkania podpisaną przez Strony.
5. Zgłoszenie zagadnienia wymagającego decyzji Kierownika Procesu migracji przez Wykonawcę musi zachować formę pisemną.

#### Zgłoszenie zmiany w pracach migracyjnych

1. Potrzeba wprowadzenia zmian musi wynikać między innymi z:
2. potrzeb, które zostały błędnie zdefiniowane, nie zostały zdefiniowane lub uległy zmianie w trakcie przebiegu Procesu migracji. W szczególności dotyczy to potrzeby zmian lub rozszerzeń funkcjonalności systemu - związanych z dopasowaniem funkcjonalności systemu do specyficznych potrzeb Zamawiającego w zakresie realizacji procesów biznesowych,
3. zaakceptowanego przez strony sposobu neutralizacji ryzyka procesu migracji,
4. wprowadzenia w trakcie wdrożenia zmian organizacyjnych u Zamawiającego, które mają wpływ na zatwierdzony sposób realizacji procesów biznesowych,
5. konieczności wprowadzenia zmian w zatwierdzonych etapach przedmiotu umowy.
6. Potrzebę zmiany będą mieli prawo i obowiązek zgłosić Kierownicy Procesu migracji ze strony Zamawiającego i Wykonawcy, jeżeli uznają, że dla zapewnienia prawidłowej realizacji migracji konieczne jest podjęcie działań mających wpływ na ustalony zakres prac.
7. Żądanie zmiany musi być dokumentowane przez zgłaszającego za pomocą formularza żądania zmiany. Wykonawca w terminie 5 dni roboczych dokonuje analizy zmiany na dokumentację Procesu migracji i przedstawia ją Kierownikowi Procesu migracji ze strony Zamawiającego. Po zapoznaniu z analizą Kierownik Procesu migracji Zamawiającego ma prawo przyjąć bądź odrzucić zmianę. Zmiany dotyczące harmonogramu procesu migracji muszą być zatwierdzone przez Kierownika Procesu migracji po stronie Zamawiającego.

#### Przebieg procesu migracji

Harmonogram realizacji Procesu migracji baz danych systemów CGM CLININET oraz CGM-ERP musi obejmować:

1. **Analizę przedwdrożeniową migracji** - opracowanie planu migracji i projektu technicznego migracji systemów HIS oraz CGM-ERP - w terminie nie dłuższym niż 14 dni kalendarzowych od dnia zawarcia Umowy.

Punkt ten musi zawierać następujące elementy:

1. uruchomienie Procesu migracji po stronie Wykonawcy,
2. przedstawienie harmonogramu prac procesowych,
3. powołanie struktury procesowej po stronie Wykonawcy i przedstawienie jej.

Przedstawienia planu migracji oraz projektu technicznego migracji zawierającego następujące elementy:

1. harmonogram procesu migracji danych,
2. analizę ryzyka związanego z procesem migracji wraz z planami odpowiedzi minimalizującymi ich wystąpienie,
3. opis konfiguracji obecnego systemu,
4. opis konfiguracji docelowego systemu,
5. szczegółowy opis procesu migracji danych ze szczególnym uwzględnieniem sposobów w jaki sposób Wykonawca chce zapewnić:
* kompletność i wiarygodność danych podlegających migracji,
* bezpieczeństwo danych podlegających migracji,
* zabezpieczenie ciągłości pracy Zamawiającego,
* integrację z innymi systemami,
1. przebieg i szczegółowy opis procedury testowej poprawności migracji,
2. szablon raportu z migracji systemu.

**2. Dostawę i instalacja oprogramowania** zakupionego w ramach przedmiotu zamówienia w terminie uzgodnionym na etapie analizy przedwdrożeniowej. Punkt ten musi obejmować następujące elementy:

1) instalacja i konfiguracja obejmie zarówno systemy operacyjne jak i serwery baz danych,

2) dostawa, instalacja i konfiguracja oprogramowania.

**3. Wykonanie procesu migracji** baz danych systemów CGM CLININET oraz CGM-ERP na wydajną bazę danych, uruchomienie i wdrożenie systemu w nowej konfiguracji w terminie uzgodnionym na etapie analizy przedwdrożeniowej.

1. Wykonanie zaakceptowanego planu migracji w szczególności zainstalowania, uruchomienia
i wdrożenia systemu na nowej wydajnej bazie danych wraz ze wszystkimi elementami niezbędnymi do jego poprawnego funkcjonowania takimi jak: systemy operacyjne, serwery aplikacyjne, konfiguracja bazy danych, konfiguracja sieci, konfiguracja i wdrożenie backupów.
2. Przeniesienia wszystkich danych z użytkowanych systemów CGM CLININET oraz CGM-ERP na nową instancję bazy danych.
3. Wykonania testów potwierdzających poprawne funkcjonowanie wszystkich modułów systemu oraz potwierdzającymi prawidłowość działania raportów, wydruków i integracji z innymi systemami.
4. Przeszkolenie administratorów wskazanych przez Zamawiającego ze struktury nowej bazy danych i udostępnienie jej do odczytu, w celu konwersji obecnie istniejących raportów, formularzy i wydruków funkcjonujących u Zamawiającego.
5. Przeszkolenia użytkowników w zakresie w jakim modyfikacji uległ interfejs graficzny użytkownika i/lub przebieg procesów w systemie.
6. Przedstawienie raportu z migracji zawierającego raporty z testów oraz potwierdzenie przeniesienia danych pomiędzy systemami.
7. Uruchomienia i wdrożenia systemu na nowej wydajnej bazie danych wraz z asystą uruchomieniową w obszarach w jakich modyfikacji uległ interfejs graficzny użytkownika i/lub przebieg procesów w systemie.
8. Osiągnięcie średniego czasu reakcji Systemu <= 1s.

##### Analiza przedwdrożeniowa Procesu migracji

W zakresie analizy przedwdrożeniowej Procesu migracji Wykonawca zobowiązany będzie do:

1. Przeprowadzenia audytu istniejącego rozwiązania celem identyfikacji i inwentaryzacji konfiguracji elementów niestandardowych systemu HIS oraz ERP użytkowanego przez Zamawiającego w szczególności:
2. raportów,
3. wydruków,
4. formularzy,
5. integracji z innymi systemami,
6. bieżącej konfiguracji systemów HIS oraz CGM-ERP,
7. konfiguracji procedur backupu systemów HIS oraz CGM-ERP.

Wszystkie elementy wynikające z audytu muszą zostać uwzględnione w planie migracji systemu. Warunkiem zaakceptowania planu migracji a następnie jej realizacji jest pełne odtworzenie istniejącej funkcjonalności obecnego systemu również w zakresie elementów niestandardowych wymienionych w pkt a-f. Zamawiający zastrzega sobie prawo rezygnacji z przenoszenia wybranych raportów i wydruków. Decyzja w tym zakresie jest wyłączną kompetencją Zamawiającego i zostanie określona na etapie analizy przedwdrożeniowej Procesu migracji.

1. Opracowania planu migracji – Plan migracji musi opisywać proces migracji danych z obecnie użytkowanej bazy do wydajnej bazy danych dostarczanej w ramach tego zamówienia i musi zawierać minimum następujące elementy:
2. wskazanie osób odpowiedzialnych za realizację planu i poszczególnych zadań po stronie Wykonawcy,
3. wskazanie zadań leżących po stronie Wykonawcy,
4. wskazanie zadań leżących po stronie Zamawiającego,
5. szczegółowy harmonogram planowanych prac ze szczególnym uwzględnieniem sytuacji w której obecnie użytkowany system będzie niedostępny,
6. opracowanie projektu technicznego migracji systemów HIS oraz ERP.
7. Opracowanie planu testów akceptacyjnych migracji systemu zawierającego:
8. plan testów,
9. scenariusze testowe.

##### Migracja danych

Wykonawca jest odpowiedzialny za przeprowadzenie pełnego procesu migracji danych pomiędzy obecnie użytkowaną bazą SYBASE ASE systemu HIS oraz używaną bazą danych MySQL systemu CGM-ERP a nową wydajną dostarczaną bazą danych.

Zamawiający na etapie realizacji umowy zapewni Wykonawcy dostęp do bazy danych obecnie użytkowanego systemu. Zamawiający zastrzega, że nie jest twórcą dokumentacji systemu HIS CGM CLINIENT oraz CGM-ERP i nie może odpowiadać za kompletność przekazanej dokumentacji. Zamawiający zastrzega, że ewentualne luki w dokumentacji struktury bazy danych nie stanowią podstawy dla Wykonawcy dla zaprzestania lub zmniejszenia zakresu migracji danych ani do przesunięcia wymaganych terminów realizacji zadania. Zamawiający do przeprowadzenia migracji bazy danych udostępni interfejs administracyjny serwerów baz danych w trybie odczytu. Wykonawca nie może ingerować w dane ani strukturę danych jak i samych baz danych obecnie użytkowanych systemów HIS CGM CLININET oraz CGM-ERP w celu przeprowadzenia procesu migracji danych.

Szczegółową konfigurację uwzględniającą również powiązanie z istniejącą infrastrukturą Zamawiającego Wykonawca zaprojektuje i przedstawi do akceptacji Zamawiającego w procesie analizy przedwdrożeniowej migracji w projekcie technicznym migracji.

W ramach konfiguracji środowiska systemu Wykonawca będzie odpowiedzialny za konfigurację serwerów i systemów zgodnie z uzgodnionym projektem technicznym migracji.

W procesie wymagane jest planowanie i przeprowadzenie procesu migracji danych przez Wykonawcę przy uwzględnieniu minimum następujących faz/kroków:

**1. Przygotowanie planu migracji danych** ‐ ustalenie zakresu danych do migracji, sposoby i zakres danych do poprawienia, struktury pośrednich, sposobu przekazania danych, sposobów weryfikacji i innych szczegółów potrzebnych do prawidłowej migracji wszystkich danych wymaganych przez Zamawiającego. Szczegółowy opis wymagań dla planu migracji zawarto w rozdziale „Analiza przedwdrożeniowa Procesu migracji”

**2.** **Pobranie danych do struktur pośrednich** – czynność musi dotyczyć przygotowania i wykonania uzgodnionych w planie migracji skryptów pobierających dane do struktur pośrednich (np. testowa baza danych, pliki XML) i eksportu danych do tych struktur.

**3. Weryfikacja poprawności danych w strukturach pośrednich** – weryfikacja poprawności procesu exportu danych z systemu źródłowego i importu do struktur pośrednich. W przypadku wystąpienia błędów przy weryfikacji danych w strukturach pośrednich, musi zostać ustalona przyczyna błędu. Jeżeli przyczyna leży w złym pobraniu danych z systemu źródłowego proces musi powrócić do kroku „Pobranie danych do struktur pośrednich”. Jeżeli problem dotyczy błędu w procedurach importu danych Wykonawca musi poprawić te procedury i ponownie dokonać importu i weryfikacji danych.

**4. Migracja testowa** - w celu realizacji migracji testowej Wykonawca zobowiązany jest do wykonania kopii docelowego środowiska wydajnej bazy danych na infrastrukturze Zamawiającego i przeprowadzenia kompletnego zasilania danymi tego środowiska za pomocą skryptów i algorytmów, które będą wykorzystywane przy docelowej migracji. Celem migracji testowej jest przetestowanie procedur eksportu/importu danych, procedur czyszczenia, uzupełniania, agregacji danych, procedur weryfikacji danych. Migracja testowa co do zasady musi być wykonywana na pełnych danych. Dopuszcza się w niektórych szczególnie wymagających obszarach (ze względu na liczbę danych) realizację migracji testowej na reprezentatywnej próbce danych, po wcześniejszym ustaleniu i zgodzie Zamawiającego.

**5.** **Weryfikacja migracji testowej** – w ramach procesu weryfikacji procesu migracji testowej Zamawiający wymaga wykorzystania następujących metod sprawdzania poprawności jej wykonania:

1. **Szczegółowa weryfikacja zapis po zapisie**

Zastosowanie jest możliwe tylko wtedy, jeżeli zbór migrowanych danych nie jest liczny i polega na porównaniu danych w starym rozwiązaniu oraz w nowym Systemie zapis po zapisie. Dla ułatwienia tego porównania Dostawca Systemu może przygotować zestawienia tabelaryczne danych z nowego systemu eksportowanie do arkusza kalkulacyjnego lub wydrukowane. Wtedy porównanie musi polegać na zaznaczeniu każdego poprawnego zapisu na wydruku lub w arkuszu.

1. **Porównanie skryptami**

Weryfikacja musi polegać na uruchomieniu napisanych wcześniej skryptów porównujących dane znajdujące się w nowym Systemie z danymi źródłowymi zapisanymi w tabelach systemu testowego i źródłowego. W takim przypadku raport zgodności / różnic musi być automatycznie wygenerowany przez dostarczone skrypty.

1. **Wyrywkowa kontrola danych przez użytkowników**

Weryfikacja musi zostać przeprowadzana przez użytkowników docelowych Systemu, mających dostęp do nowego środowiska testowego Systemu oraz Systemu źródłowego. Proces ten będzie polegał na wyszukaniu wybranych danych w jednym i drugim systemie oraz ich porównaniu. Wykonawca wykonana na środowisku testowym uzgodniony na etapie analizy przedwdrożeniowej zestaw testów funkcjonalnych systemu i przedstawi Zamawiającemu raport z ich realizacji. Dodatkowo Wykonawca udostępni wskazanym pracownikom Zamawiającego środowisko testowe na okres min. 2 tygodni tak by mogli oni sprawdzić poprawność działania systemu po migracji wyżej opisaną metodą.

1. **Porównanie raportów i wydruków z Systemu źródłowego oraz Systemu testowego**

Proces ten musi polegać na uruchomieniu i porównaniu wybranych raportów/wydruków wygenerowanych z Systemu testowego oraz Systemu źródłowego przez wskazane osoby przez Zamawiającego.

1. **Weryfikacja statystyczna**

Proces ten musi polegać na przygotowaniu kryteriów poprawności dla migrowanych danych np. liczby rekordów w obydwu systemach dla konkretnych tabel w bazie danych, wartość i liczby świadczeń przekazanych do NFZ itp. Wykonaniu przez dostawcę zestawień porównawczych z obydwu systemów, które umożliwią stwierdzenie poprawności migracji.

W ramach testowania poprawności migracji muszą zostać zrealizowane minimum następujące testy:

1. Testy funkcjonalne
2. Testy integracji

**6. Migracja docelowa produkcyjna** – właściwa migracja, po której musi rozpocząć się produkcyjna praca w nowym Systemie. W przypadku braku stwierdzonych istotnych problemów w trakcie wcześniejszych kroków procesu migracji Zamawiający podejmie decyzję o przeprowadzeniu procesu migracji do nowego, docelowego Systemu opartego o wydajną bazę danych. Wykonawca po procesie migracji jest zobowiązany do weryfikacji poprawności przeniesionych danych – końcowa weryfikacja danych poprzez wykonanie testów poprawności migracji (walidacji danych po migracji) oraz testów wydajności. Pozytywny wynik kończy proces migracji danych.

Wykonawca zobowiązany jest zabezpieczyć trwale dane z systemu źródłowego z momentu migracji danych w postaci kopii bezpieczeństwa danych systemu źródłowego i w przypadku niepowodzenia procesu migracji w założonym harmonogramie przywrócić działanie poprzedniego systemu. Kopie danych oraz systemu w wersji użytkowanej przez Zamawiającego w liczbie sztuk 2 muszą zostać przekazane Zamawiającemu.

Wykonawca musi przeprowadzać migracje w siedzibie Zamawiającego. W przypadku, gdy nie będzie to możliwe, Wykonawca zobowiązany jest do zabezpieczenia pozyskanych od Zamawiającego migrowanych danych w sposób uniemożliwiający wejście w ich posiadanie przez osoby nieupoważnione do ich przetwarzania. Po wykonaniu migracji, wszelkie dane pozyskane w toku migracji przez Wykonawcę zamówienia muszą zostać usunięte ze wszystkich nośników Wykonawcy w sposób uniemożliwiający ich odzyskanie. Jeżeli wystąpi konieczność przekazania Wykonawcy danych do migracji poza siedzibę Zamawiającego, przekazanie musi odbywać się protokolarnie upoważnionemu przedstawicielowi Wykonawcy, a prace związane z obróbką pozyskanych danych odbywać się muszą jedynie w siedzibie Wykonawcy. Wykonawca nie jest upoważniony do przekazywania danych z migracji innym podmiotom.

Dodatkowe wymagania dla procesu migracji zawiera poniższa tabela:

|  |  |
| --- | --- |
| Nr wymagania  | Opis  |
| MIG.001  | W ramach procesu migracji Wykonawca zobowiązany jest do zachowania ciągłości procedur i procesów realizowanych przez Zamawiającego w szczególności musi zachować ciągłość i format wszystkich numeracji stosowanych w procesach leczenia (nr księgi głównej, ksiąg zabiegowych, nr kartotek pacjentów itp.)  |
| MIG.002  | W procesie migracji muszą zostać przeniesione wszystkie dane historyczne zgromadzone i przetwarzane obecnie przez Zamawiającego w systemach HIS CGM CLININET oraz CGM-ERP. |
| MIG.003  | Proces migracji musi zapewnić ciągłość rozliczeń z NFZ zarówno w zakresie nowych danych prowadzanych do zmigrowanego Systemu jak i korekty danych wcześniej przekazanych do płatnika.  |
| MIG.004  | Wykonawca musi wykonać migrację danych do nowej wydajnej bazy danych zgodnie z zaakceptowanym planem migracji danych. Wykonawca jest odpowiedzialny za wykonanie migracji wszystkich danych potrzebnych do prawidłowego działania Systemu.  |
| MIG.005  | Proces migracji nie może zaburzyć wzajemnych powiązań logicznych danych. Wzajemne relacje pomiędzy danymi w systemie muszą być zachowane.  |
| MIG.006  | Migracja musi być przeprowadzona w dwóch etapach: * migracja testowa
* migracja produkcyjna.
 |
| MIG.007 | Warunkiem możliwości wykonania migracji produkcyjnej jest akceptacja przez Zamawiającego wyników migracji testowej na podstawie raportu z testów migracji przedstawionego przez Wykonawcę.  |
| MIG.008  | Wykonawca ponosi odpowiedzialność za poprawność danych migrowanych do nowego Systemu i jest zobowiązany bez zbędnej zwłoki usunąć wszelkie skutki wynikające z błędów migracji i dokonać naprawy danych i działania Systemu nawet w przypadku jeżeli nieprawidłowości wystąpią w procesie eksploatacji systemu po odbiorze procedury migracji. Zobowiązanie to dotyczy całości trwania okresu umowy |

### Odbiór procesu migracji

W ramach realizacji przedmiotu umowy Wykonawca zobowiązany jest przeprowadzić zestaw testów potwierdzających poprawność wykonania migracji. W skład testów realizowanych w ramach procesu migracji systemów HIS oraz CGM-ERP powinny zostać zrealizowane minimum następujące testy:

**Testy funkcjonalne** – zestaw testów potwierdzających możliwość realizacji kluczowych procesów na środowisku systemu po migracji na nowy silnik bazy danych.

**Testy wydajnościowe** – testy mające na celu potwierdzenie, że założone w procesie migracji wskaźniki zwiększenia wydajności systemu poprzez migrację na nowy silnik bazy danych zostały osiągnięte.

**Testy integracji** – testy potwierdzające zdolność systemu po migracji do współpracy z innymi systemami dla których konieczność integracji została opisana OPZ.

