**Numer sprawy: 9/PN/18 Załącznik nr 2**

**SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA**

**Wymagania minimalne**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **OPIS PRZEDMIOTU ZAMÓWIENIA** | | | | | |
| **Lp** | **Oznaczenie produktu zamówienia** | **Wymóg graniczny (TAK / NIE) lub informacja o wyborze punktowanym** | **Wymóg spełniony (TAK / NIE / OPCJA – w wybranych polach)** | | |
| 1. **Serwer aplikacyjny – 2 sztuki** | | | | | |
|  | Obudowa:   * Typu RACK, wysokość nie więcej niż 2U; * Szyny umożliwiające pełne wysunięcie serwera z szafy stelażowej wraz z ramieniem porządkującym kable | TAK | | |  |
|  | Płyta główna:   * Dwuprocesorowa; * Wyprodukowana i zaprojektowana przez producenta serwera * Możliwość instalacji modułu TPM 2.0 * Możliwość instalacji procesorów 28-rdzeniowych; * 6 złącz PCI Express generacji 3w tym:   + 3 złącza o prędkości x16;   + 3 złącza o prędkości x8; * 24 gniazda pamięci RAM; * Obsługa minimum 3072GB pamięci RAM; * Wsparcie dla technologii:   + Memory Scrubbing   + SDDC   + Advanced ECC   + Rank Sparing; | TAK | | |  |
|  | Procesory:   * Dwa procesory 8-rdzeniowe * Architektura x86 * Taktowanie 2,1GHz * 11MB cache | TAK | | |  |
|  | Pamięć RAM:   * Zainstalowany rozmiar: 128 GB pamięci RAM * Typ: DDR4 Registered * Częstotliwość: 2666Mhz | TAK | | |  |
|  | Dyski twarde i napędy:   * Minimum 4 wnęki dla dysków twardych Hotplug 3,5”; * Możliwość rozbudowy do 8 wnęk dla dysków twardych Hotplug 3,5”; | TAK | | |  |
|  | 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 i iSCSI boot; * Karta LAN 4x 1Gbit Base-T; możliwość wymiany zainstalowanych interfejsów LAN na interfejsy 4x 10Gbit SFP lub 2x 10Gbit Base-T bez potrzeby wymiany całego układu lub instalacji dodatkowych kart w slotach PCI Express | TAK | | |  |
|  | Kontrolery I/O:   * Możliwość zainstalowania kontrolera RAID obsługującego dyski NVMe * Zainstalowanie dwa nośniki flash o pojemności 64GB w konfiguracji RAID-1, rozwiązanie dedykowane dla hypervisora, niezajmujące zatok dla dysków hot-plug * Zainstalowana jedna karta dwuportowa FC 16Gb | TAK | | |  |
|  | Porty:   * Zintegrowana karta graficzna ze złączem VGA z tyłu serwera; * 2 porty 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; | TAK | | |  |
|  | Zasilanie, chłodzenie:   * Redundantne zasilacze hotplug o sprawności 94% (tzw. klasa Platinum) o mocy 450W; * Redundantne wentylatory hotplug; | TAK | | |  |
|  | Zarządzanie:   * Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera; * 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;   + 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;   + Dostęp poprzez przeglądarkę Web, SSH;   + Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii;   + Zarządzanie alarmami (zdarzenia poprzez SNMP)   + Możliwość przejęcia konsoli tekstowej   + Możliwość zarządzania przez 6 administratorów jednocześnie   + Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM)   + Obsługa serwerów proxy (autentykacja)   + Obsługa VLAN   + Możliwość konfiguracji parametru Max. Transmission Unit (MTU)   + Wsparcie dla protokołu SSDP   + Obsługa protokołów TLS 1.0, TLS 1.1, TLS 1.2, SSL v3   + Obsługa protokołu LDAP   + Integracja z HP SIM   + Synchronizacja czasu poprzez protokół NTP   + 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 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; | TAK | | |  |
|  | Wspierane systemy operacyjne:   * Microsoft Windows Server 2016 oraz 2012 R2 * VMWare vSphere 6.5 oraz 6 * Suse Linux Enterprise Server 12 * Red Hat Enterprise Linux 6 oraz 7 | TAK | | |  |