## Przygotowanie i dostarczenie dokumentacji projektowej oraz powykonawczej

Zamawiający wymaga, aby Wykonawca dostarczył do każdego przekazanego elementu systemu dokumentację Administratora – zawierająca opis wymaganych czynności i działań związanych z instalacją i konfiguracją danego elementu, a także opis wymagań odnośnie konfiguracji środowiska eksploatacyjnego (platformy sprzętowej, systemowej, bazodanowej i aplikacyjnej). Dokumentacja musi zawierać wszystkie niezbędne loginy, hasła, kody dostępu, itp. pozwalające na odtworzenie pełnego zakresu systemu po awarii, zarządzanie w pełnym zakresem dostarczonym rozwiązaniem oraz pełnienie usługi serwisu przez inny podmiot po okresie trwałości projektu.

Zamawiający wymaga, aby Wykonawca dostarczył do każdego przekazanego elementu systemu dokumentację Użytkownika – opis działania danego elementu Systemu w zakresie niezbędnym do jego prawidłowego użytkowania przez personel skierowany do jego użytkowania.

Dokumentacja musi być sporządzona w języku polskim i dostarczona w wersji elektronicznej z możliwością przeszukiwania treści.

# Etap II – Adaptacja budowlana serwerowni

### Informacje ogólne

Zamawiający wymaga aby Wykonawca przygotował pomieszczenie serwerowi zgodnie z załączonymi do SIWZ dokumentami (m.in.: program funkcjonalno-użytkowy). Wszelkie prace budowlane należy uzgodnić z Zamawiającym co do terminu i godzin pracy.

Uzyskanie wszelkich pozwoleń, zgód, dopuszczeń w tym pozwolenie na budowę, zmiana sposobu użytkowania, itp. leży po stronie wykonawcy.

Zadaniem okablowania strukturalnego, wymaganego to utworzenia w ramach projektu, jest połączenie dwóch serwerowni (istniejącej z wykonywaną) kablami światłowodowymi w celu zabezpieczenia infrastruktury przetwarzania danych. Instalację należy wykonać kablem multimodowym min. dwudziesto-cztero włóknowym, zawierającym niepodtrzymujące palenia powłoki ochronne przeznaczone do instalacji wewnątrz budynku. Oba końce tras optycznych należy zakończyć adapterami LC/APC w przełącznicach światłowodowych zamontowanych w szafach 19” RACK (Przełącznica 1U 19'' 12xLC duplex - wysuwalna).

Zamawiający wymaga dostarczenia kompletu kompatybilnych multimodowych patchcordów światłowodowych (LC/APC duplex) w dwóch długościach: 3mb oraz 5mb.

Instalację miedzianą należy wykonać kablami miedzianymi (*pot. „skrętka”*) w kategorii min. 6.

Instalacja strukturalna prowadzona musi być w korytach ochronnych PCV.

### Instalacja elementów w modernizowanej serwerowni zapasowej

Wykonawca zobowiązany jest do instalacji [tj. wypakowane, zmontowane, zamontowane w szafach RACK lub na biurkach, uruchomione i skonfigurowane] wszystkich dostarczonych elementów infrastruktury IT w miejscy wskazanym przez Zamawiającego w terminie wskazanym przez Zamawiającego [miejsce i termin instalacji należy uzgodnić na min. 2 dni robocze przed planowaną dostawą urządzeń]. Wykonawca zobowiązany jest dostarczyć wszystkie elementy niezbędne do instalacji i uruchomienia sprzętu (np. szyny, kable, przewody, panele, maskownice, śruby, baterie, itp.). Cały sprzęt musi zostać zainstalowany i uruchomiony zgodnie z zaleceniami producenta i zabezpieczony przed nieautoryzowanym dostępem. Wykonawca odpowiedzialny jest za odpowiednie zabezpieczenie (również fizyczne, np. kontrola dostępu, monitoring, itp.) dostarczonego sprzętu w trakcie prowadzonych prac – do momentu odbioru. Dostarczony sprzęt musi być monitorowany pod kątem bezpieczeństwa fizycznego (np. ciągły monitoring wizyjny oraz monitorowanie parametrów fizycznych – temperatura, wilgotność, zalanie, włamanie, itp.). Wykonawca odpowiedzialny jest za zapewnienie odpowiednich warunków niezbędnych do prawidłowego podłączenia całego dostarczonego sprzętu (np. modernizację rozdzielnicy elektrycznej, podłączenie światłowodów, itp.). Zamawiający zaleca wykonanie wizji lokalnej w celu uwzględnienia wszystkich niezbędnych w ofercie elementów/kosztów.

Wszystkie urządzenia i systemy operacyjne serwerów muszą być zsynchronizowane z serwerem czasu.

#### Klimatyzatory

Należy dostarczyć zestaw redundantnych klimatyzatorów pracujących min. w dwóch trybach: naprzemiennym i rezerwy. Sterowanie klimatyzatorami należy zainstalować na ścianie wewnątrz serwerowni przy drzwiach wejściowych. Jednostki wewnętrzne klimatyzacji należy zamontować zgodnie z przepływem powietrza w urządzeniach zainstalowanych w szafach – „F2B”. Skropliny należy wyprowadzić na zewnątrz budynku – jeśli wymagane będzie zastosowanie pompki skroplin, należy ją dostarczyć i zainstalować. Jednostkę zewnętrzną należy zamontować zgodnie z zaleceniami producenta na dedykowanym stelażu.

* Parametry minimalne klimatyzacji:
* Moc chłodząca klimatyzatora min. 6kW,
* Klasa efektywności energetycznej min. A++,
* Maksymalny pobór mocy elektrycznej: 4kW,
* Zakres temperatur pracy jednostki zewnętrznej (chłodzenie): -15 ~ +40°C,
* System klimatyzacji musi umożliwiać zdalne sterowanie za pomocą sieci LAN/WiFi.

Wszystkie kable i przewody należy ułożyć w istniejących kanałach wentylacyjnych.

Jeśli do prawidłowej pracy klimatyzacji niezbędne będą do wykonania jakiekolwiek dodatkowe prace instalacyjne Wykonawca musi je uwzględnić w cenie oferty. Jednostki zewnętrzne należy zainstalować na dachu.

#### Wideomonitoring

Wykonawca dostarczy dedykowany system wideo-monitoringu. Rejestrator należy zainstalować w serwerowni w szafie RACK. Kamery należy zainstalować tak aby zminimalizować do absolutnego minimum występowanie martwych punktów – niedopuszczalne jest występowanie martwych punktów bezpośrednio przy drzwiach oraz przy oknie.

Parametry minimalne kamer CCTV:

* Typ: kamera IP, kopułowa
* Rozdzielczość: min. 8MPix przy min. 15 k/s
* Matryca min. 1/2.5”
* Obiektyw o ogniskowej ok. 3mm +/- 10% F2,
* Kompresja: min. H.265 / H.264 / MJPEG
* Promiennik podczerwieni o zasięgu min 20m,
* Stosunek S/N: min. 40 dB
* Zasilanie PoE lub 12VDC,

Kamery montowane na zewnątrz pomieszczenia serwerowni muszą być wandaloodporne.

Parametry minimalne rejestratora wideo:

* Kontrola: mysz, klawiatura, sieć
* Obsługa kamer IP: min. 8 kanałów
* Strefy prywatności: 4 definiowane strefy detekcji na każdym kanale
* Podział ekranu: 1 / 4 / 8
* OSD: min.: nazwa kamery, czas, zanik video, blokada kamery, detekcja ruchu, nagrywanie
* Nagrywanie w rozdzielczościach: 8Mp, 6Mp, 5Mp, 4Mp, 3Mp, 1080p
* Kompresja : min. H.265 / H.264 / MJPEG
* Jakość CBR, VBR (1~6 poziomów)
* Zajętość pasma : 16kbps ~ 20Mbps, max birate 320Mbps
* Priorytet nagrań : ręczne > alarm > MD > regularne
* Interwały nagrań : 1~120 min. , 1~30 sek. - pre-record, 1~300 sek. - post-record
* Tryby nagrań: ręczne / terminarz (regularne (ciągłe)) / MD (video detekcja ruchu, zanik, zasłonięcie, alarm) / stop
* Funkcje odtwarzania: wolny/szybki/zwykły, play, pause, tył/przód, następny/poprzedni plik, następna/poprzednia kamera, pełny ekran, powtórzenie, archiwizacja, cyfrowy zoom
* Archiwizacja: pendrive / USB HDD / USB CD&DVD-RW / ściąganie przez sieć
* Detekcja ruchu strefy: min. 300, z funkcją ustawienia czułości,
* Wyzwalanie zdarzeń: nagrywanie, alarm, FTP, e-mail, buzzer i komunikaty ekranowe
* Obsługa dysków HDD: min. 2x SATA III, pojemność łączna pozwalająca na przechowywanie materiału wideo monitoringu przez około 90 dni z wszystkich kamer w ich pełnej rozdzielczości.
* Interfejsy: 1x HDMI 4K, 1x VGA, 1x USB 2.0, 1x USB 3.0, RS232, 1x RJ-45 10/100/1000Mbps
* Switch PoE: min. 8 portów IEEE802.3af/at
* Wymiary: 1U
* Zasilanie: 240 V AC.

#### Kontrola dostępu

Wykonawca zainstaluje system kontroli dostępu do pomieszczenia serwerowni. System kontroli dostępu będzie autonomicznym systemem umożliwiającym kontrolę dostępu do pomieszczeń sekcji IT. Centrala systemu kontroli dostępu musi zostać zainstalowana wewnątrz pomieszczenia serwerowni. Centrala musi posiadać własny system podtrzymywania zasilania. System musi posiadać mechanizm logowania zdarzeń dla wybranych lub wszystkich punktów logowania z retencją min. 1 roku [dopuszcza się skonfigurowanie systemu do ciągłego logowania do zewnętrznego systemu syslog]. System musi umożliwiać zdefiniowanie min. 10 użytkowników z różnymi prawami dostępu. System musi umożliwiać integrację z usługą Active Directory.

Nowe drzwi muszą zostać wyposażone w samozamykacze z blokadą otwarcia drzwi w zakresie min. od 90° do 140°. Kierunek otwierania każdych drzwi (lewe/prawe, do wewnątrz/na zewnątrz) należy ustalić z Zamawiającym przed montażem.

#### System monitorowania parametrów fizycznych

Pomieszczenie serwerowni należy wyposażyć w system monitorowania parametrów fizycznych, tj. min. temperatury, wilgotności, zalania, obecności dymu, wykrywania ruchu. System musi być wyposażony w moduł GSM powiadamiający wybranych odbiorców (min. SMS) o wybranych alarmach.

Wykonawca dostarczy i zainstaluje system składający się z min.:

* Centrali monitorującej z systemem zdalnego dostępu po sieci LAN/WLAN oraz modułem GSM,
* Czujników zalania / obecności wody – min. 2 szt. –w okolicy możliwych źródeł zalania,
* Czujników temperatury – min. 4 szt. (2 szt. w szafach RACK, 1 szt. pod sufitem, 1 szt. na ścianie na wysokości około 1,5m od posadzki),
* Czujnika otwarcia drzwi – 1 szt.,
* Detektorów ruchu – 2 szt.,
* Czujników/detektorów dymu,
* Czujników wibracyjnych lub zbicia szyby – min. 1 szt. zamontowany w każdym oknie,
* Syreny alarmowej zamontowanej na elewacji budynku.

##### Czujnik dymu, wilgotności i temperatury zainstalowany pod sufitem

Wrażliwość: 0,05 - 0,2 db/m;

Czas reakcji: około 10 sec +/- 20%;

Zakres pomiaru temperatury: -10 ÷ +80°C; z dokładnością pomiarów: max. 1°C;

Zakres pomiaru wilgotności: 0 - 95%RH; z dokładnością pomiarów: max. 3%RH;

Możliwość podłączenia za pomocą kabla RJ-12 do CAN wejścia jednostki sterującej lub do CAN wyjścia innego czujnika. Określenie rodzaju czujnika i połączenie musi następować automatycznie. System musi umożliwiać podłączenie kilku czujników do liniowego układu.

##### Czujnik temperatury wewnętrzny

Zakres pomiarowy: 0 ~ +80°C; Dokładność pomiarów: max. 1°C;

Możliwość podłączenia kablem RJ-11 do kontrolera. Identyfikacja rodzaju czujnika i połączenie musi następować automatycznie.

##### Czujnik zalania

Możliwość podłączenia za pomocą kabla RJ-11 do jednostki sterującej. Określenie rodzaju czujnika i połączenie musi następować automatycznie. Czujnik musi być dostarczony i podłączony z odpowiednim kablem detekcyjnym.

##### Detektor ruchu

Kąt widzenia: min. 100°;

Odległość detekcji: min. 10 m; Możliwość podłączenia za pomocą kabla RJ-11 do jednostki sterującej. Określenie rodzaju czujnika i połączenie musi następować automatycznie.

#### Tablica elektryczna TI

Dla potrzeb zasilania szaf serwerowych oraz urządzeń instalacji klimatyzacji serwerowni, Wykonawca rozbuduje tablicę elektryczną TI, która zainstalowana zostanie w pomieszczeniu serwerowni.

W tablicy elektrycznej TI zamontować dostarczane aparaty elektryczne:

* wyłącznik główny tablicy TI,
* lampki sygnalizujące obecność napięcia zasilającego w tablicy elektrycznej,
* ograniczniki przepięć, chroniące instalację elektryczną obiektu przed skutkami czynności łączeniowych oraz wyładowaniami atmosferycznymi,
* wyłączniki różnicowoprądowe, stanowiące dodatkową ochronę przed porażeniem prądem elektrycznym,
* wyłączniki nadprądowe zabezpieczające obwody elektryczne przed prądami przetężeniowymi,
* aparaty łączeniowe (przełączniki) oraz inne aparaty stosownie do potrzeb.

#### Instalacja zasilania szaf serwerowych

W serwerowni zainstalowana zostanie obecnie jedna szafa RACK serwerowa, wymagająca zasilania napięciem 240V, o mocy min. 4kW.

Dla potrzeb zasilania szaf serwerowych przewidziano dwa gniazda 230V/16A. Gniazda należy zainstalować wewnątrz szafy. Instalację zasilania szaf serwerowych należy wykonać za pomocą: gniazd wtyczkowych 1-fazowych 230V, 16A - podłączone przewodem YDYżo min. 3x2,5mm2.

Przewody należy prowadzić w korycie kablowym lub peszlu – zgodnie z obowiązującymi przepisami prawa w tym zakresie. Wszystkie montowane gniazda wtyczkowe powinny być przystosowane do podłączenia przewodu ochronnego PE. Kolorystykę oraz producenta gniazd należy ustalić z Zamawiającym przed montażem osprzętu.

#### Ochrona dodatkowa od porażeń prądem elektrycznym

Ochrona przed dotykiem bezpośrednim realizowana jest poprzez izolowanie części czynnych – izolacja przewodów oraz obudowy aparatów i urządzeń elektrycznych. Uzupełnieniem tej ochrony jest zastosowanie wyłączników różnicowoprądowych o prądzie różnicowym 30mA. Ochrona przed dotykiem pośrednim zrealizowana jest poprzez samoczynne wyłączenie zasilania w układzie TN-S oraz połączenia wyrównawcze. Do szyny PE należy przyłączyć wszystkie metalowe elementy instalacji wodno-kanalizacyjnej i wentylacyjnej (klimatyzacji), metalowe rury instalacji elektrycznej oraz wszelkie metalowe elementy konstrukcyjne. Połączenia wyrównawcze wykonać przewodem min. LgYżo 8 mm2.

#### Ochrona przeciwpożarowa

W tworzonym pomieszczeniu serwerowni należy zainstalować system gaszenia pożarów gazem obojętnym FE-36. Przewody i kable elektryczne wraz z zamocowaniem zastosowane w systemie zasilania i sterowania urządzeniami pożarowymi powinny zapewniać ciągłość dostawy energii elektrycznej lub przekazu sygnału przez czas wymagany do uruchomienia i działania urządzenia.

Wymagane do zainstalowania elementy systemu:

a) zbiorniki ze środkiem gaśniczym o poj. Min. 7,5l (typu CA 6F),

b) uchwyty do mocowania zbiorników,

c) łączniki butlowe z manometrem,

d) zawory elektromagnetyczne,

e) krańcowe wyłączniki ciśnieniowe (presostaty),

f) dysze dozujące,

g) rurki miedziane,

h) układ sterowania SUG z centralą automatycznego gaszenia,

i) czujka optyczna z gniazdem,

j) okablowanie.

Zbiorniki służyć mają do magazynowania środka gaśniczego FE-36 pod ciśnieniem 1,5 MPa. Zbiorniki zamocowane muszą być za pomocą wieszaków. W zbiorniki wkręcone głowice zaworowe wyposażone w manometr, krańcowe wyłączniki ciśnieniowe oraz zawory elektromagnetyczne.

Zawory elektromagnetyczne należy połączyć z dyszami dozującymi rurkami miedzianymi o długości dostosowanej do potrzeb instalacji, o średnicy 13/15 mm. Wylot dysz dozujących ustawiony musi być pod takim kątem, aby zapewnić równomierne wypełnienie środkiem gaśniczym całej przestrzeni chronionego pomieszczenia oraz tak, aby zapewnić najkrótszy czas penetracji znajdujących się w pomieszczeniu urządzeń.

Zainstalowany system musi być przystosowany do pracy w pomieszczeniach serwerowni (zamkniętych) w zakresie temperatur min.: 0-50°C i wilgotności względnej do 95%.

Zbiorniki muszą być zainstalowane w miejscu nie narażonym na uszkodzenia mechaniczne oraz bezpośrednie działanie źródeł ciepła.

Wymaga się aby system posiadał centralę monitorującą automatycznie uruchamiającą proces gaszenia – musi jednak istnieć możliwość ręcznego uruchomienia procesu gaszenia. Centrala musi być wyposażona we własne źródło zasilania awaryjnego (np. akumulator). Centrala powinna powiadamiać odpowiednie służby o wystąpieniu pożaru. W serwerowni należy zainstalować minimum dwie czujki dymu. Przed drzwiami serwerowni należy umieścić sygnalizator powiadamiający min. o trwającym procesie gaszenia (informujący o zakazie wejścia do serwerowni).

|  |  |
| --- | --- |
| Czas opróżnienia zbiorników  | < 10 s |
| Czas utrzymania stężenia gaśniczego  | 10 min. |
| Stosowany środek gaśniczy  | FE-36 |
| Napięcie zasilania centrali (z sieci)  | 230 V; 50 Hz |
| Napięcie zasilania centrali (z akumulatorów)  | 2x12 V; 7 Ah |
| Stopień ochrony obudowy centrali  | IP 30 |
| Zakres temperatur pracy  | 0 ÷ 50 °C |
| Pojemność zbiorników CA 6F  | Min. 7,5 dm3  |
| Ciśnienie robocze gazu (w zbiornikach)  | 1,5 MPa +/- 10% |

W celu odprowadzenia gazów należy wykonać w pomieszczeniu instalację wentylacji mechanicznej.

#### Ochrona przepięciowa

W celu zabezpieczenia instalacji elektrycznej od skutków przepięć powstałych na skutek:

* wyładowań atmosferycznych,
* czynności łączeniowych w energetyce,

należy zainstalować ochronę przepięciową klasy D w tablicy elektrycznej TI. Połączenia wykonać przewodem miedzianym o przekroju min. 16 mm2. Ochronniki przepięć należy zamontować na typowej szynie szerokości 35 mm.

#### Instalacja zasilania klimatyzatorów

Dla potrzeb wentylacji serwerowni, zainstalowane zostaną dwie jednostki zewnętrzne oraz dwie jednostki wewnętrzne. Jednostki zewnętrzne zasilane będą kablem min. YKYżo 3x2,5mm2 z tablicy TI, natomiast jednostki wewnętrzne zasilane są z jednostek zewnętrznych kablem YKYżo 4x1,5mm2 (Wykonawca dostosuje przewody do wymogów producenta w przypadku innego schematu podłączenia zaoferowanych urządzeń). Łączny pobór prądu przez zestaw jednostki zewnętrznej/wewnętrznej powinien wynosić maksymalnie 4kW [8kW dla zestawu redundantnych klimatyzatorów]. Kable zasilające prowadzić w na zewnątrz w rurze ochronnej. Obudowy klimatyzatorów oraz wszystkie elementy instalacji klimatyzacji (np. kanały wentylacyjne) należy objąć instalacją połączeń wyrównawczych. Jednostki zewnętrzne należy zamontować na dachu budynku.

# Etap III – Wdrożenie oprogramowania

|  |
| --- |
| WYMAGANIA OGÓLNE |
| System posiada graficzny interfejs użytkownika. Zapewniona jest praca w środowisku graficznym na wszystkich stanowiskach użytkowników. |
| System komunikuje się z użytkownikiem w języku polskim. |
| Aby ułatwić pracę personelowi medycznemu pochodzącemu spoza Polski, istnieje możliwość uruchomienia systemu w przynajmniej dwóch innych językach poza polskim (np. angielskim i rosyjskim). |
| Dostępność polskich znaków diakrytycznych wymagana jest w każdym miejscu i dla każdej funkcji w systemie - dotyczy także wyszukiwania, sortowania (według kolejności liter w polskim alfabecie), drukowania i wyświetlania na ekranie. |
| Do wybranych przycisków widocznych w oknie programu przypisane są skróty klawiszowe. Skróty są stosowane konsekwentnie w całym systemie.  |
| Opcja podglądu wydruku jest dostępna dla wszystkich drukowalnych dokumentów. |
| Minimum w zakresie funkcjonalnym zleceń i dokumentacji medycznej istnieje możliwość automatycznego wydruku bezpośrednio na drukarkę sieciową zarejestrowaną w systemie, bez konieczności podglądu wydruku. |
| System musi umożliwiać każdemu użytkownikowi zdefiniowanie domyślnie drukarki, na której będzie pracował. Domyślna drukarka będzie podpowiadała się przy każdym wydruku z systemu. |
| W modułach dostępnych poprzez przeglądarkę internetową, system wykorzystuje centralny mechanizm zarządzania wydrukami. Definiowanie i konfiguracja drukarek odbywa się z jednego miejsca w systemie bez konieczności instalacji sterowników drukarek na stacjach użytkowników, aby zapewnić łatwe zarządzanie jednolitą listą dostępnych drukarek i możliwość drukowania dla bezdyskowych stacji graficznych, tabletów oraz pozostałych stacji roboczych. Drukarki lokalne (skonfigurowane na stacji roboczej) są widoczne w aplikacji tak samo jak drukarki skonfigurowane w centralnym mechanizmie zarządzania wydrukami. |
| Co najmniej w zakresie modułów służących obsłudze: pacjenta (obsługa oddziału, izby przyjęć, rejestracja w poradni, gabinet lekarski); gospodarki lekami (obsługa apteki, apteczek oddziałowych, zlecania leków); bloku operacyjnego; rehabilitacji; bloku porodowego; dializ; pracowni diagnostycznej; zarządzania zakładem radiologii; administracji systemem (konfiguracja i zarządzenie słownikami, usługami, formularzami, opcjami systemu, dokumentacją formularzową) - system działa w oparciu o przeglądarkę internetową (minimum Mozilla Firefox) będącą klientem końcowym aplikacji w architekturze trójwarstwowej, z identyczną funkcjonalnością na systemach Windows, Linux, MacOS. |
| System nie może wymagać korzystania ze specjalnych programów klienckich technologii typu Citrix, VNC lub wirtualizacji desktop w celu realizacji wymagań funkcjonalnych interfejsu użytkownika dostępnego przez przeglądarkę internetową. |
| System nie wymaga instalowania w przeglądarce internetowej żadnych dodatkowych pluginów (np. Java, Flash, ShockWave). |
| Z wyjątkiem funkcjonalności obsługi kart kryptograficznych, system nie wymaga instalowania w przeglądarce internetowej żadnych rozszerzeń (AddOns). |
| System może korzystać z oprogramowania Java Runtime Environment zainstalowanego na stacji roboczej. Dopuszczalne jest korzystanie wyłącznie z wersji wspieranej przez producenta. |
| System musi umożliwiać pracę na stacjach roboczych wykorzystujących różne systemy operacyjne, w tym przynajmniej: MS Windows, LINUX, MacOS. |
| Komunikacja pomiędzy klientem końcowym aplikacji a serwerem aplikacji odbywa się poprzez szyfrowane połączenie. |
| Co najmniej w zakresie obsługi pracowni diagnostyki obrazowej, oddziału, izby przyjęć i gabinetu lekarskiego system musi umożliwiać użytkownikowi wybór spośród minimum trzech stylów aplikacji (tzw. "kompozycji"). Style aplikacji powinny odróżniać się przynajmniej kolorystyką (np. ciemne tło i jasna czcionka dla użytkowników pracujących w zaciemnionym pomieszczeniu) lub rozdzielczością (optymalizacja aplikacji dla niskiej rozdzielczości stacji roboczej).  |
| W trosce o bezpieczeństwo gromadzonych danych, system działa w oparciu o komercyjny motor bazy danych. |
| Niezależność systemu od motoru bazy danych - obsługa minimum dwóch komercyjnych, relacyjnych motorów baz danych głównych dostawców na rynku (Oracle, Microsoft, Sybase, IBM). |
| System musi umożliwiać uruchamianie tego samego lub innego modułu w ramach jednej sesji dowolną ilość razy, np. w trybie pilnym pozwalając na szybkie wykonanie dodatkowych czynności bez przerywania obecnie wykonywanej pracy i bez konieczności ponownego logowania się. |
| System musi umożliwiać administratorom (użytkownikom ze specjalnymi uprawnieniami) zalogowanie się do systemu z uprawnieniami innego użytkownika, w celu weryfikacji uprawnień lub weryfikacji zgłaszanych problemów. System loguje tego typu sytuacje prezentując jaki użytkownik, kiedy zalogował się z wykorzystaniem uprawnień innego użytkownika. |
| Co najmniej w modułach związanych z obsługą pacjenta w ambulatorium i szpitalu (gabinet lekarski, oddział, izba przyjęć) - system posiada funkcję prezentującą zalogowanemu użytkownikowi włączone i wyłączone funkcje i opcje systemowe. Dzięki temu administrator systemu może zweryfikować np. jakie uprawnienia należy dodać lub odebrać użytkownikowi lub jakie opcje konfiguracyjne powinny zostać włączone lub wyłączone. |
| System musi umożliwiać uwierzytelnianie użytkowników za pomocą struktury kont LDAP. |
| System musi umożliwiać zarządzanie konfiguracją uwierzytelnienia użytkowników za pomocą kont LDAP:- wyłączenie wybranych użytkowników z uwierzytelniania za pomocą konta LDAP - wskazani użytkownicy uwierzytelniani będą za pomocą konta w systemie (nie LDAP),- wskazanie nazwy atrybutu (z obiektu użytkownika LDAP) przechowującego login użytkownika,- wskazanie identyfikatora obiektu w drzewie LDAP, który przechowuje konta użytkowników systemu,- wskazanie identyfikatora obiektu użytkownika w drzewie LDAP, który posiada uprawnienia do odczytu listy użytkowników,- przechowywanie hasła użytkownika z serwera LDAP, który posiada uprawnienia do odczytu listy użytkowników,- wskazanie nazwy atrybutu z obiektu użytkownika LDAP przechowującego imię użytkownika,- wskazanie nazwy atrybutu z obiektu użytkownika LDAP przechowującego nazwisko użytkownika,- wskazanie czy mechanizm autentykacji powinien używać szyfrowanego (TLS) połączenia z serwerem LDAP,- wskazanie odnośnika (adresu URL), na który ma zostać przekierowana osoba chcąca zmienić hasło w LDAP,- wskazanie identyfikatora grupy w drzewie LDAP, do którego należą konta użytkowników systemu. |
| System używa mechanizmu podwójnej weryfikacji uprawnień użytkownika - zarówno po stronie części klienckiej jak i serwerowej. |
| Wszystkie wywołania usług systemu (uruchomione przez użytkowników i/lub systemy zewnętrzne) są logowane. Log wywołań usług zawiera: moment uruchomienia usługi; czas trwania obsługi żądania; nazwę użytkownika lub systemu zewnętrznego, który uruchomił usługę; IP komputera, z którego przyszło żądanie; nazwę usługi. |
| Wszystkie akcje biznesowe użytkowników są logowane. Log akcji zawiera co najmniej: nazwę biznesową akcji (np. przyjęcie na oddział, edycja danych pacjenta, itp.); moment wywołania akcji; czas trwania akcji; nazwę użytkownika lub systemu, który uruchomił akcję; identyfikator rekordu, na którym wykonywana była akcja (w szczególności: identyfikator pacjenta, wizyty, hospitalizacji, pobytu). |
| System udostępnia raport umożliwiający przeglądanie akcji użytkowników. |
| System posiada historię zmian danych osobowych i medycznych pacjentów z uwzględnieniem treści danych, które zostały zmienione, kiedy i przez kogo. |
| Wyszukiwanie historii choroby (według danych personalnych pacjenta, kodu kreskowego, nr Księgi Głównej, okresów pobytu). |
| Automatyczne przygotowanie przez System listy zamówionych dokumentacji do archiwum papierowego na podstawie zarezerwowanej wizyty/pobytu do archiwum papierowego przez lekarza. |
| Ewidencja przyjęcia dokumentacji do archiwum: - data przyjęcia, - pracownik szpitala, który oddał historię choroby,  - pracownik archiwum, który ją przyjął. |
| Ewidencja wydania z archiwum dokumentacji:- data wydania,- dane osoby(lekarz, pacjent, osoba upoważniona) instytucji, której wydano historię,- pracownik archiwum, który ją wydał,- postać dokumentu (kopia, oryginał),- przewidywana data zwrotu,- osoba odbierająca,- cel zamówienia (bieżące, do celów naukowy),- uwagi. |
| Możliwość wydawania dokumentacji: - Wydawanie z zamówienia,- Wydawanie bez wcześniejszego zamówienia. |
| Możliwość zamawiania dokumentacji:- wprowadzanie zamówień dokumentacji przez lekarzy i przez pracowników archiwum. Możliwość umieszczania wielu pozycji na jednym zamówieniu,- modyfikowanie danych wcześniej wprowadzonego zamówienia,- dane zamówienia: lista wybranych dokumentacji, podmiot zamawiający (lekarz, pacjent, osoba upoważniona, instytucja), postać dokumentu (kopia, oryginał), data zamówienia, przewidywana data zwrotu, cel zamówienia (bieżące, do celów naukowy), priorytet (pilny , rutynowy), uwagi. |
| Wyszukanie wszystkich dokumentacji danego pacjenta. |
| Zestaw raportów umożliwiający minimum poniższe zestawienia:  - ewidencja historii statusu dokumentacji, - ewidencja wydanych dokumentacji, - przekroczony termin zwrotu. |
| System musi umożliwiać odnotowanie informacji o kasacji dokumentów z wydrukowaniem protokołu kasacji. |
| System musi umożliwiać nałożenie limitów wypożyczeni dokumentacji w zależności od tego, czy jest ona wypożyczana do celów bieżących, naukowych. |
| Dodawanie różnego rodzaju dokumentacji medycznych:- Dokumentacja szpitalna (historia choroby) Dane dokumentacji: numer dokumentacji (nr księgi głównej); numer teczki, w której znajduje się dokumentacja; okres z którego pochodzi dokumentacja (data przyjęcia i wypisu ze szpitala); Pacjent, którego dotyczy dokumentacja; Dane dokumentacji, które dotyczą wszystkich rodzajów dokumentacji: stan dokumentacji (wybrakowana, zagubiona); osoba dostarczająca dokumentację; osoba przyjmująca dokumentację (pracownik archiwum); data przyjęcia, uwagi; - Dokumentacja szpitalna – historyczna (dokumentacja sprzed wdrożenia systemu) Dane takie jak: numer dokumentacji, pacjent, miejsce pobytu, data przyjęcia i wypisu wprowadzane są ręcznie w odróżnieniu od poprzedniego rodzaju dokumentacji, gdzie dane te są pobierane automatycznie po wybraniu księgi głównej.- Dokumentacja szpitalna – oddziałowa (gdy oddziały prowadzą oddzielną dokumentację) Pozwala na dodawanie dokumentacji dla pojedynczych pobytów na oddziałach. Można wskazać dowolny pobyt/pobyty spośród wszystkich pobytów hospitalizacji i dodać dla niego/nich dokumentację. Dane dokumentacji: numer dokumentacji (kolejny numer w danym roku, nadawany przez system w momencie dodawania dok. do archiwum); okres, z którego pochodzi dokumentacja (data przyjęcia i wypisu z oddziału)- Księga przyjęć i odmów z Izby przyjęć Dane dokumentacji: specjalizacja, okres z którego pochodzi dokumentacja, numer dokumentacji (kolejny numer w danym roku dla określonej specjalizacji).- Teczka Kart informacyjnych z izby przyjęć Dane dokumentacji: takie same jak dla dokumentacji typu: 'Księga przyjęć i odmów'.- Książka raportów pielęgniarskich Dane dokumentacji: jednostka organizacyjna (oddział), okres z którego pochodzi dokumentacja, numer dokumentacji (kolejny numer w danym roku dla określonego oddziału).- Książka raportów lekarskich Dane dokumentacji: takie same jak dla dokumentacji typu: 'Książka raportów lekarskich'. |