|  | Gwarancja:   * 5 lat gwarancji producenta serwera w trybie on-site z gwarantowanym czasem usunięcia usterki do końca następnego dnia od zgłoszenia. * Zgłaszanie usterek i awarii sprzętowych poprzez automatyczne założenie zgłoszenia w systemie helpdesk/servicedesk producenta sprzętu; * Firma serwisująca musi posiadać ISO 9001:2000 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 w trybie onsite z gwarantowanym skutecznym zakończeniem naprawy serwera najpóźniej w następnym dniu roboczym od zgłoszenia usterki (podać koszt na dzień składania oferty); | TAK | | |  |
|  | 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 – wymaganie oświadczenie wykonawcy lub producenta; | TAK | | |  |
|  | Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera; | TAK | | |  |
|  | 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; | TAK | | |  |
|  | 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; | TAK | | |  |
|  | Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w UE – wymagane oświadczenie wykonawcy lub producenta; | TAK | | |  |
|  | 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. | Warunek opcjonalny, dodatkowo punktowany:  - spełnione (TAK): 1pkt  - niespełnione (NIE): 0pkt | | |  |
|  | Sprzęt wyprodukowany na terenie Unii Europejskiej | Warunek opcjonalny, dodatkowo punktowany:  - spełnione (TAK): 1pkt  - niespełnione (NIE): 0pkt | | |  |
| 1. **Serwer bazodanowy – 2 sztuki** | | | | | |
|  | Obudowa:   * Typu RACK, wysokość nie więcej niż 2U; * Szyny umożliwiające pełne wysunięcie serwera z szafy stelażowej wraz z ramieniem porządkującym kable | TAK | | |  |
|  | Płyta główna:   * Dwuprocesorowa; * Wyprodukowana i zaprojektowana przez producenta serwera * Możliwość instalacji modułu TPM 2.0 * Możliwość instalacji procesorów 28-rdzeniowych; * 6 złącz PCI Express generacji 3w tym:   + 3 złącza o prędkości x16;   + 3 złącza o prędkości x8; * 24 gniazda pamięci RAM; * Obsługa minimum 3072GB pamięci RAM; * Wsparcie dla technologii:   + Memory Scrubbing   + SDDC   + Advanced ECC   + Rank Sparing; | TAK | | |  |
|  | Procesor:   * Jeden procesor 8-rdzeniowy * Architektura x86 * Taktowanie 3,5GHz * 24MB cache | TAK | | |  |
|  | Pamięć RAM:   * Zainstalowany rozmiar: 128 GB pamięci RAM * Typu: DDR4 Registered * Częstotliwość: 2666Mhz | TAK | | |  |
|  | Dyski twarde i napędy:   * Minimum 4 wnęki dla dysków twardych Hotplug 3,5”; * Możliwość rozbudowy do 8 wnęk dla dysków twardych Hotplug 3,5”; * Zainstalowane 3 dyski 600GB SAS 12G 15 000 obr./min. | TAK | | |  |
|  | 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 i iSCSI boot; * Karta LAN 4x 1Gbit Base-T; możliwość wymiany zainstalowanych interfejsów LAN na interfejsy 4x 10Gbit SFP lub 2x 10Gbit Base-T bez potrzeby wymiany całego układu lub instalacji dodatkowych kart w slotach PCI Express | TAK | | |  |
|  | Kontrolery I/O:   * Kontroler SAS RAID 12G 0,1,1E,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, niezajmujące zatok dla dysków hot-plug * Zainstalowana jedna karta dwuportowa FC 16Gb | TAK | | |  |
|  | Porty:   * Zintegrowana karta graficzna ze złączem VGA z tyłu serwera; * 2 porty 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; | TAK | | |  |
|  | Zasilanie, chłodzenie:   * Redundantne zasilacze hotplug o sprawności 94% (tzw. klasa Platinum) o mocy 450W; * Redundantne wentylatory hotplug; | TAK | | |  |