**EDM – Elektroniczna Dokumentacja Medyczna**

|  |
| --- |
| WYMAGANIA OGÓLNE |
| Moduł tworzy dokumentację elektroniczną w oparciu o elektroniczny rekord pacjenta prowadzony w systemie HIS oraz archiwum badań obrazowych PACS |
| Moduły przechowujące elektroniczną dokumentację medyczną działają w oparciu o ten sam motor bazy danych |
| Interfejs użytkownika systemu jest zrealizowany jako aplikacja WWW |
| Wytworzona dokumentacja elektroniczna w każdym momencie jest zgodna z obowiązującym stanem prawnym; w szczególności na dzień prowadzenia postępowania przetargowego spełnia wszystkie wymagania Rozdziału 8 Rozporządzenia Ministra Zdrowia z dn. 21 grudnia 2010 r. w sprawie rodzajów i zakresu dokumentacji medycznej oraz sposobu jej przetwarzania |
| Wykonawca przygotuje dla Zamawiającego plany, o których mowa w §86 pkt. 2 ust. 5 Rozporządzenia Ministra Zdrowia z dn. 21 grudnia 2010 r. w sprawie rodzajów i zakresu dokumentacji medycznej oraz sposobu jej przetwarzania |
| System musi umożliwiać prowadzenie dokumentacji elektronicznej i zapewnia: |
| 1) zabezpieczenie dokumentacji przed uszkodzeniem lub utratą; |
| 2) zachowanie integralności i wiarygodności dokumentacji; |
| 3) stały dostęp do dokumentacji dla osób uprawnionych oraz zabezpieczenie przed dostępem osób nieuprawnionych; |
| 4) identyfikację osoby udzielającej świadczeń zdrowotnych i rejestrowanych przez nią zmian, w szczególności dla odpowiednich rodzajów dokumentacji przyporządkowanie cech informacyjnych; |
| 5) udostępnienie, w tym przez eksport w postaci elektronicznej dokumentacji albo części dokumentacji będącej formą dokumentacji określonej w rozporządzeniu, w formacie XML i PDF; |
| 6) eksport całości danych w formacie XML, w sposób zapewniający możliwość odtworzenia tej dokumentacji w innym systemie teleinformatycznym; |
| 7) wydrukowanie dokumentacji w formach określonych w rozporządzeniu |
| System dla dokumentacji prowadzonej w formie elektronicznej: |
| 1) zapewnia jej dostępność wyłącznie dla osób uprawnionych; |
| 2) chroni przed przypadkowym lub nieuprawnionym zniszczeniem; |
| 3) stosuje metody i środki ochrony dokumentacji, których skuteczność w czasie ich zastosowania jest powszechnie uznawana |
| Dokumentację stanowi: |
| 1) dokumentacja indywidualna — odnosząca się do poszczególnych pacjentów korzystających ze świadczeń zdrowotnych; |
| 2) dokumentacja zbiorcza — odnosząca się do ogółu pacjentów lub określonych grup pacjentów korzystających ze świadczeń zdrowotnych |
| Dokumentacja indywidualna obejmuje: |
| 1) dokumentację indywidualną wewnętrzną — przeznaczoną na potrzeby Zamawiającego; |
| 2) dokumentację indywidualną zewnętrzną — przeznaczoną na potrzeby pacjenta korzystającego ze świadczeń zdrowotnych udzielanych przez Zamawiającego |
| Dokumentację indywidualną wewnętrzną stanowią w szczególności: |
| 1) historia zdrowia i choroby; |
| 2) historia choroby; |
| 3) karta indywidualnej opieki pielęgniarskiej |
| Dokumentację indywidualną zewnętrzną stanowią w szczególności: |
| 1) skierowanie do szpitala lub innego podmiotu udzielającego świadczeń zdrowotnych; |
| 2) skierowanie na badanie diagnostyczne lub konsultację; |
| 3) zaświadczenie, orzeczenie, opinia lekarska; |
| 4) karta informacyjna z leczenia szpitalnego |
| W dokumentacji indywidualnej wewnętrznej system musi umożliwiać dokonania wpisu o wydaniu dokumentacji indywidualnej zewnętrznej lub załączenia jej kopii |
| System musi umożliwiać dokonanie wpisu w dokumentacji niezwłocznie po udzieleniu świadczenia zdrowotnego, w sposób czytelny i w porządku chronologicznym |
| Każdy wpis w dokumentacji system opatruje oznaczeniem osoby dokonującej wpisu. System opatruje dokumentację oznaczeniem osoby udzielającej świadczeń zdrowotnych. Minimalny zakres danych dla tych oznaczeń zawiera: |
| a) nazwisko i imię, |
| b) tytuł zawodowy, |
| c) uzyskane specjalizacje, |
| d) numer prawa wykonywania zawodu — w przypadku lekarza, pielęgniarki i innych zawodów medycznych, dla których wymagane jest PWZ |
| Wpis dokonany w dokumentacji nie może być z niej usunięty, a jeżeli został dokonany błędnie, system musi umożliwiać tworzenie historii zmian i naniesienie adnotacji o przyczynie błędu oraz daty i oznaczenie osoby dokonującej adnotacji |
| W przypadku sporządzania wydruku z dokumentacji prowadzonej w postaci elektronicznej, strony wydruku są numerowane |
| W przypadku sporządzania wydruku z dokumentacji indywidualnej prowadzonej w postaci elektronicznej, każda strona wydruku oznaczona jest co najmniej imieniem i nazwiskiem pacjenta |
| Jeżeli nie jest możliwe ustalenie tożsamości pacjenta, w dokumentacji istnieje możliwość oznaczenia „NN”, z podaniem przyczyny i okoliczności uniemożliwiających ustalenie tożsamości |
| Do dokumentacji indywidualnej wewnętrznej możliwe jest włączenie kopii przedstawionej przez pacjenta dokumentacji lub wprowadzenia adnotacji zawartych w niej informacji istotnych dla procesu diagnostycznego, leczniczego lub pielęgnacyjnego |
| Dokument włączony w systemie do dokumentacji indywidualnej wewnętrznej nie może być z niej usunięty |
| Nazwa i numer statystyczny rozpoznania choroby, problemu zdrowotnego lub urazu są wpisywane w dokumentacji według Międzynarodowej Statystycznej Klasyfikacji Chorób i Problemów Zdrowotnych Rewizja Dziesiąta |
| System musi umożliwiać prowadzenie dokumentacji indywidualnej wewnętrznej i zamieszczania w niej lub dołączania do niej: |
| 1) cyfrowo odwzorowane oświadczenie pacjenta o upoważnieniu osoby bliskiej do uzyskiwania informacji o jego stanie zdrowia i udzielonych świadczeniach zdrowotnych, ze wskazaniem imienia i nazwiska osoby upoważnionej oraz danych umożliwiających kontakt z tą osobą, albo oświadczenie o braku takiego upoważnienia |
| 2) cyfrowo odwzorowane oświadczenie pacjenta o upoważnieniu osoby bliskiej do uzyskiwania dokumentacji, ze wskazaniem imienia i nazwiska osoby upoważnionej, albo oświadczenie o braku takiego upoważnienia; |
| 3) cyfrowo odwzorowane oświadczenie pacjenta o wyrażeniu zgody albo zezwolenie sądu opiekuńczego na przeprowadzenie badania lub udzielenie innego świadczenia zdrowotnego, na zasadach określonych w rozdziale 5 ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta |
| System osobie kierującej na badanie lub konsultację musi umożliwiać zarejestrowanie na potrzeby przekazania podmiotowi, do którego kieruje pacjenta, wraz ze skierowaniem, informacji z dokumentacji indywidualnej wewnętrznej pacjenta niezbędnych do przeprowadzenia tego badania lub konsultacji |
| System musi umożliwiać przeprowadzającemu badanie lub konsultację zarejestrowanie na potrzeby przekazania podmiotowi, który wystawił skierowanie, wyników tych badań lub konsultacji |
| System musi umożliwiać Zamawiającemu rejestrowanie, prowadzenie danych w postaci elektronicznej niezbędnych, aby sporządzić w szczególności: |
| 1) dokumentację indywidualną wewnętrzną w formie historii choroby; |
| 2) dokumentację zbiorczą wewnętrzną w formie: |
| a) księgi głównej przyjęć i wypisów, |
| b) księgi odmów przyjęć i porad ambulatoryjnych udzielanych w izbie przyjęć, |
| c) listy oczekujących na udzielenie świadczenia zdrowotnego, |
| d) księgi chorych oddziału, |
| e) księgi raportów lekarskich, |
| f) księgi raportów pielęgniarskich, |
| g) księgi zabiegów, |
| h) księgi bloku operacyjnego albo sali operacyjnej, |
| i) księgi pracowni diagnostycznej; |
| 3) dokumentację indywidualną zewnętrzną w formie karty informacyjnej z leczenia szpitalnego, skierowania lub zlecenia na świadczenia zdrowotne realizowane poza jednostkami Zamawiającego oraz z dokumentacji dla celów określonych w odrębnych przepisach; |
| 4) dokumentację zbiorczą zewnętrzną składającą się z dokumentacji prowadzonej dla celów określonych w odrębnych przepisach |
| System rejestr danych Historii choroby zakłada niezwłocznie po przyjęciu pacjenta do szpitala |
| System wyświetla całą dokumentację medyczną pacjenta w sposób ustrukturyzowany, a prezentacja struktury odpowiada obowiązującym przepisom |
| System musi umożliwiać przeglądanie zawartości dokumentacji medycznej przez uprawnionych użytkowników |
| Dostęp do dokumentów bezpośrednio ze skojarzonych z elektroniczną dokumentacją ekranów systemu medycznego mających taką możliwość |
| System przechowuje informacje w sposób dający możliwość udostępnienia, w tym przez eksport w postaci elektronicznej dokumentacji albo części dokumentacji będącej formą dokumentacji określonej w rozporządzeniu MINISTRA ZDROWIA z dnia 21 grudnia 2010 r. w sprawie rodzajów i zakresu dokumentacji medycznej oraz sposobu jej przetwarzania, w formacie XML i PDF |
| W przypadku, gdy do dokumentacji prowadzonej w postaci elektronicznej ma być dołączona dokumentacja utworzona w innej postaci, w tym zdjęcia radiologiczne lub dokumentacja utworzona w postaci papierowej, system daje możliwość korzystania z funkcji zintegrowanego modułu archiwum cyfrowej dokumentacji oraz zintegrowanego modułu archiwum PACS i przechowywania w systemie informatycznym wszystkich dokumentów w sposób zapewniający czytelność, dostęp i spójność dokumentacji medycznej |
| System musi umożliwiać w przypadku wykonania odwzorowania cyfrowego dokumentacji wydawanie na życzenie pacjenta albo zniszczenie w sposób uniemożliwiający identyfikację pacjenta, a w przypadku oświadczeń pacjentów odnotowanie zarchiwizowania dokumentu w archiwum medycznym po wykonaniu cyfrowego odwzorowania i załączeniu go do archiwum elektronicznej dokumentacji medycznej |
| W przypadku, gdy istnieje potrzeba udostępniania w postaci papierowych wydruków dokumentacji prowadzonej w postaci elektronicznej, osoba upoważniona przez Zamawiającego musi mieć możliwość potwierdzenia ich zgodności z dokumentacją w postaci elektronicznej i opatrzenia swoim oznaczeniem |
| Dokumentacja wydrukowana z systemu musi umożliwiać identyfikację osoby udzielającej świadczeń zdrowotnych |
| W przypadku przeniesienia dokumentacji z innego systemu teleinformatycznego, do przeniesionej dokumentacji system przyporządkowuje datę przeniesienia oraz informację, z jakiego systemu została przeniesiona |
| System uprawnień pozwalający na precyzyjne definiowanie obszarów dostępnych dla danego użytkownika pełniącego określoną rolę. |
| Możliwość zarządzania uprawnieniami dostępu do określonych operacji w repozytorium. Przykłady uprawnień systemowych: uruchomienie systemu, zarządzanie uprawnieniami użytkowników, zarządzanie parametrami konfiguracyjnymi, zarządzanie typami dokumentów. |
| Możliwość zarządzania uprawnieniami do wykonywania operacji na poszczególnych typach dokumentów w ramach całej placówki lub poszczególnych jednostek organizacyjnych. Przykłady uprawnień do dokumentów: dodawanie dokumentów do repozytorium, odczyt dokumentu, podpisywanie dokumentu, znakowanie czasem dokumentu, import i eksport dokumentu, anulowanie dokumentu, wydruk dokumentu itd. |
| Możliwość definiowania nowych typów dokumentów obsługiwanych przez repozytorium dokumentów elektronicznych. |
| Zakłada się także możliwość indeksowania dokumentów, których elektroniczna postać nie jest przechowywana w Oprogramowaniu - np. indeksowanie dokumentów papierowych, obrazów radiologicznych przechowywanych w PACS. |
| PRZEGLĄDANIE ORAZ DOSTĘP DO DOKUMENTACJI MEDYCZNEJ |
| Dostęp do wybranych dokumentów bezpośrednio ze skojarzonych z dokumentami ekranów systemu medycznego |
| Przeglądanie zawartości dokumentów możliwych do wydrukowania wyłącznie w postaci plików PDF niedających możliwości nanoszenia przez użytkownika zmian bez wprowadzenia ich w systemie |
| Możliwość przeglądania zawartości archiwum dla uprawnionych użytkowników |
| Możliwość przeszukiwania zawartości archiwum według zdefiniowanych kryteriów |
| Dostęp do archiwum z poziomu systemu medycznego (minimum Oddział, Izba przyjęć, Poradnia, Gabinet) bez konieczności zmiany modułu i ponownego logowania się do systemu |
| Dostęp do zawartości archiwum z poziomu danych pobytu pacjenta |
| Możliwość wyszukiwania dokumentów za pomocą zaawansowanych kryteriów oraz meta danych. |
| System musi umożliwić udostępnianie dokumentacji: |
| - w celu realizacji procesów diagnostyczno-terapeutycznych w Zamawiającego |
| - pacjentom i ich opiekunom |
| - podmiotom upoważnionym (np. Prokurator) |
| CYFROWE REPOZYTORIUM DOKUMENTÓW MEDYCZNYCH |
| Wpisy w danych dokumentacji medycznej oznaczone są czasem wprowadzenia oraz opatrzone oznaczeniem osoby dokonującej wpisu lub zmian |
| System otwarty jest na możliwość opatrywania określonych wpisów podpisem elektronicznym oraz oznaczania czasem |
| System zapewnia automatyczne kopie bezpieczeństwa zawartości archiwum elektronicznego dokumentacji medycznej |
| Możliwość automatycznego zarchiwizowania dokumentacji medycznej na daną chwilę (w tym opcja automatycznego archiwizowania po elektronicznym podpisaniu) i przechowanie go w formacie PDF |
| Istnieje możliwość przygotowania eksportu całości danych dokumentacji medycznej w formacie XML, w sposób zapewniający możliwość odtworzenia tej dokumentacji w innym systemie teleinformatycznym |
| Możliwość archiwizacji dokumentacji medycznej w postaci elektronicznej. |
| Generowanie wydruków zgodnych z obowiązującymi przepisami prawa |
| Możliwość archiwizacji dokumentów złożonych, wieloczęściowych i przyrostowych tj. księgi |
| Możliwość rejestracji dokumentów elektronicznych utworzonych poza Oprogramowaniem Zamawiającego, manualna rejestracja dokumentów zewnętrznych |
| Cyfryzacja dokumentu papierowego i dołączanie go do dokumentacji elektronicznej |
| Możliwość weryfikacji podpisu |
| Możliwość weryfikacji integralności dokumentu |
| Możliwość wydruku dokumentu |
| Możliwość wersjonowania przechowywanych dokumentów z dostępem do pełnej historii poprzednich wersji. |
| Repozytorium EDM musi umożliwiać: |
| - rejestrację dokumentu |
| - pobieranie dokumentów w formacie XML |
| - pobieranie dokumentów w formacie PDF |
| - wyszukiwanie materializacji dokumentów |
| Repozytorium EDM musi współdzielić z Oprogramowaniem Zamawiającego: |
| - słownik jednostek organizacyjnych, |
| - rejestr użytkowników, |
| - rejestr pacjentów, |
| Indeksowane powinny być wszystkie wersje dokumentu |
| Możliwość indeksowania dokumentów w celu łatwego jej wyszukiwania wg zadanych kryteriów |
| Indeks dokumentacji powinien być zorientowany na informacje o dokumencie: autor, data powstania, rozmiar, typ, data powstania. |
| Cyfrowe archiwum medycznej jest modułem dostarczonym przez Wykonawcę zintegrowanym z modułem elektronicznej dokumentacji medycznej |
| Możliwość przechowywania dokumentów elektronicznych w dowolnym formacie, w tym PDF |
| Możliwość przechowywania dokumentów podpisanych lub niepodpisanych podpisem elektronicznym |
| Możliwość porządkowania dokumentacji w folderach w kontekście rekordu medycznego pacjenta |
| System zapewnia automatyczne kopie bezpieczeństwa zawartości archiwum dokumentów |
| System zapewnia oznaczenie czasu i jednoznaczne przypisanie osoby dodającej dokument cyfrowy |
| System zapewnia automatyczne kopie bezpieczeństwa zawartości archiwum dokumentów |
| Przechowywanie w systemie informatycznym wszystkich dokumentów w sposób zapewniający czytelność, dostęp i spójność z dokumentacją prowadzaną w module elektronicznej dokumentacji medycznej |
| CYFROWY PODPIS DOKUMENTÓW MEDYCZNYCH |
| Możliwość złożenia podpisu elektronicznego na dokumencie oraz na zbiorze dokumentów w formacie PDF |
| Możliwość złożenia podpisu elektronicznego na zbiorze dokumentów |
| AUTORYZACJA WYNIKÓW USŁUG MEDYCZNYCH |
| System HIS jest wyposażony w funkcjonalność autoryzacji wyników usług. |
| Możliwość opatrywania dokumentów podpisem elektronicznym oraz oznaczenia czasem |
| System zapewnia oznaczenie czasu i jednoznaczne przypisanie osoby dodającej dokument cyfrowy |
| Autoryzacja wyniku polega na złożeniu pod wpisanym wynikiem podpisu zgodnie z regułą autoryzacji zdefiniowaną dla danego formularza badania / usługi. |
| W przypadku, gdy zdefiniowana została reguła autoryzacji, po wpisaniu wyniku badanie otrzyma status Wynik do weryfikacji. Na ekranie wyniku występuje tabela autoryzacji reprezentująca regułę autoryzacji z listą niezbędnych podpisów / autoryzacji. |
| Reguły autoryzacji można definiować w module administracyjnym systemu HIS dla każdego z formularzy usług z osobna. |
| Istnieje możliwość wyznaczenia konkretnego użytkownika, od którego oczekiwane jest złożenie podpisu pod badaniem/usługą. |
| Po wskazaniu konkretnego użytkownika autoryzującego, wybrany użytkownik powinien pojawić się w tabeli autoryzacji badania/usługi w wierszu z wybranym typem użytkownika. |
| Możliwość zmiany osoby wyznaczonej do autoryzacji przez wyszukanie w jej miejsce innego użytkownika. |
| Jeśli jakaś osoba jest wyznaczona do złożenia podpisu, to tylko ona może go złożyć. |
| Nie można wyznaczyć jednej osoby dwa razy |
| Użytkownik, który otwiera okno wyniku badania musi należeć do typu użytkownika, który jest wyznaczony do autoryzacji, by mógł zobaczyć tabelę z listą podpisów/autoryzacji do złożenia. |
| W tabeli autoryzacji prezentują się typy podpisów użytkowników, które są wymagane bądź opcjonalne do pełnej autoryzacji, czyli takiej sytuacji, gdy złożone będą wszystkie podpisy obowiązkowe. |
| Jednoznaczne oznaczenie podpisów obowiązkowych i opcjonalnych. |
| Gdy podpis danego typu zostanie złożony, to obok nazwy typu podpisu pojawi się imię i nazwisko osoby, która ten podpis złożyła oraz data złożenia podpisu. |
| Autoryzacja zostanie zakończona pozytywnie, jeśli spełnione są następujące warunki: - Poprawny login użytkownika - Poprawne hasło użytkownika - Użytkownik należy do typu użytkownika wybranego w tabelce autoryzacji - Typ użytkownika ma uprawnienie do autoryzacji - Nie ma jeszcze złożonego podpisu tego samego użytkownika w jednym badaniu - Wybrany typ podpisu w tabeli autoryzacji nie jest jeszcze złożony |
| W przypadku, gdy przed złożeniem podpisu, użytkownik zmodyfikował jakiekolwiek dane w wyniku badania, zostanie poproszony o potwierdzenie tej decyzji, gdyż wiąże się ona z zapisem wyniku oraz cofnięciem procesu autoryzacji do początku (nadaniu badaniu statusu początkowego z reguły autoryzacji - wszystkie podpisy będzie trzeba złożyć ponownie). Następnie użytkownik będzie mógł autoryzować zmieniony wynik. |
| Każdy złożony podpis w tabelce autoryzacji jest natychmiast zapisywany. |
| System pozwalający na digitalizację dokumentów wypełnianych długopisem cyfrowym w zakresie zgód pacjenta. |
| Integracja z system szpitalnym HIS w zakresie opracowania we współpracy z zamawiającym 10 sztuk formularzy, które będą mogły być wypełniane z wykorzystaniem długopisu cyfrowego. Zakłada się że średnia wielkość formularza nie powinna przekroczyć dwóch stron w formacie A4. Wypełniony formularz będzie z wykorzystaniem USB lub innych łączy transmisyjnych przenoszony automatycznie do systemu szpitalnego importowany i mapowany na odpowiednie pola w systemie tak by zapis danych nie różnił się od formularzy wypełnianych za pomocą interfejsu systemu HIS. System będzie umożliwiał zapis formularza w formie przetwarzalnej – rozkodowanej na poszczególne pola w bazie danych jak i zapis oryginału w postaci skanu np. w formacie PDF. |
| Formularze w formacie PDF będą składowane w centralnym repozytorium EDM z możliwością wyszukiwania i przeglądania. |
| Dostęp do funkcji przeglądania będzie możliwy bezpośrednio z poziomu systemu HIS bez konieczności budowy dodatkowych interwale i integracji. |
| Długopis cyfrowy powinien umożliwiać odwzorowanie (tak jakby został zeskanowany ) formularza papierowego w wersji elektronicznej. |
| Opis wymagania Długopis cyfrowy powinien umożliwiać automatyczne powiązanie z rodzajem formularza, który został z jego pomocą wypełniony. |
| Opis wymagania Aplikacja powinna umożliwiać stworzenie formularza za pomocą wbudowanego w Aplikację edytora WYSIWYG bazującego na przeciąganiu predefiniowanych elementów. |
| Opis wymagania Aplikacja powinna umożliwiać stworzenie formularza bazując na imporcie dowolnego dokumentu w formacie PDF. |
| Opis wymagania Aplikacja powinna umożliwiać w importowanej ankiecie zaznaczenie regionów aktywnych, pól tekstowych oraz nadanie im unikalnych nazw. |
| Opis wymagania Aplikacja powinna umożliwiać wydruk formularza w ten sposób, aby każdy wydrukowany formularz był unikalny. Oznacza to, że wypełnienie papierowego formularza długopisem cyfrowym tworzy wzajemnie jednoznacznie przyporządkowaną do niego wersje elektroniczną dokumentu. |
| Opis wymagania Aplikacja powinna umożliwiać pobranie danych z długopisów cyfrowych za pomocą stacji dokującej USB bądź też komunikacji bezprzewodowej bluetooth. Dane są jednoznacznie przyporządkowywane do formularzy. |
| Opis wymagania Aplikacja powinna umożliwiać przeglądanie oraz eksport nieprzetworzonych danych z wypełnionych formularzy do formatu PDF będącego wizualizacji „skanów” wypełnionych dokumentów. |
| Opis wymagania Aplikacja powinna umożliwiać edycję przetworzonych danych zwizualizowanej na formularzu z pól tekstowych i pól numerycznych przy jednoczesnym podglądzie danych pochodzących bezpośrednio z długopisów cyfrowych. |
| Opis wymagania Aplikacja powinna umożliwiać definiowanie kluczy pozwalających na określanie poprawnych odpowiedzi oraz punktacji za poszczególne pola zaznaczone w testach. Możliwość eksportu danych przetworzonych w wyniku analizy zgodnie z podaną punktacją. |
| Opis wymagania Aplikacja powinna umożliwiać automatyczne generowanie wyników testów wypełnionych papierowo przy pomocy długopisu cyfrowego. |
| Opis wymagania Aplikacja powinna umożliwiać publikację dowolnej z ankiet stworzonej w Systemie na stronie internetowej. |
| Opis wymagania Aplikacja powinna umożliwiać wypełnianie ankiet stworzonych w Aplikacji w trybie on-line, tj. korzystając z dowolnej przeglądarki internetowej. |
| Opis wymagania Aplikacja powinna umożliwiać tworzenie kont użytkownikom w obrębie firmy oraz przydzielania im uprawnień do poszczególnych funkcjonalności lub ankiet. Uprawnienia dotyczą tworzenia nowych formularzy, wydruku formularzy, analizy formularzy, przeglądania wypełnionych formularzy, eksportu przetworzonych danych. |
| Opis wymagania Aplikacja powinna umożliwiać podgląd stanu podłączonych do komputera długopisów cyfrowych, w szczególności stanu ich naładowania. |
| Opis wymagania Aplikacja powinna umożliwiać nadawanie długopisom unikalnych nazw i przypisywania ich do użytkowników. |
| SKANOWANIE DOKUMENTÓW PAPIEROWYCH DO EDM oraz HIS |
| Możliwość zeskanowania papierowego dokumentu i automatycznego dołączenia do archiwum medycznego do rekordu pacjenta |
| bezpośrednie skanowanie dokumentów poziomu oprogramowania systemu szpitalnego klasy HIS, poprzez integrację z dowolnym skanerem pracującym pod kontrolą systemu MS Windows |
| zeskanowania papierowego dokumentu i automatycznego dołączenia do archiwum medycznego do rekordu pacjenta lub do pobytu |
| bezpośrednie wskazania pliku ze skanem dokumentu i podpięcie go do rekordu pacjenta lub pobytu |
| Dodanie komentarza do skanowanego pliku |
| Dodanie do skanowanego dokumentu dodatkowych cech (tagi) umożliwiających szybsze wyszukiwanie dokumentów |
| Możliwość wyboru typu skanowanego dokumentu |
| Możliwość wyszukiwania zeskanowanych dokumentów bezpośrednio w systemie HIS, z wykorzystanie takich kryteriów jak: nazwisko pacjenta, nazwa pobytu, typ dokumentu, data archiwizacji) |

Dodatkowe moduły/funkcje systemu niezbędne do realizacji wszystkich wymaganych funkcjonalności EDM oraz e-Usług.

|  |
| --- |
| Moduł umożliwiający wystawianie recept dla wskazanego pacjenta wybranego z bazy pacjentów systemu. |
| Moduł dostępny co najmniej z modułów obsługujących gabinet lekarski, izbę przyjęć, oddział. |
| Wydruk recepty lekarskiej jest zgodny z rozporządzeniem Ministra Zdrowia z dnia 8 marca 2012 r. w sprawie recept lekarskich (Dz. U. z 2017 r. poz. 1570) i późniejszymi zmianami w tym zakresie. |
| Moduł musi umożliwiać wyszukiwanie leków z następujących słowników: baza leków, leków recepturowych, leków preferowanych. |
| Moduł musi umożliwiać wyszukiwanie leków według nazwy handlowej lub nazwy międzynarodowej. |
| Na liście wyszukanych leków, moduł prezentuje co najmniej: nazwę handlową, nazwę międzynarodową, postać, dawkę, opakowanie. Dla leków refundowanych prezentowane są możliwe wartości odpłatności, sugerowana cena oraz wskazania do stosowania odpłatności. W przypadku leków recepturowych, moduł prezentuje co najmniej: nazwę oraz kategorię dostępności. |
| Moduł musi umożliwiać tworzenie słownika leków recepturowych i zarządzania tym słownikiem. Słownik zawiera co najmniej: nazwę leku, skład chemiczny, kategorię dostępności. |
| Moduł musi umożliwiać automatyczną aktualizację słownika leków wykorzystywanych do wypisywania recept. Dodatkowo z poziomu modułu administracyjnego istnieje możliwość wykonania importu słownika leków. |
| Moduł prezentuje użytkownikowi wystawiającemu receptę informację o wersji słownika leków oraz dacie wydanie słownika. |
| Moduł musi umożliwiać zawężenia listy wyszukanych leków - do samych leków refundowanych. |
| Moduł musi umożliwiać tworzenie podręcznego słownika leków preferowanych przez użytkownika. Dodanie nowej pozycji słownika jest możliwe z poziomu listy wyszukanych leków z bazy leków lub leków recepturowych. |
| Moduł musi umożliwiać tworzenie podręcznego słownika leków preferowanych dla jednostki organizacyjnej. Dodanie nowej pozycji do słownika jest możliwe z poziomu listy wyszukanych leków z bazy leków lub leków recepturowych. |
| Podczas dodawania leku do listy leków preferowanych, moduł musi umożliwiać konfigurację domyślnego dawkowania wskazanego leku. Dzięki temu podczas wystawiania kolejnej recepty moduł musi umożliwiać wybór leku preferowanego i ustawienie domyślnego dawkowania. |
| Podczas dodawania leku do listy leków preferowanych, moduł musi umożliwiać konfigurację domyślnego dawkowania leku dla pacjenta, któremu wystawiana jest recepta. Dzięki temu przy kolejnym wystawianiu recepty dla danego pacjenta moduł musi umożliwiać wybór leku preferowanego i ustawienie domyślnego dawkowania. |
| Moduł musi umożliwiać wybór leku oraz wskazanie liczby opakowań (także niepełnych opakowań), dawkowania, odpłatności, dodania komentarza, zastrzeżenia zamiany leku. |
| Moduł musi umożliwiać przeliczanie dobowej liczby dawek oraz liczby dni kuracji. |
| Moduł automatycznie nanosi na receptę oddział NFZ lub kod państwa w przypadku pacjentów zagranicznych, a także niezbędne dane pacjenta. W przypadkach, gdy pacjent jest nieubezpieczony, automatycznie ustawiany jest brak ubezpieczenia. |
| Moduł nanosi automatycznie na formularz i wydruk recepty dane świadczeniodawcy. Odpowiedni świadczeniodawca wybierany jest automatycznie na podstawie miejsca pobytu pacjenta (oddział/poradnia). |
| Moduł automatycznie nanosi na receptę zalogowanego lekarza, datę wystawienia oraz termin realizacji. Jeśli zalogowany użytkownik nie jest lekarzem, na receptę wstawia się lekarz prowadzący (oddział) lub lekarz z wizyty. Użytkownik może te dane zmieniać, przy czym lekarza może wybrać ze słownika lekarzy w systemie.  |
| Moduł musi umożliwiać oznaczenia pilności recepty. |
| Moduł musi umożliwiać wybór drukarki, na której nastąpi wydruk. |
| Moduł musi umożliwiać zdefiniowanie zakresu numerów recept dla lekarza poprzez import z pliku xml lub poprzez ręczne zdefiniowanie zakresu. |
| Moduł zapisuje numery recept na lekarza i świadczeniodawcę. |
| Jeśli placówka medyczna ma wiele lokalizacji i na każdą oddzielną umowę z NFZ, wskazany we wprowadzaniu zakresów recept lekarz może mieć oddzielną pulę numerów na każdą z przychodni, w których udziela świadczeń. |
| Podczas wprowadzania numerów recept moduł automatycznie weryfikuje poprawność wprowadzonego numeru recepty. |
| Moduł automatycznie rejestruje i numeruje recepty ze zdefiniowanej listy numerów recept lekarza. |
| Moduł musi umożliwiać zdefiniowanie zakresu numerów recept dla lekarza z uwzględnieniem świadczeniodawcy wybieranego ze słownika jednostek organizacyjnych szpitala w Systemie |
| Moduł automatycznie wyświetla licznik numerów recept pozostałych do wykorzystania. |
| Moduł ewidencjonuje wszystkie leki przepisywane pacjentowi. |
| W przypadku wystawiania recept dla dzieci nieposiadających numeru PESEL, na wydruku umieszczany jest PESEL opiekuna zapisany w systemie. |
| Moduł musi umożliwiać zapis recepty w celu późniejszego jej wydrukowania lub modyfikacji. |
| Moduł blokuje możliwość edycji lekarza na recepcie, gdy został wykorzystany numer recepty z puli danego lekarza. |
| Moduł musi umożliwiać usuwanie zapisanych recept. Usunięcie recepty skutkuje odzyskaniem numeru recepty i włączeniu go do puli numerów recept do wykorzystania. |
| Usunięcie recept wydrukowanych jest możliwe tylko da użytkowników z dodatkowymi uprawnieniami. |
| Moduł ostrzegający użytkownika w przypadku próby edycji wydrukowanej recepty. |
| Moduł ostrzegający przed próbą ponownego wydrukowania tej samej recepty |
| Moduł ostrzegający przed usunięciem zapisanej/wydrukowanej recepty |
| W momencie wydruku moduł automatycznie zapisujący receptę. |
| Moduł umożliwiający ewidencjonowanie leków przypisywanych pacjentowi bez recepty. |
| Moduł prezentujący zapisane recepty po ponownym uruchomieniu funkcji. |
| Moduł prezentujący zachowane recepty i listy leków bez recepty w postaci zakładek i zapisuje je na pobyt/wizytę. |
| Moduł umożliwiający wydrukowanie listy leków dla pacjenta z dawkowaniem. |
| Moduł umożliwiający kopiowanie recept i leków na podstawie historii wystawionych recept. |
| Moduł prezentujący leki, które przyjmuje pacjent. Prezentowane są one w dodatkowej zakładce z możliwością wyboru i naniesienia na receptę. |
| Moduł umożliwiający wydruk pustych recept dla pacjenta (recept, na których lekarz będzie mógł ręcznie wprowadzić same nazwy leków, odpłatność i dawkowanie).  |
| Moduł umożliwiający wydruk pustych recept bez danych pacjenta (recept, na których lekarz będzie mógł ręcznie wprowadzić dane pacjenta, nazwy leków, odpłatność i dawkowanie). |
| Moduł umożliwiający wyszukiwanie zamienników leków (zamienniki, zamienniki tańsze, zamienniki dawka, zamienniki dawka tańsze). |
| Moduł umożliwiający zdefiniowanie minimalnej ilości recept, której przekroczenie skutkowało będzie pojawianiem się komunikatu ostrzegawczego podczas wejścia przez użytkownika do modułu recept. |
| Moduł udostępniający funkcję zarządzania pulami recept. Uprawniony użytkownik musi mieć możliwość wyszukania lekarzy o dowolnej ilości pozostałych recept. Funkcjonalność prezentuje w postaci listy co najmniej następujące informacje: lekarz / pielęgniarka / położna, nazwa świadczeniodawcy, dostępna ilość recept, kategoria recept, oznaczenie czy pula recept została zablokowana, informacja czy jest to pula numerów komercyjnych, informacje czy jest to pula numerów indywidulnej praktyki lekarskiej, pierwszy numer puli recept, ostatni numer puli, data od, data do. |
| Moduł umożliwiający wgląd do listy leków podawanych pacjentowi podczas pobytu w szpitalu i zapisania ich na recepcie. |
| Moduł umożliwiający wprowadzanie i sprawdzanie interakcji pomiędzy lekami. |
| Moduł umożliwiający duplikację recepty. Użytkownik musi mieć możliwość wskazania liczby duplikowanych recept oraz ilości dni, co które powinna być możliwa ich realizacja. Moduł automatycznie musi ustawiać datę realizacji od dnia, według ustawionej ilości dni.  |
| Moduł umożliwiający wystawienie recepty na leki psychotropowe i odurzające. Moduł ogranicza ilość leków na recepcie do jednego, przelicza ilość substancji czynnej i wskazuje ją w postaci opisu słownego.  |
| Moduł umożliwiający wystawienia recept pielęgniarkom i położnym. |
| Moduł umożliwiający wystawienie recepty transgranicznej. |
| Moduł ostrzega użytkownika w przypadku braku adresu pacjenta. |
| Moduł ostrzega użytkownika w przypadku braku kodu administracyjnego w adresie pacjenta. |
| Moduł ostrzega użytkownika w przypadku braku aktualnego ubezpieczenie pacjenta. |

|  |
| --- |
| AP-KOLCE |
| Dodania kolejki oczekujących do AP-KOLCE |
| Aktualizacji kolejek oczekujących w AP-KOLCE |
| Dodania pacjenta do AP-KOLCE |
| Aktualizacji danych pacjenta w AP-KOLCE |
| Dodania pacjenta na kolejkę oczekujących w AP-KOLCE |
| Aktualizacji wpisu pacjenta na kolejkę oczekujących w AP-KOLCE. |
| Raport błędów synchronizacji danych z AP-KOLCE (raport o listach oczekujących, pacjentach oraz ich wpisach na listy, których się nie udało zsynchronizować z NFZ-ową usługą AP-KOLCE). Raport prezentuje informacje w następujących grupach:Pacjent jakiego nie udało się wysłać - Kod i opis błędu Kolejka jakiej nie udało się wysłać - Kod i opis błędu Wpis na kolejkę jakiego nie udało się wysłać - Kod i opis błędu |
| Raport błędów synchronizacji danych do AP-KOLCE. Raport prezentuje informacje w następujących grupach:grupach: Pacjent jakiego nie udało się wysłać - Kod i opis błędu Kolejka jakiej nie udało się wysłać - Kod i opis błędu Wpis na kolejkę jakiego nie udało się wysłać - Kod i opis błędu |
| System obsługuje zlecenia we współpracy z modułem zleceń i modułami specjalizowanymi – wysłanie/skierowanie pacjenta na konsultację, badanie diagnostyczne, laboratoryjne, zabieg, obsługa pacjenta konsultowanego w formie elektronicznej (sieć komputerowa) oraz tradycyjnej (wydruk zlecenia). Wszystkie funkcje opisane w module Zleceń Medycznych można uruchomić bezpośrednio z poziomu dowolnego modułu obsługi pacjenta z wyłączeniem modułów integrujących się bezpośrednio z urządzeniami medycznymi. |
| Wysłanie zlecenia wykonania elementu leczenia (badania) do jednostki realizującej (pracownia diagnostyczna). |
| Możliwość śledzenia stanu wykonania zlecenia.(czas pobrania próbki, moment rejestracji w pracowni diagnostycznej, czas autoryzacji wyniku w pracowni) |
| Możliwość umieszczenia na jednym ekranie w postaci tabeli lub wykresu (w celu porównania) wyników badań diagnostycznych z dawkami leków np.: poziom glukozy we krwi a dawki insuliny.  |
| Zwrotne otrzymanie wyniku realizacji zlecenia (wyniku badania). |
| Możliwość automatycznej aktualizacji stanów magazynowych apteczek na podstawie zewidencjonowanego podczas wykonania zlecenia zużycia zasobów. |
| Automatyczne kodowanie ICD9 na podstawie zleceń medycznych. Usługa (Badanie/operacja/konsultacja) może mieć przypisane kody ICD9 z możliwością wskazania jednego, domyślnego. Jej wykonanie w module zleceń skutkuje automatycznym zakodowaniem domyślnego kodu ICD9. Dodatkowo w chwili wprowadzania wyniku zlecenia użytkownik musi mieć możliwość zmiany ICD9, które zostało automatycznie zakodowane przez system, jeżeli do zleconej usługi jest przyporządkowane więcej niż jedno ICD9. Zmiany ICD9 w takim przypadku są spójne (nie występuje redundancja danych) niezależnie, czy zostały dokonane w module statystyka, czy w module zleceń medycznych. |
| System ostrzega, że zlecana usługa już jest zlecona w zdefiniowanym przez administratora okresie czasu, w celu wyeliminowania przypadkowego podwójnego zlecenia tego samego badania. |
| Możliwość powtarzania zleceń na podstawie już istniejących. Funkcja dostępna jest z ekranu prezentującego zlecenia i wyniki pacjenta. Użytkownik musi mieć możliwość wyboru zleceń, które chce powtórzyć. |
| Możliwość prezentacji aktualnych zleceń pacjenta w chwili zlecania (każdy użytkownik indywidualnie dla siebie może włączyć lub wyłączyć tę funkcję) |
| Możliwość autoryzowania wykonania zlecenia dla zleceń ze skonfigurowaną regułą autoryzacji, przez osoby uprawnione do autoryzacji np. ordynator oddziału. Możliwość autoryzacji pojedynczych zleceń lub grupy zleceń wybranych z listy. |
| Możliwość zleceń badań przedmiotowych niepowiązanych z pacjentem (np. badania czystościowe, wymazy z brudowników, czy też wymiana żarówki w urządzeniu).  |
| System posiada oddzielną listę roboczą do śledzenia statusu oraz wykonania zlecenia przedmiotowego. |
| Możliwość rejestrowania wartości Wagi, Wzrostu, grupy krwi pacjenta poprzez formularz. System przy zapisie formularza aktualizuje te atrybuty w rekordzie medycznym pacjenta i przy kolejnych badaniach automatycznie podpowiada ostatnio uzupełnioną wartość. |
| Możliwość konfiguracji priorytetów zlecanych badań oraz definiowania terminów, na jakie badanie z danym priorytetem może być zlecane (np. CITO na czas bieżący, rutynowy na dzień następny na godzinę 12:00). |
| Możliwość definiowania podręcznego panelu zleceń: - definiowanie panelu ogólnego, jaki i spersonalizowanego dla użytkownika lub jednostki organizacyjnej na której przebywa pacjent, - możliwość dodawania usług do panelu, - możliwość dodawania grupy usług do panelu i wprowadzenia nazwy grupy, - możliwość zlecania usług/grup usług z panelu jednym kliknięciem bez konieczności szukania w słowniku, - możliwość zlecania wszystkich pozycji z panelu jednym kliknięciem bez konieczności szukania w słowniku.- możliwość zgrupowania paneli w zakładki- możliwość zdefiniowana panelu dla wskazanych kodów diagnoz ICD-10 (panel pojawia się tylko dla pacjentów, ze wskazaną w konfiguracji diagnozą ICD-10). |
| System posiada możliwość informowania użytkownika o wynikach badań. Użytkownik zlecający badanie może wskazać, o których wynikach badań chce zostać poinformowany poprzez powiadomienie systemowe, SMS lub e-mail. Użytkownik może wskazać innych użytkowników, którzy powinni zostać poinformowani o wynikach badań.  |
| Stworzone przez użytkownika w panelu grupy usług wyszukują się również w polu wyszukiwania usług. |
| Prezentacja listy wszystkich zleconych badań |
| Moduł musi umożliwiać prowadzenie Karty TISS-28 oraz Karty TISS-28 dla dzieci. |
| Moduł automatycznie tworzy odpowiednią kartę TISS-28 lub TISS-28 dla dzieci dla każdego dnia pobytu pacjenta na oddziale. |
| Moduł automatycznie tworzy odpowiednią kartę TISS-28 biorąc pod uwagę wiek pacjenta. Dla pacjentów do 18 roku życia - kartę TISS-28 dla dzieci, dla pacjentów w wieku powyżej 18 lat kartę TISS-28. |
| Moduł musi umożliwiać uzupełnienie formularza karty TISS-28 oraz TISS-28 dla dzieci. |
| Karta TISS oraz automatycznie zakodowane świadczenia NFZ są zgodne z aktualnymi zarządzaniami Prezesa NFZ. |
| Moduł musi umożliwiać automatyczne kodowanie świadczeń NFZ na podstawie uzupełnionego formularza TISS-28 oraz TISS-28 dla dzieci. |
| W przypadku edycji lub modyfikacji uzupełnionego formularza TISS-28 i TISS-28 dla dzieci, moduł modyfikuje również zakodowane świadczenia NFZ - dodając lub usuwając świadczenia. |
| Moduł musi umożliwiać wydruk karty TISS-28 oraz karty TISS-28 dla dzieci. Wydruk jest zgodny z aktualnymi zarządzeniami Prezesa NFZ. |
| Moduł posiada ekran prezentujący wszystkie uzupełnione dla pacjenta karty TISS-28 oraz TISS-28 dla dzieci, zawierający co najmniej: liczbę porządkową; datę wykonania badania; jednostkę organizacyjną; wynik badania w postaci ilości punktów; świadczenie kontraktowe; status świadczenia NFZ. |

|  |
| --- |
| eZWOLNIENIA |
| Moduł zapewnia zgodność z interfejsem ZUS PUE, umożliwiającym wystawianie oraz korektę zwolnień lekarskich bezpośrednio z poziomu systemów dziedzinowych zewnętrznych względem ZUS dostawców oprogramowania. |
| Moduł musi umożliwiać logowanie do systemu ZUS PUE bezpośrednio z systemu medycznego. Logowanie możliwe jest poprzez podpisanie oświadczenia wygenerowanego przez ZUS lub podpisu elektronicznego. |
| Moduł zapewnia wylogowanie z systemu ZUS PUE w momencie wylogowania się z systemu medycznego. |
| Moduł musi umożliwiać wystawianie zaświadczenia lekarskiego w trybie bieżącym. Moduł musi umożliwiać posługiwanie się zarówno danymi lokalnymi jak i danymi pobieranymi z systemu ZUS PUE. |
| Moduł musi umożliwiać podpisanie dokumentu zaświadczenia lekarskiego za pomocą oświadczenia wygenerowanego przez ZUS, podpisu kwalifikowanego lub profilu zaufanego e-PUAP. |
| Moduł musi umożliwiać przekazywanie utworzonych dokumentów zaświadczeń lekarskich do systemu ZUS PUE. |
| Moduł musi umożliwiać wydruk dokumentu zaświadczenia lekarskiego zgodnie z opublikowanym przez ZUS wzorem. |
| Moduł musi umożliwiać anulowanie zaświadczenia lekarskiego, jeżeli nie zostało przekazane do ZUS. |
| Moduł musi umożliwiać przegląd dokumentów zaświadczeń lekarskich wystawionych w systemie medycznym. |
| Moduł obsługuje anulowanie dokumentu ZLA - AZLA. |
| Moduł posiada archiwum wydruków eZLA na szablonach ZUS. |
| Dane z systemu lokalnego, walidowane są przez usługi systemu ZUS, przed wysłaniem dokumentu eZLA. Zapewnienie prawidłowych danych, na przesyłanym dokumencie. |
| System medyczny jest zabezpieczony przed przekroczeniem pobrania dopuszczalnej przez system ZUS ilości identyfikatorów na potrzeby dokumentu eZLA. W przypadku rozpoczęcia pracy z modułem eZwolnienia i zakończenia bez wysyłki eZLA (wyłączenie przeglądarki), pobrane identyfikatory, pozostają na koncie lekarza. |
| Dla aplikacji testowej eZwolnienia, możliwość łączenia się ze środowiskiem testowym systemu ZUS. |
| Obsługa podpisu kwalifikowanego z karty i podpisów różnych (kilku) lekarzy z PUE ZUS. |
| Moduł musi umożliwiać wystawianie zaświadczenia lekarskiego przez asystenta medycznego. |
| Moduł musi umożliwiać integrację z systemem Banku Krwi w zakresie przekazywania zamówień na krew i materiały krwiopochodne. |
| Moduł musi umożliwiać zlecenie transfuzji krwi dla pacjenta przebywającego w szpitalu. |
| Podczas zlecania transfuzji moduł wymusza uzupełnienie wymaganego zasobu lub jego opisu. |
| Moduł musi umożliwiać oznaczenie zlecenia transfuzji jako CITO. |
| Moduł musi umożliwiać zamówienie preparatów krwi dla pacjenta. |
| Moduł musi umożliwiać użytkownikowi zamówienie preparatów krwi na podstawie zleconej transfuzji. |
| Podczas zamawiania krwi użytkownik musi mieć możliwość wskazania daty na kiedy powinna być ona dostarczona. |
| Moduł musi umożliwiać oznaczenie zamówienia preparatów krwi statusem CITO. |
| Podczas zamawiania preparatów krwi użytkownik musi mieć możliwość wskazania zamawianego zasobu oraz wymaganej ilości jednostek. |
| Moduł musi umożliwiać jednoczesne zamówienie wielu zasobów. |
| Moduł musi umożliwiać wydruk zamówienia na preparaty krwi. |
| Moduł musi umożliwiać konfigurację różnych wydruków zamówienia dla różnych preparatów krwi. |
| W przypadku integracji z modułem laboratorium serologicznego, podczas zamawiania preparatów krwi możliwe jest automatyczne zlecenia próby krzyżowej. |
| Moduł musi umożliwiać przyjęcie wydanych przez Bank Krwi zasobów za pomocą czytnika kodów kreskowych. Moduł weryfikuje poprawność skanowanych kodów kreskowych z kodami przesłanymi drogą elektroniczną przez Bank Krwi. Jedynie poprawna weryfikacja kodów pozwala przyjąć zasoby.  |
| Moduł posiada ekran prezentujący listę preparatów pacjenta. |
| Moduł musi umożliwiać przekazanie i zwrot donacji do Banku Krwi. |
| Moduł musi umożliwiać odnotowanie wykonania transfuzji wraz z odnotowaniem wykorzystanych donacji. |
| Moduł musi umożliwiać odnotowanie powikłania podczas transfuzji. |
| Moduł musi umożliwiać ręczne wprowadzenie grupy krwi pacjenta. Wprowadzenie grupy krwi wymaga autoryzacji wyniku przez drugiego użytkownika. |
| Moduł posiada ekran prezentujący listę prób krzyżowych pacjenta, na którym prezentowane są ich wyniki. |
| Moduł musi umożliwiać domyślną konfigurację zasobów ze świadczeniami zawartymi w umowach z NFZ. |
| Moduł musi umożliwiać automatyczne kodowanie domyślnych świadczeń NFZ dla zużytych podczas transfuzji zasobów. |
| Moduł musi umożliwiać konfigurację kilku świadczeń NFZ, które muszą zostać zakodowane po zużyciu jednego zasobu. |
| Moduł musi umożliwiać konfigurację domyślnej krotności świadczenia, która zostanie zakodowana po zużyciu zasobu. |

|  |
| --- |
| AP-DILO integracja, KRN Integracja |
| Wsparcie procesu Szybkiej Terapii Onkologicznej |
| W ramach wsparcia procesu SSO moduł udostępnia następujące funkcje: |
| a. Możliwość wprowadzenia i oddrukowania karty DiLO |
| b. Podpowiadanie numeru karty DiLO na ekranie kodowania |
| c. Oznaczenie pobytu PL, SSO |
| d. Oznaczenie pacjenta na zielono w podstawowym zakresie – tylko kolor |
| e. Oznaczenie pacjenta DiLO ze szczegółami terminów dot. SSO |
| f. Integracja z aplikacją DiLO (jak NFZ będzie gotowy) |
| System HIS zapewnia pełną elektroniczną integrację z systemem ApDILO w tym zakresie umożliwia: |
| a. Wydanie karty Diagnostyki i leczenia onkologicznego w kontekście pacjenta |
| b. System HIS rejestruje nadany numer przez system ApDILO z rekordem medycznym pacjenta |
| c. System musi umożliwiać rejestrację karty diagnostyki i leczenia onkologicznego wydanej w innej jednostce. |
| d. System HIS odbiera komunikaty zwrotne wysyłane z ApDILO |
| e. System HIS musi umożliwiać rozpoczęci i zakończenie etapu diagnostyki i leczenia onkologicznego. |
| f. System HIS musi umożliwiać automatyczne rozliczenie świadczeń wykonanych na pobytach/wizytach (np. w AOS) oznaczonych oraz powiązanych z diagnostyką i leczeniem onkologicznym |
| g. System HIS udostępnia funkcję automatycznego oznaczania pacjenta posiadającego wydana aktywna kartę diagnostyki i leczenia onkologicznego |
| h. System HIS udostępnia funkcję wskazującą aktualny etap diagnostyki i leczenia onkologicznego oraz jeżeli to jest możliwe prezentuje liczbę dni jaka upłynęła od rozpoczęcia danego etapu. |
| Wsparcie procesu zapisu na kolejkę oczekujących w zakresie: |
| a. Rozdzielenie kolejek na pierwszorazowych i kontynuujących leczenie |
| b. 10 kolejek centralnych o najdłuższych czasach oczekiwania |
| c. Obowiązek podmiotów do cotygodniowego raportowania |
| d. Spersonalizowane kolejki w komunikacie LIOCZ |
| e.14 dni na dostarczenie oryginału skierowania przez pacjenta |
| Elektroniczna KZNZ i integracja z KRN |
| System musi umożliwiać wprowadzanie klasyfikacji nowotworu. |
| System musi umożliwiać tworzenie w postaci elektronicznej Karty Zgłoszenia Nowotworu Złośliwego. |
| System musi umożliwiać automatyczne wysłanie w postaci elektronicznej Karty Zgłoszenia Nowotworu Złośliwego do Krajowego Rejestru Nowotworów. |
| System musi umożliwiać śledzenia statusu Karty Zgłoszenia Nowotworu Złośliwego w Krajowym Rejestrze Nowotworów. |
| W przypadku wprowadzenia przez użytkownika diagnozy z zakresu nowotworów - system powinien poinformować go o konieczności wprowadzania Klasyfikacji nowotworu oraz Karty Zgłoszenia Nowotworu Złośliwego. |
| W zależności od wprowadzonej diagnozy ICD-10, system wymusza uzupełnienie odpowiedniej klasyfikacji nowotworu (TNM, FIGO, Gleasona, Ann Arbour, Astlerra-Collera, Clarka). |
| System musi umożliwiać przegląd wprowadzonych klasyfikacji nowotworu na jednym ekranie (historii) w celu analizy zmian. |
| System musi umożliwiać uzupełnienie Karty Zgłoszenia Nowotworu Złośliwego - zgodnie z aktualnym stanem prawnym i wytycznymi Krajowego Rejestru Nowotworów. |
| System podpowiada użytkownikowi o konieczności wypełnienia Karty Zgłoszenia Nowotworu Złośliwego zgodnie z instrukcją wypełniania karty. |
| System posiada ekran prezentujący wszystkie stworzone Karty Nowotworu Złośliwego pacjenta. System prezentuje na nim min.: status karty w Krajowym Rejestrze Nowotworów (Status karty w Krajowym Rejestrze Nowotworów aktualizowany jest automatycznie); rozpoznanie; data wypełnienia, numer karty. |
| W przypadku przekazania przez Krajowy Rejestr Nowotworu informacji o błędzie w wypełnieniu Karty Zgłoszenia Nowotworu Złośliwego - system powinien prezentować tą informację na ekranie listy wszystkich kart pacjenta. |

|  |
| --- |
| System musi umożliwiać wprowadzanie klasyfikacji nowotworu. |
| Po wrowadzeniu rozpoznania zasadniczego z zakresu nowotworowego system przypomina o wprowadzeniu klasyfikacji nowotworu i wypełnieniu Karty Zgłoszenia Nowotworu Złośliwego (KZNZ) |
| System musi umożliwiać tworzenie w postaci elektronicznej Karty Zgłoszenia Nowotworu Złośliwego. |
| System musi umożliwiać automatyczne wysłanie w postaci elektronicznej Karty Zgłoszenia Nowotworu Złośliwego do Krajowego Rejestru Nowotworów oraz automatyczne zapisanie przydzielonego przez KRN numeru karty |
| System musi umożliwiać śledzenia statusu Karty Zgłoszenia Nowotworu Złośliwego w Krajowym Rejestrze Nowotworów. |
| W zależności od wprowadzonej diagnozy ICD-10, system powinien wymuszać uzupełnienie odpowiedniej klasyfikacji nowotworu (TNM, FIGO, Gleasona, Ann Arbour, Astlerra-Collera, Clarka). |
| System musi umożliwiać przegląd wprowadzonych klasyfikacji nowotworu na jednym ekranie (historii) w celu analizy zmian. |
| System musi umożliwiać uzupełnienie Karty Zgłoszenia Nowotworu Złośliwego - zgodnie z aktualnym stanem prawnym i wytycznymi Krajowego Rejestru Nowotworów. |
| System podpowiada użytkownikowi o konieczności wypełnienia Karty Zgłoszenia Nowotworu Złośliwego zgodnie z instrukcją wypełniania karty. |
| System posiada ekran prezentujący wszystkie stworzone Karty Nowotworu Złośliwego pacjenta. System prezentuje na nim min.: status karty w Krajowym Rejestrze Nowotworów (Status karty w Krajowym Rejestrze Nowotworów aktualizowany jest automatycznie); rozpoznanie; data wypełnienia, numer karty. |
| W przypadku przekazania przez Krajowy Rejestr Nowotworu informacji o błędzie w wypełnieniu Karty Zgłoszenia Nowotworu Złośliwego - system powinien prezentować tą informację na ekranie listy wszystkich kart pacjenta.  |

Wymagania ogólne dot. e-Usług

|  |
| --- |
| eUsługi dostępne w ramach systemu to zestaw funkcji, które umożliwiają interakcję z użytkownikiem (szczególnie pacjentem i lekarzem) metodą zdalną, między innymi za pośrednictwem internetu, w tym niektóre mogą być zabezpieczone dodatkowymi kanałami szyfrowanej komunikacji jak VPN i/lub HTTPS. Moduły są ściśle zintegrowane z częścią białą systemu, tj. HIS/RIS/PACS/WEB. Moduły te mają korzystać z tego samego zbioru danych co część medyczna. |
| Moduły eUsług dla pacjentów (tj. eUsługi portalu ePacjent, część dynamiczna portalu) opublikowane w internecie mają korzystać z tej samej bazy danych (w rozumieniu zbioru danych i modelu danych) co moduły systemu medycznego HIS i RIS, ale nie mogą łączyć się bezpośrednio do tej bazy, a jedynie poprzez dodatkowy zabezpieczony interfejs komunikacji (np. WebServices) w celu podniesienia bezpieczeństwa bazy danych osobowych i wrażliwych danych medycznych przetwarzanych w systemie HIS/RIS/PACS. |
| Z racji na podniesienie bezpieczeństwa przetwarzanych danych medycznych w publicznej sieci internet, nie akceptowalna jest realizacja wymagań udostępniania pacjentom danych medycznych za pomocą dodatkowej, pośredniej bazy danych bezpośrednio dostępnej z poziomu aplikacji publikowanych w internecie, do której byłyby kopiowane, a następnie przetwarzane dane osobowe i medyczne, co mogłoby znacząco obniżyć poziom bezpieczeństwa tych danych. |
| eUsługi dostępne w internecie dla pacjentów do komunikacji z częścią systemu w intranecie placówki (system HIS/RIS/PACS) mają wykorzystywać zabezpieczony kanał komunikacji (podniesienie bezpieczeństwa Systemu). |
| Wszystkie eUsługi związane są bezpośrednią komunikacją z pozostałymi modułami systemu medycznego (w szczególności związane z ruchem chorych, dokumentacją medyczną) są zarządzane spójnie przez jeden moduł administracyjny dla całego systemu medycznego przynajmniej w zakresie ruchu chorych, zarządzania lekami, dokumentacją medyczną opisową i obrazową, zleceniami medycznymi, grafikami dostępności. |

|  |
| --- |
| ePortal pacjenta to system zintegrowanych eUsług dedykowanych pacjentowi, świadczonych w formie elektronicznej, do których pacjent ma dostęp z dowolnego miejsca za pośrednictwem internetu. |
| System prowadzi dziennik aktywności użytkowników w ePortalu pacjenta. Dziennik musi umożliwiać przegląd co najmniej akcji: anulowania wizyty przez pacjenta; blokady konta przez pacjenta; edycji danych konta pacjenta; logowania do ePortalu pacjenta; nieudanego logowania do ePortalu pacjenta; rejestracji wizyty w ePortalu pacjenta; wylogowania z ePortalu pacjenta; założenia konta pacjenta. |
| System musi umożliwiać założenie konta w ePortalu pacjenta poprzez udostępniony na stronie głównej formularz rejestracyjny. |
| Formularz rejestracyjny zawiera dane, które jednoznacznie identyfikują nowego użytkownika. Nowy użytkownik musi obligatoryjnie uzupełnić co najmniej: imię, nazwisko, PESEL, numer telefonu oraz adres e-mail. |
| System weryfikuje dane wprowadzone przez nowego użytkownika pod kątem zawartości i zgodności w systemie medycznym. |
| System musi umożliwiać założenia konta w ePortalu pacjenta dla opiekuna pacjenta. |
| System musi umożliwiać konfigurację, w której konto użytkownika ePortalu pacjenta będzie zakładane automatycznie po uzupełnieniu danych lub wymagana będzie weryfikacja danych przez użytkownika systemu medycznego. |
| System musi umożliwiać upoważnionym użytkownikom systemu medycznego dostęp do listy złożonych wniosków o założenie konta w ePortalu pacjenta. Upoważniony użytkownik może zaakceptować lub odrzucić wniosek. |
| System musi umożliwiać wygenerowanie unikalnego identyfikatora dla nowego użytkownika ePortalu pacjenta - przez użytkownika systemu medycznego. Tak założone konto zostaje automatycznie powiązane z numerem pacjenta w systemie medycznym. |
| System musi umożliwiać dostęp do funkcji ePortalu pacjenta po wprowadzeniu unikalnego identyfikatora w systemie (tzw. loginu) oraz hasła. |
| ePortal pacjenta musi umożliwiać użytkownikowi (pacjent) zmianę hasła oraz nazwy użytkownika.  |
| System musi umożliwiać założenie nowego konta w ePortalu pacjenta za pomocą autoryzacji profilem zaufanym ePUAP. |
| System musi umożliwiać nadanie automatycznych uprawnień dostępu do korzystaniu z ePortalu w imieniu danego pacjenta dla innego użytkownika ePortalu, który jest wskazany w systemie ruchu chorych i wykazie pacjentów systemu medycznego HIS/RIS jako osoba upoważniona lub opiekun tego pacjenta. |
| Użytkownik modułu musi mieć możliwość udostępnienia swoich danych medycznych takich jak: wyniki badań, historie choroby, obrazy diagnostyczne osobom trzecim w trybie tylko do odczytu. |
| ePortal pacjenta korzysta z tej samej bazy danych (w rozumieniu zbioru danych i modelu danych) co system medyczny w intranecie. Nie może jednak łączyć się bezpośrednio do tej bazy (podniesienie bezpieczeństwa systemu), tylko za pomocą zabezpieczonego interfejsu, np. WebServices. |
| W przypadku braku danych kontaktowych (e-mail, telefon), system informuje o tym tuż po zalogowaniu do ePortalu pacjenta. |
| System musi umożliwiać pacjentowi przesłanie wiadomości dotyczącej działania serwisu; sugestii modyfikacji serwisu lub opinii na temat poziomu świadczonych usług.  |
| System prezentuje listę jednostek organizacyjnych wraz z danymi teleadresowymi, godzinami przyjęć, informacjami dodatkowymi i lokalizacją na mapie. |
| System prezentuje listę kolejek oczekujących wraz z przybliżonym czasem oczekiwania na przyjęcie, wyliczonym na podstawie danych z poprzedniego miesiąca. |
| Użytkownik musi mieć możliwość zmiany języka ePortalu pacjenta. Dostępne są co najmniej: język polski, język angielski, język rosyjski. |
| ePortal pacjenta spełnia wymagania dostępności serwisu www dla osób zagrożonych wykluczeniem cyfrowym. Wymagany poziom zgodności ze standardem WCAG 2.0 na poziomie co najmniej AA. |
| ePortal pacjenta musi oferować funkcjonalności zmiany wielkości czcionki za pomocą linku widocznego na stronie głównej portalu. Niedopuszczalne jest przyjęcie zmiany wielkości czcionki za pomocą powiększenia zawartości okna przeglądarki internetowej. |
| ePortal pacjenta musi oferować funkcjonalność zmiany kontrastu za pomocą ikony widocznej na stronie głównej portalu. |
| Co najmniej dla funkcjonalności eRejestracji - ePortal pacjenta musi współpracować z czytnikami transkrypcji mowy umożliwiając osobie niedowidzącej skorzystanie z eusługi i przejście procesu rejestracji na wizytę. |
| Moduł ePortal pacjenta zaprojektowany jest w technice RWD (Responsive Web Design). |
| Moduł musi umożliwiać rezerwację wizyt przez pacjenta metodą zdalną, za pośrednictwem internetu. |
| Moduł jest zintegrowany z system medycznym, w tym modułem grafików i kolejek oczekujących. Informacja o dokonanej rezerwacji trafia do systemu medycznego, gdzie wizyty z eRejestracji można odróżnić od pozostałych. Jednocześnie moduł korzysta z definicji tych samych grafików co system medyczny. |
| Rejestracja przez internet ma taki sam charakter i status jak rejestracja dokonana bezpośrednio w placówce medycznej. |
| Moduł musi umożliwiać pacjentowi wyszukanie wolnych terminów wizyt co najmniej wg kryteriów: lekarz, poradnia, usługa medyczna, data wizyty oraz czasu jej trwania (od-do). Do wyszukania najbliższego wolnego terminu, niezbędne jest podanie co najmniej nazwy usługi medycznej. |
| Po wybraniu jednego z kryteriów (lekarza, poradni lub usługi medycznej) lista wyboru dla pozostałych kryteriów zawęża się. |
| Po uzupełnieniu kryteriów wyszukiwania, moduł wyświetla listę wszystkich wolnych terminów spełniających kryteria. |
| Moduł prezentuje pacjentowi możliwych płatników za wizytę, wynikających z jego uprawnień (np. NFZ, komercja, abonament). Pacjent musi mieć możliwość wyboru płatnika. |
| Po wybraniu terminu z listy, moduł udostępnia ekran, na którym pacjent ostatecznie potwierdza wszystkie dane. |
| Moduł musi umożliwiać pacjentowi uzupełnienie danych skierowania lub załączenie skanu/zdjęcia skierowania podczas rezerwacji wizyty. Uzupełnione dane lub załączony skan/zdjęcie skierowania widoczne są w module służącym rejestracji wizyt w systemie medycznym.  |
| Moduł musi umożliwiać udostępnienie w eRejestracji tylko wybranych poradni. |
| Moduł musi umożliwiać ograniczenie liczby jednocześnie wprowadzanych przez pacjenta rezerwacji. |
| Moduł musi umożliwiać zablokowanie możliwości rejestracji on-line dla pacjenta pierwszorazowego w danej poradni. |
| Możliwość określenia procentowej puli grafika do wykorzystania przez eRejestrację. |
| Wszyscy pacjenci mogą korzystać z tej samej puli dostępnych terminów z uwzględnieniem definiowanego przez administratora procentowego podziału puli grafika na rejestracje przez internet oraz tradycyjne. |
| Moduł musi umożliwiać zablokowanie możliwości elektronicznej rejestracji wizyt w przypadku nie zjawienia się przez pacjenta na określonej liczbie potwierdzonych wizyt. Ilość wizyt może zostać skonfigurowane przez administratora. |
| Portal musi umożliwiać wskazanie lokalizacji poradni (Google maps) i prezentacji lokalizacji poradni pacjentowi (e-Mapy). Możliwość wskazania przez administratora współrzędnych poradni. |
| Moduł ma korzystać z tej samej bazy danych (w rozumieniu zbioru danych i modelu danych) co moduł ruchu chorych, ale nie może łączyć się bezpośrednio do tej bazy (podniesienie bezpieczeństwa systemu). |
| Aplikacja do komunikacji z systemem i bazą danych w intranecie placówki ma wykorzystywać zabezpieczony kanał komunikacji (podniesienie bezpieczeństwa systemu). |
| Wspólny moduł administracyjny z systemem medycznym. |
| System musi umożliwiać zdefiniowanie okresu w jakim pacjent musi potwierdzić zarezerwowaną wizytę (np. wizyty zarezerwowane na 7 dni przed terminem musza być potwierdzone od 4 do 2 dni przed wizytą, inaczej rezerwacja jest anulowana). |
| Możliwość konfiguracji terminu przypomnienia pacjentowi o wizycie. |
| Możliwość śledzenia statusu pacjenta na kolejce oczekujących zdefiniowanej w oddziale, poradni, pracowni. |
| Dla pacjentów przewlekle chorych system musi umożliwiać przesłanie „zamówienia” na wystawienie recepty na lek związany z terapią choroby przewlekłej w ramach rezerwacji wizyty recepturowej. |

|  |
| --- |
| eWYNIKI |
| Aplikacja musi umożliwiać pacjentowi przeglądanie wyników badań i obrazów diagnostycznych w formacie DICOM/JPG metodą zdalną za pośrednictwem internetu. |
| Pacjent korzystając z przygotowanej witryny internetowej może się zalogować, wybrać na podstawie różnych kryteriów (jednostka wykonująca, nazwa badania, status) interesujące go wyniki a następnie odczytać je, pobrać lub wydrukować. |
| Wyniki mogą być prezentowane jako lista lub hierarchicznie z podziałem na jednostki zlecające. |
| Możliwość konfiguracji okresu widoczności danego wyniku na liście wyników pacjenta. |
| Pełna integracja z Elektronicznym Rekordem Medycznym Pacjenta systemu medycznego, korzystanie z tego samego źródła danych, wspólnego modułu administracyjnego oraz słowników. |
| Moduł musi umożliwiać administratorom systemu wskazanie, których typów usług wyniki będą prezentowane pacjentowi. |

|  |
| --- |
| eDOKUMENTACJA |
| Moduł musi umożliwiać pacjentowi przeglądanie dokumentacji medycznej zapisanej w systemie medycznym. |
| Moduł udostępnia dokumentację zapisaną w repozytorium dokumentacji medycznej w systemie medycznym. |
| Pacjent musi mieć możliwość przejrzenia i wydruku dokumentacji medycznej. |
| Moduł prezentuje datę utworzenia dokumentacji medycznej. |
| Moduł musi umożliwiać filtrowanie dokumentacji medycznej co najmniej według: nazwy dokumentacji, daty utworzenia od, daty utworzenia do. |
| Pacjent musi mieć możliwość załączenia zeskanowanych załączników. Lekarz pracując w systemie medycznym może zdecydować, które z załączników dołączyć do dokumentacji medycznej wizyty lub pobytu. |
| Moduł musi umożliwiać załączanie przez pacjenta zewnętrznej dokumentacji medycznej. |
| Moduł musi umożliwiać załączanie dokumentów .pdf, .jpg, .png, .doc, .docx. |
| Podczas załączania dokumentu, pacjent musi mieć możliwość dodania opisu dokumentu. |
| Załączone przez pacjenta dokumenty widoczne są w module eDokumentacja. |
| Załączone przez pacjenta dokumenty widoczne będą w systemie medycznym w rekordzie medycznym pacjenta. |
| Pacjent musi mieć możliwość usuwania załączonych przez siebie dokumentów. |

|  |
| --- |
| eWYWIAD |
| Moduł musi umożliwiać pacjentowi przekazanie lekarzowi przed wizytą istotnych informacji dotyczących swojego stanu zdrowia. |
| Moduł musi umożliwiać skorzystanie ze zdefiniowanych formularzy strukturyzowanych stworzonych w module Generator formularzy systemu medycznego. |
| Moduł musi umożliwiać stworzenie różnych formularzy ewywiadu dla poszczególnych jednostek organizacyjnych. Formularze mogą różnić się zawartością i formą. |
| Wprowadzony przez pacjenta ewywiad widoczny jest w dokumentacji formularzowej w module gabinet lekarski systemu medycznego. |
| Lekarz musi mieć możliwość zapoznania się z ewywiadem przed wizytą. System musi umożliwiać poinformowanie lekarza o uzupełnieniu przez pacjenta ewywiadu. Lekarz musi mieć możliwość zadania dodatkowego pytania pacjentowi. |
| Moduł musi umożliwiać pacjentowi posiadającemu dostęp do ePortalu pacjenta wyznaczenie osób upoważnionych do uzyskiwania informacji o jego stanie zdrowia oraz do wglądu w dokumentację medyczną. |
| Moduł musi umożliwiać pacjentowi dodanie nowych osób lub wybór osób spośród tych, które są już zapisane w bazie danych. W celu uniknięcia pomyłek, dodanie nowej osoby lub wybór istniejącej, wymaga wprowadzenia imienia, nazwiska oraz peselu. Aby wybrać osobę zapisaną wcześniej w bazie danych - imię, nazwisko i pesel muszą być takie same.  |
| Moduł musi umożliwiać pacjentowi określenie stopnia pokrewieństwa z osobą, która zostaje wskazana. |
| Moduł musi umożliwiać pacjentowi wprowadzenie numeru telefonu osoby, która zostaje wskazana. |
| Moduł musi umożliwiać wskazanie zakresu upoważnienia wskazanej osoby, dat obowiązywania oraz dodanie ewentualnego komentarza. |
| Słownik upoważnień jest tożsamy ze słownikiem upoważnień w systemie medycznym. |
| Moduł musi umożliwiać administratorowi wskazanie, które z upoważnień dostępnych w systemie medycznym widoczne są w module. |
| Moduł musi umożliwiać pacjentowi przegląd listy osób upoważnionych wraz z zakresem upoważnień. |
| Moduł przenosi upoważnienia z modułu eZgoda do systemu medycznego oraz z systemu medycznego do modułu eZgoda. A więc upoważnienia i zgody dodane w module eZgoda widoczne są w systemie medycznym, a zgody i upoważnienia dodane w sytemie medycznym widoczne są w module eZgoda. |
| Moduł musi umożliwiać pacjentowi wygenerowanie dokumentu upoważnienia oraz podpisanie go kwalifikowanym podpisem elektronicznym lub profilem zaufanym ePUAP. Podpisany dokument zapisany zostanie w repozytorium elektronicznej dokumentacji medycznej w systemie medycznym. |
| Elektroniczna usługa skierowana do lekarzy, która ułatwi dostępność do specjalistów, którzy są nieobecni w miejscu świadczenia e-Usługi. Jest to usługa elektroniczna uruchomiona on-line na skierowana do lekarzy i współpracujących podmiotów medycznych wspomagająca proces leczenia. Wspiera proces komunikacji z innymi placówkami oraz lekarzami za pomocą funkcjonalności udostępnionej w komunikatorze. |
| Elektroniczna usługa skierowana do pacjentów, która umożliwi przeprowadzenie wideokonferencji z lekarzem w celu wykonania konsultacji medycznej. Za pomocą funkcjonalności udostępniania dokumentacji medycznej przez pacjenta w trakcie wideo konsultacji, lekarz będzie miał dostęp do udostępnionej na portalu dokumentacji medycznej (wyników badań, karty informacyjnej, obrazów diagnostycznych). |
| Usługa zapewnia bezpieczną transmisję danych zgodną z obecnie panującymi standardami i wymogami prawnymi. |
| Konsultacje on-line obrazu i dźwięku mogą odbywać się w jakości HD oraz niższej, w zależności od podłączonej stacji nadawczej i możliwości sieci. Wideo konsultacje realizowane są zdalnie, mogą obsługiwać do kilkunastu jednoczesnych połączeń (np. konsultacja 4-ech lekarzy jednocześnie) i zapewniają jakość wideo i audio umożliwiającą prowadzenie zdalnych konsultacji, mogą być realizowane z dedykowanych terminali, telefonów, tabletów, komputerów PC, pozwalając na udostępnienie np. obrazu z pulpitu roboczego. |

|  |
| --- |
| Wspólny moduł administracyjny dla portalu e-Pacjent oraz systemu HIS musi umożliwiać administrację funkcjami e-Pacjent oraz wspólnymi słownikami.  |
| Minimalny zakres funkcjonalności administracyjnych to: |
| W nagłówku portalu może zostać umieszczone logo jednostki medycznej. |
| Moduł administracyjny musi umożliwiać administratorowi na definiowanie przynajmniej następujących parametrów e-usług e-Portalu pacjenta: |
| umożliwia konfigurację szablonu wiadomości, jakie System będzie automatycznie wysyłał do pacjentów: przypomnienia o wizycie, przypomnienie o potwierdzeniu wizyty, anulowanie niepotwierdzonej wizyty |
| Umożliwia wskazanie E-mail: adres serwera i parametry SMTP (serwer poczty wychodzącej). |
| Czas generowania wiadomości: w momencie wykonania akcji w Systemie lub wyrażenie cron. |
| Aplikacja musi umożliwiać zawężenie listy poradni, w których pacjent może zarezerwować wizytę on-line. Listę wybranych poradni definiuje się w module administracyjnym. Nieustawienie tej opcji skutkuje tym, że pacjent musi mieć możliwość rezerwacji wizyty w dowolnej poradni szpitala, o ile istnieją na niej grafiki lekarzy. |
| umożliwia oznaczenie lekarza, jako „niewidocznego z poziomu e-Rejestracji”. W tym celu będzie można wybrać lekarza ze słownika i ewentualnie kolejną osobę, tworząc listę |
| Maksymalna liczba otwartych rezerwacji - Określa maksymalną liczbę otwartych rezerwacji na pacjenta. |
| Możliwość rezerwacji pacjentów pierwszorazowych - W przypadku włączenia opcji pacjent będzie mógł zarezerwować wizytę w dowolnej poradni. |
| Potwierdzanie wizyty - Opcja pozwala na zdefiniowanie czasu przeznaczonego na potwierdzenie wizyty przez pacjenta-(np. pomiędzy 10 do 3 dni przed wizytą), a w tym:• Początek okresu potwierdzenia- liczba dni przed wizytą. Wtedy wysyłany jest komunikat z prośbą o potwierdzenie wizyty.• Liczba dni na potwierdzenie wizyty: Dzień przed końcem okresu potwierdzania wysyłana jest kolejna wiadomość o konieczności potwierdzenia wizyty. Jeśli wizyta nie zostanie potwierdzona w określonym czasie, system anuluje ją automatycznie.  |
| Przypomnienie o wizycie - Opcja określa na ile dni przed wizytą ma zostać wysłane pacjentowi przypomnienie o wizycie. |
| Procentowa pula wizyt dla e-rejestracji - Opcja musi umożliwiać zdefiniowanie procentowej puli rezerwacji wizyt na dany dzień, na danego lekarza w danym gabinecie. Za każdym razem, gdy pacjent wyszukuje wizytę, sprawdzane ma być czy danego dnia, dla danej poradni i lekarza przekroczony został procentowo podany limit wizyt przewidzianych dla rezerwacji internetowych. Przykładowo jeśli dla parametru 20% mechanizm grafików wspólny dla systemu HIS i eRejestracji obliczy, że danego dnia jest zarezerwowanych internetowo 21% wizyt, to na ekranie wyszukiwania w eRejestracji, pacjent nie będzie mógł zarezerwować wizyty danego dnia przez Internet. |
| Maksymalna ilość prób logowania - Po wprowadzeniu liczby prób, włączone zostanie ograniczenie na liczbę nieudanych prób logowania. Po wykorzystaniu wszystkich prób, dostęp do konta zostanie zablokowany na czas określony w opcji „Czas blokady konta” |
| Czas blokady konta - Opcja pozwala na określenie czasu (w minutach), na jaki konto pacjenta zostanie zablokowane, po tym jak wykorzysta limit nieudanych prób logowania. |
| Adres internetowy do powiadomień - Opcja określa widziany adres e-mail w powiadomieniach wysyłanych pacjentowi. |
| Liczba minimalnych dni przed rezerwacją wizyty - Opcja określa liczbę dni przed terminem wizyty, kiedy pacjent nie może zarezerwować wizyty. Np.:- Wartość 0 oznacza, że pacjent może zarezerwować wizytę w dniu, kiedy ów wizyta ma się odbyć. - Wartość 1 oznacza, że pacjent może zarezerwować wizytę najpóźniej dzień przed planowaną. - Wartość 2 oznacza, że pacjent może zarezerwować wizytę najpóźniej 2 dni przed planowaną. itd. |
| Położenie poradni w google maps - Opcja określająca czy będzie możliwość podejrzenia położenia jednostek organizacyjnych w Google Maps. |
| Ilość nieobecności, po której następuje blokada użytkownika - Opcja określa maksymalną liczbę kolejnych nieobecności pacjenta na wizytach, po których blokowana jest możliwość rezerwacji |
| Limit e-rezerwacji na poradnię -Opcja określa maksymalną ilość oczekujących rezerwacji pacjenta na poradnię. Pacjent nie może zarezerwować na daną poradnię więcej niż X terminów. Brak ustawienia skutkuje brakiem limitów. |
| Mail do opiekuna eRejestracji - Adres e-mail do administratora systemu po stronie szpitala, odpowiedzialnego za kontakt mailowy z pacjentami |
| Dostępność (dni) wyników badań - Opcja określa okres (w dniach), przez jaki wyniki badania będą dostępne do podglądu przez pacjenta poprzez Portal pacjenta. Po dokonaniu pierwszego wydruku badania obowiązuje czas określony w opcji „Dostępność (dni) wyników badań po dokonaniu pierwszego wydruku wyników przez pacjenta”. |
| Dostępność (dni) wyników badań po dokonaniu pierwszego wydruku wyników przez pacjenta - Opcja określa okres (w dniach), przez jaki wyniki badania będą dostępne do podglądu przez pacjenta poprzez ePortal, po dokonaniu pierwszego wydruku wyników |
| Rezerwacje kolejkowe - Opcja określa czy użytkownik będzie miał możliwość przeglądania swoich danych odnośnie rezerwacji kolejkowych (np. przyczyny przesunięcia wizyty). |
| Login rzecznika praw pacjentaE-mail rzecznika praw pacjentaE-mail do pytań od pacjentówLogin osoby odpowiedzialnej za odpowiedzi na pytania pacjentów |
| informacje marketingowe – włączanie lub wyłączanie funkcji wysyłki informacji marketingowych do użytkowników e-Portalu pacjenta |

|  |
| --- |
| BEZPIECZEŃSTWO I KONFIGURACJA E-PACJENT |
| Serwer WWW powinien być udostępniony (chroniony) za dostarczanym UTM. |
| ePortal będzie wyposażony w certyfikat SSL. Będzie posiadał odpowiednią nazwę domenową. |
| Kluczowym elementem w infrastrukturze obsługującej ePortal jest certyfikat SSL. Umieszczony jest on na serwerze dostępowym do aplikacji. Zapewnia on bezpieczną, zaszyfrowaną komunikację przez sieć między stacją kliencką a serwerem. Infrastruktura klucza publicznego przewiduje, iż certyfikat taki jest wystawiany przez zaufany urząd certyfikacji (CA). Zamawiający zapewni Wykonawcy do instalacji wymagany certyfikat. |
| Dostarczony certyfikat musi pochodzić od dostawców uprawnionych do wystawiania certyfikatów SSL uznawanych przez wszystkie przeglądarki jako bezpieczne, np: GeoTrust, Thawte. Wykonawca dostarczy certyfikat na okres minimum 5 lat (lub będzie odnawiał certyfikaty w tym okresie) |
| Pole certyfikatu Common Name będzie taka sama jak nazwa subdomeny np. e-rejestracja.szpital-bartoszyce.pl. |
| Zamawiający utworzy adres poczty elektronicznej (e-mail) do powiadomień przekazywanych z usługi eRejestracja. |
| Zamawiający przeznaczy minimalne łącze internetowe z co najmniej jednym, statycznym adresem publicznym o przepustowości co najmniej 2Mbps dla ePortalu pacjenta. |
| ePortal pacjenta będzie zainstalowany na dedykowanej do tego celu maszynie, na który przeznaczone zostanie około: 2GB pamięci, 40GB przestrzeni dyskowej, 4 rdzenie CPU |

|  |
| --- |
| eKONTRAHENT |
| Moduł musi umożliwiać dwustronną wymianę zleceń badań i konsultacji pomiędzy placówką i jej kontrahentami (np. innymi jednostkami medycznymi). Moduł musi umożliwiać kontrahentom również rezerwowanie terminów wizyt dla pacjentów w placówce medycznej. Zlecenia badań i konsultacji oraz rezerwacje terminów wizyt odbywają się za pośrednictwem internetu. Kontrahenci korzystają ze specjalnie przygotowanej witryny internetowej. |
| eKontrahent posiada wspólny moduł administracyjny z systemem medycznym.  |
| System prowadzi dziennik logowań do modułu. |
| Moduł korzysta z tej samej bazy danych (w rozumieniu zbioru danych i modelu danych) co system medyczny w intranecie, ale nie może łączyć się bezpośrednio do tej bazy (podniesienie bezpieczeństwa systemu). |
| Do komunikacji z systemem medycznym w intranecie placówki, moduł wykorzystuje zabezpieczony kanał komunikacji (podniesienie bezpieczeństwa systemu). |
| Moduł musi umożliwiać określenie zakresu usług możliwych do rezerwacji i zlecania przez danego kontrahenta. |
| Moduł musi umożliwiać kontrahentom rezerwacje wizyty, zlecanie badań i konsultacji zarówno dla pacjentów przypisanych do danego kontrahenta jak również dla innych pacjentów zapisanych w bazie systemu medycznego.  |
| W przypadku wyszukiwania wśród pacjentów przypisanych do danego kontrahenta, istnieje możliwość wyszukiwania co najmniej według następujących kryteriów: pesel, imię, nazwisko, miasto, ulica, kod pocztowy. |
| W przypadku wyszukiwania wśród wszystkich pacjentów zapisanych w systemie medycznym - kontrahent musi wprowadzić poprawne: pesel lub datę urodzenia, imię, nazwisko. Wyszukanie pacjenta możliwe jest dopiero po wprowadzenia poprawnie łączenie trzech danych pacjenta. |
| Kontrahent musi mieć możliwość dodania nowego pacjenta do bazy systemu medycznego wprowadzając co najmniej: imię, nazwisko, pesel, płeć, datę urodzenia. Możliwe jest również wprowadzenie: telefonu, adresu e-mail oraz pełnego adresu. |
| Moduł musi umożliwiać kontrahentom rezerwacje terminów wizyty dla swoich pacjentów.  |
| Kontrahent musi mieć możliwość wyszukiwanie wolnych terminów dla wizyt co najmniej według: nazwy usługi, typu wizyty, lekarza, specjalności, jednostki organizacyjnej, daty i godziny. |
| Moduł eKontrahent korzysta z tej samej definicji grafików przychodni co system medyczny oraz moduł eRejestracja, dzięki czemu prezentowane są w nim tylko wolne terminy wizyt. |
| Podczas rezerwacji wizyty, kontrahent musi mieć możliwość uzupełnienia danych skierowania co najmniej w zakresie: rodzaju skierowania, daty skierowania, lekarza kierującego, jednostki kierującej, rozpoznania. W celu usprawnienia wprowadzania danych skierowania, moduł powinien automatycznie podpowiadać datę skierowania jako bieżącą, lekarza kierującego jako zalogowanego użytkownika oraz jednostkę kierującą jako jednostkę w której zatrudniony jest zalogowany użytkownik. |
| Moduł musi umożliwiać wydruk potwierdzenia rezerwacji wizyty. |
| Moduł musi umożliwiać przegląd zaplanowanych wizyt dla wybranych pacjentów kontrahenta wraz z informacją o statusie wizyty. |
| Moduł musi umożliwiać kontrahentom zlecenie badań i konsultacji, które zostają przesłane do systemu medycznego. |
| Podczas zlecenia badania lub konsultacji, kontrahent musi mieć możliwość wskazania co najmniej: nazwy usługi, priorytetu zlecenia, preferowanej daty wykonania, jednostki wykonującej, lekarza kierującego. |
| Moduł musi umożliwiać załączenie do zlecenia, obrazów w formie plików DICOM i przesłanie ich do konsultacji w systemie medycznym. |
| Zlecone przez kontrahenta badanie lub konsultacja trafia do systemu medycznego, gdzie może zostać wykonana. Po wykonaniu w systemie medycznym, wynik badania lub konsultacji wraca na listę zleceń wychodzących w module eKontrahent, gdzie możliwy jest przegląd wyniku. |
| Lista zleceń wychodzących w module eKonrahent prezentuje co najmniej: datę zlecenia, nr zlecenia, nazwę usługi, priorytet, datę wykonania, status, pacjenta, pesel, datę urodzenia. |
| Kontrahent musi mieć możliwość wyszukiwania zleceń na liście zleceń wychodzących co najmniej według: daty zlecenia od, daty zlecenia do, pacjenta (nazwisko, imię, pesel), statusu zlecenia, priorytetu, nazwy badania, nr zlecenia. |
| Moduł musi umożliwiać kontrahentom przyjmowanie zleceń badań i konsultacji wychodzących z systemu medycznego. |
| Użytkownik po stronie systemu medycznego, do zlecania badań lub konsultacji kontrahentom, używa tego samego modułu zleceń, za pomocą którego zlecane są badania wewnątrz placówki. |
| Użytkownik zlecający badanie w systemie medycznym musi mieć możliwość zadecydowania czy badanie lub konsultacja powinna być wykonana przez kontrahenta. Użytkownik musi mieć możliwość wyboru konkretnego kontrahenta, do którego zlecenie zostanie przesłane. |
| Użytkownik zlecający badanie lub konsultacje w systemie medycznym musi mieć możliwość załączenia poprzednich wyników badań pacjenta do tworzonego zlecenia. Mogą to być również badania posiadające obrazy w formie plików DICOM. |
| Użytkownik zlecający badanie lub konsultacje w systemie medycznym musi mieć możliwość zanonimizowania danych pacjenta. W takiej sytuacji w module e-Kontrahent nie będą widoczne: imię, nazwisko i pesel pacjenta. |
| Zlecenie badanie lub konsultacji przekazywane jest do moduł eKontrahent, gdzie pojawia się na liście zleceń przychodzących. |
| Moduł eKontrahent weryfikuje uprawnienia użytkownika. Zalogowany użytkownik widzi na liście zleceń przychodzących tylko zlecenia kierowane do kontrahenta, gdzie jest zatrudniony. |
| Lista zleceń przychodzących w module eKonrahent prezentuje co najmniej: datę zlecenia, nr zlecenia, nazwę usługi, priorytet, datę wykonania, status, imię i nazwisko pacjenta, pesel, datę urodzenia. |
| Kontrahent musi mieć możliwość wyszukiwania zleceń na liście zleceń przychodzących co najmniej według: daty zlecenia od, daty zlecenia do, statusu zlecenia, priorytetu, nazwy badania, nr zlecenia. |
| Kontrahent musi mieć możliwość podejrzenia danych zlecenia - a więc informacji uzupełnionych podczas zlecania badania w systemie medycznym placówki. |
| Kontrahent musi mieć możliwość podglądu załączonych do zlecenia plików DICOM, za pomocą przeglądarki diagnostycznej dostępnej z poziomu modułu e-Kontrahent.  |
| Kontrahent musi mieć możliwość wprowadzenia wyniku badania lub konsultacji, który zostaje przesłany do systemu medycznego. Wynik wprowadzony przez kontrahenta, jest prezentowany w systemie medyczny w taki sam sposób jak wyniki pochodzące z systemów wewnętrznych placówki. |

|  |
| --- |
| eOBCHÓD |
| System wyposażony jest w moduł dedykowany do pracy na urządzeniach mobilnych wyposażonych wyłącznie w ekran dotykowy.  |
| Moduł jest zrealizowany w architekturze trójwarstwowej oraz musi mieć możliwość pracy z wykorzystaniem przeglądarki internetowej bez konieczności instalacji dodatkowej aplikacji. |
| Moduł jest w pełni zintegrowany z systemem szpitalnym i działa na tym samym motorze bazy danych co system szpitalny. Dane zapisane w Module są dostępne natychmiast także w systemie szpitalnym. Dane zapisane równolegle przez innych użytkowników w systemie szpitalnym są także natychmiast dostępne w Module. |
| Moduł działa na urządzeniach typu tablet opartych na systemach operacyjnych Windows, iOS, Android. |
| Użyte w interfejsie graficznym Modułu komponenty wprowadzania danych i nawigacji dostosowane są do pracy z wykorzystaniem ekranu dotykowego (m.in. większe przyciski, pola edycyjne, zakładki, itp.). Wykorzystanie klawiatury ekranowej jest ograniczone do niezbędnego minimum. |
| Moduł współpracuje z Systemem Identyfikacji Pacjenta systemu HIS. W szczególności możliwe jest zidentyfikowanie pacjenta z opaski ze znakiem identyfikacyjnym, w którą został zaopatrzony pacjent w szpitalu. |
| Program na urządzeniu klienckim nie może trwale gromadzić przetwarzanych danych osobowych i medycznych. Musi być możliwość poprawnej pracy rozwiązania bez konieczności korzystania z lokalnej bazy danych na urządzeniu. |
| Do uruchomienia wystarczająca jest przeglądarka stron WWW (przynajmniej Chrome, Safari). |
| Identyfikacja pacjenta wg znaku identyfikacyjnego pacjenta i wyszukiwanie w systemie. |
| Możliwość podglądu danych pacjentów znajdujących się w szpitalu, na poszczególnych oddziałach w zakresie: |
| - data rozpoczęcia pobytu, |
| - historia pobytu, |
| - sala/oddział/izba przyjęć, |
| - diagnoza, |
| - lekarz prowadzący, |
| - status pobytu, |
| - zlecone badania i wyniki, |
| - zlecone leki, |
| - zdjęcia radiologiczne z PACS dla badań wraz z opisami, |
| - opisowe dane dokumentacji medycznej, |
| - podgląd graficzny karty gorączkowej. |
| Możliwość sprawdzenia wyników badań pacjenta w ramach pobytu. |
| Możliwość wprowadzania danych: |
| - składanie zleceń nowych podań leków, |
| - składanie zleceń badań, |
| - składanie zleceń badań z panelów zleceń o wspólnej konfiguracji z modułem oddział, |
| - składanie zleceń badań przez wyszukiwanie badań ze słownika, |
| - odnotowanie podań zleconych leków, |
| - odnotowanie czynności pielęgniarskich, |
| - odnotowywanie parametrów życiowych i karty gorączkowej. |
| Prezentacja podręcznych informacji lekarskich/wbudowanych zestawień danych, z których można wybrać pacjenta i rozpocząć pracę na wybranym rekordzie z listy (co najmniej): |
| - 'moi pacjenci', |
| - 'moje dokumenty w trybie szkic', |
| - 'moje zadania na dziś' |
| - 'wyniki badań pacjentów' |
| Możliwość wyszukiwania pacjentów. |
| - wg struktury organizacyjnej oddziałów i sal |
| - wg wybranych danych pacjenta (przynajmniej nazwisko, identyfikator pacjenta, identyfikator Systemu Identyfikacji Pacjenta) |
| Możliwość uruchomiania podglądu obrazów diagnostycznych w postaci referencyjnej:- system prezentuje dane pacjenta, opis oraz miniaturkę obrazu (tzw. thumbnails) z możliwością podglądu obrazu w jakości referencyjnej.- w przypadku wyniku serii obrazów DICOM (np. tomografia) moduł udostępnia odrębny JPG dla każdego obrazu serii, a następnie musi umożliwiać jego płynne odtworzenie w jakości referencyjnej. |
| Jednolity sposób logowania do Modułu na urządzenia mobilne typu tablet oraz dostarczanego systemu szpitalnego - za pomocą tego samego loginu i hasła. |
| System szpitalny wraz z Modułem korzystają ze wspólnej definicji wykorzystywanych w systemie słowników (badania, użytkownicy, uprawnienia, lekarze zlecający, lekarze opisujący, inne wykorzystywane w systemie HIS oraz niezbędne w dostarczanym rozwiązaniu). Zmiana w jednym systemie powoduje automatyczną zmianę pozycji słownikowej w drugim systemie. |
| System szpitalny i Moduł są zintegrowane w sposób umożliwiający ograniczenie wielokrotnego wpisywania tych samych danych. Dane wprowadzone w systemie tabletowym są natychmiast widoczne w systemie HIS. |
| Moduł oraz system szpitalny korzystają z tego samego rejestru pacjentów. |
| Moduł oraz system szpitalny zarządzane są przez jeden moduł administracyjny. |
| Moduł prezentuje ustrukturyzowane formularze dokumentacji medycznej systemu szpitalnego korzystając z tej samej definicji formularzy co system szpitalny i moduł administracyjny systemu szpitalnego - formularz podzielony jest na te same atrybuty. |
| Moduł pozwala na identyfikację pacjenta na podstawie opaski z kodem identyfikującym pacjenta. |

|  |
| --- |
| Moduł eSamokontrola dostęny musi być dla pacjenta w ePortalu pacjenta. |
| Moduł umożliwia administratorom systemu dowolne tworzenie badań, które dostępne będą do zlecania w ramach samokontroli dla pacjenta. |
| Moduł musi umożliwiać administratorom systemu tworzenie formularzy, które udostępniane będą do uzupełnienia dla pacjenta, w ramach realizacji badań samokontroli.  |
| Moduł zintegrowany jest z systemem medycznym i musi umożliwiać lekarzom zlecanie badań samokontroli za pomocą modułu zleceń dostępnego w ramach obsługi pacjenta w gabinecie lekarskim i szpitalu. |
| Moduł musi umożliwiać lekarzowi zlecenie badań samokontroli na określony okres (od dnia do dnia) i w określonych częstotliwościach (np. 3x dziennie o 8:00, 12:00, 16:00). |
| Zlecone badania samokontroli prezentowane są pacjentowi w module pod datą i godziną, na które zostały zlecone. |
| Wprowadzone przez pacjenta wyniki badań samokontroli, dostępne są w systemie medycznym w sposób analogiczny na wyniki innych badań. |
| Wprowadzone przez pacjenta wyniki badań samokontroli, dostępne są w module eSamkontrola dla pacjenta. |
| Moduł musi umożliwiać lekarzowi przekazanie zaleceń dotyczących realizacji badań (np. na czczo, tuż po jedzeniu itd.). Zalecenia widoczne są dla pacjenta w module eSamokontrola. |
| Moduł musi umożliwiać prezentację norm, w których powinny zawierać się wyniki badań. Normy mogą być widoczne dla pacjenta. |
| Wyniki wprowadzonych badań samokontroli mogą być dostępne dla lekarza zlecającego z ekranu głównego systemu medycznego. |

# Przeszkolenie pracowników Zamawiającego z dostarczanych rozwiązań

Szkolenia mają na celu osiągniecie odpowiedniej wiedzy z zakresu używania Systemu na odpowiednich stanowiskach służbowych. Przeprowadzenie pakietu szkoleń powinno zostać odpowiednio skoordynowane z przeprowadzeniem procesu wdrożenia, a w szczególności z procedurą migracji danych.

Wykonawca przeprowadzi szkolenie dla użytkowników (co najmniej 120 osób; 65 kobiet i 55 mężczyzn) w wymiarze co najmniej 4 godzin w grupach nie większych niż 15 osób lub w formie warsztatów przystanowiskowych. W przypadku szkoleń grupowych Wykonawca zapewni sprzęt na szkolenie (1 komputer dla każdego użytkownika szkoleń, projektor). Zamawiający zapewni salę szkoleniową celem realizacji szkoleń.

W ramach szkoleń Wykonawca przeszkoli grupy użytkowników odpowiednio do wdrażanych rozwiązań systemowych.

# Gwarancja i wsparcie

Świadczenie usługi gwarancji i wsparcia ma na celu zapewnienie ciągłości sprawnego działania Systemu poprzez realizację działań naprawczych wynikających z analizy ujawnionych problemów, wykrytych Dysfunkcji systemów, niewłaściwego działania systemu, spadku wydajności, wykryciu zagrożenia włamania, itp. Zakres i warunki opisane w umowie.

Wykonawca zobowiązuje się do dostarczania wolnych od wad kolejnych wersji Systemu.

Wykonawca zobowiązuje się do aktualizacji dokumentacji Użytkownika i/lub Administratora.

Wykonawca zobowiązuję się do świadczenia konsultacji dla Administratorów w zakresie niezbędnych zmian w konfiguracji systemu.

Wykonawca zapewni usługę wsparcia użytkowników udostępniając:

* + usługę typu helpdesk w ramach gwarancji, udostępnioną pod adresem e-mail, numerem telefonu
	+ portal – dostępny on-line w trybie 365/7/24, gdzie będą publikowane m.in. statusy zgłoszeń oraz ich treść i historia korespondencji
	+ przez niniejszy portal będą mogły być dokonywane zgłoszenia Dysfunkcji

Wsparcie użytkowników obejmuje świadczenie usługi wsparcia technicznego, merytorycznego oraz konsultacji w celu utrzymania poprawnej pracy systemu zgodnego z wymaganiami zamówienia. W ramach usługi Wykonawca zobowiązany jest do udzielania odpowiedzi na pytania Administratorów związane z bieżącą eksploatacją Systemu.

Wykonawca zapewni w godzinach pracy Zamawiającego w dni robocze obecność specjalistów mających niezbędną wiedzę i doświadczenie z zakresu eksploatacji Systemów.

Wykonawca zapewni wystarczającą ilość konsultantów do zapewnienia ciągłości usługi gwarancji.

Wykonawca będzie świadczył na rzecz Zamawiającego usługi serwisu w zakresie przedmiotu zamówienia (umowy) w zaoferowanym w postępowaniu okresie (licząc od daty podpisania protokołu odbioru) zapewniając jednocześnie odpowiednie wsparcie merytoryczne.

W ramach usługi Wykonawca zobowiązany jest do nieodpłatnego usuwania dysfunkcji:

* + z przyczyn zawinionych przez Wykonawcę będących konsekwencją wystąpienia: Dysfunkcji w Systemie, błędu lub wady fizycznej pakietu aktualizacyjnego lub instalacyjnego, błędu w dokumentacji administratora lub w dokumentacji użytkownika, błędu w wykonaniu usług przez Wykonawcę;
	+ związanych z realizacją usługi wdrożenia Systemu;
	+ spowodowanych aktualizacjami Systemu.

Wykonawca musi informować Zamawiającego o dostępnych aktualizacjach i poprawkach Systemów.

Zgłaszający, w przypadku wystąpienia dysfunkcji przesyła do Wykonawcy przy pomocy środków komunikacji formularz zgłoszenia wystąpienia Dysfunkcji. W Zgłoszeniu powinny być wypełnione wszystkie obligatoryjne pola formularza, a opis sytuacji prowadzącej do wystąpienia błędu lub awarii powinien umożliwiać jej odtworzenie przez zespół serwisowy Wykonawcy. Jeżeli odtworzenie błędu nie będzie możliwe w środowisku Wykonawcy, wówczas zdiagnozuje on błąd w środowisku Zamawiającego, a terminy usunięcia Dysfunkcji ulegają wydłużeniu o czas oczekiwania na dostęp do środowiska Zamawiającego.

Wykonawca zobowiązany jest do potwierdzenia w ciągu 1 godziny przyjęcia Zgłoszenia oraz jego klasyfikację. Potwierdzenie zostanie wysłane przez Wykonawcę do zgłaszającego.

Wykonawca zapewnia dostosowanie do obowiązujących przepisów nie później niż w dniu ich wejścia w życie.

Zgłoszenia będą klasyfikowane zgodne ze słownikiem pojęć, zawartym w Załączniku nr 3 do Umowy, przez Zamawiającego w uzgodnieniu z Wykonawcą.

Wykonawca zobowiązany jest do usunięcia dysfunkcji w terminach wymienionych w pkt 6 procedury podejmowania prac serwisowych zawartej w Załączniku nr 3 do Umowy.

W każdym przypadku Zgłaszający i Wykonawca mogą uzgodnić inny czas dostarczenia rozwiązania niż określono w warunkach gwarancji. W takim przypadku niezbędne jest potwierdzenie ustalonego terminu w formie pisemnej, faksem lub e-mailem.

1. Parametr ważny ze względu na sposób wykorzystania serwerów. [↑](#footnote-ref-2)
2. Nazwa własna użyta ze względu na wymóg użycia konkretnego silnika bazodanowego. [↑](#footnote-ref-3)
3. Nazwa własna użyta ze względu na wymóg użycia konkretnego silnika bazodanowego. [↑](#footnote-ref-4)