|  | Zarządzanie:   * Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera; * 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;   + 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;   + Dostęp poprzez przeglądarkę Web, SSH;   + Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii;   + Zarządzanie alarmami (zdarzenia poprzez SNMP)   + Możliwość przejęcia konsoli tekstowej   + Możliwość zarządzania przez 6 administratorów jednocześnie   + Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM)   + Obsługa serwerów proxy (autentykacja)   + Obsługa VLAN   + Możliwość konfiguracji parametru Max. Transmission Unit (MTU)   + Wsparcie dla protokołu SSDP   + Obsługa protokołów TLS 1.0, TLS 1.1, TLS 1.2, SSL v3   + Obsługa protokołu LDAP   + Integracja z HP SIM   + Synchronizacja czasu poprzez protokół NTP   + 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 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; | TAK | | |  |
|  | Wspierane systemy operacyjne:   * Microsoft Windows Server 2016 oraz 2012 R2 * VMWare vSphere 6.5 oraz 6 * Suse Linux Enterprise Server 12 * Red Hat Enterprise Linux 6 oraz 7 | TAK | | |  |
|  | Gwarancja:   * 5 lat gwarancji producenta serwera w trybie on-site z gwarantowanym czasem usunięcia usterki do końca następnego dnia od zgłoszenia. * Uszkodzone dyski twarde nie muszą być zwracane organizacji serwisowej * Zgłaszanie usterek i awarii sprzętowych poprzez automatyczne założenie zgłoszenia w systemie helpdesk/servicedesk producenta sprzętu; * Firma serwisująca musi posiadać ISO 9001:2000 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 w trybie onsite z gwarantowanym skutecznym zakończeniem naprawy serwera najpóźniej w następnym dniu roboczym od zgłoszenia usterki (podać koszt na dzień składania oferty); | TAK | | |  |
|  | 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 – wymaganie oświadczenie wykonawcy lub producenta;  Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w UE – wymagane oświadczenie wykonawcy lub producenta; | TAK | | |  |
|  | 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; | TAK | | |  |
|  | 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; | TAK | | |  |
|  | Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera; | TAK | | |  |
|  | 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. | Warunek opcjonalny, dodatkowo punktowany:  - spełnione (TAK): 1pkt  - niespełnione (NIE): 0pkt | | |  |
|  | Sprzęt wyprodukowany na terenie Unii Europejskiej | Warunek opcjonalny, dodatkowo punktowany:  - spełnione (TAK): 1pkt  - niespełnione (NIE): 0pkt | | |  |
| 1. **Serwer backupowy – 1 sztuka** | | | | | |
|  | Obudowa:   * Typu RACK, wysokość nie więcej niż 2U; * Szyny umożliwiające pełne wysunięcie serwera z szafy stelażowej wraz z ramieniem porządkującym kable | TAK |  | | |
|  | Płyta główna:   * Dwuprocesorowa; * Wyprodukowana i zaprojektowana przez producenta serwera * Możliwość instalacji modułu TPM 2.0 * Możliwość instalacji procesorów 28-rdzeniowych; * 6 złącz PCI Express generacji 3w tym:   + 3 złącza o prędkości x16;   + 3 złącza o prędkości x8; * 24 gniazda pamięci RAM; * Obsługa minimum 3072GB pamięci RAM; * Wsparcie dla technologii:   + Memory Scrubbing   + SDDC   + Advanced ECC   + Rank Sparing; | TAK |  | | |
|  | Procesory:   * Jeden procesor 8-rdzeniowy * Architektura x86 * Taktowanie 2,1GHz * 11MB cache | TAK |  | | |
|  | Pamięć RAM:   * Zainstalowany rozmiar: 128 GB pamięci RAM * Typu: DDR4 Registered * Częstotliwość: 2666Mhz | TAK |  | | |
|  | Dyski twarde i napędy:   * Minimum 12 wnęk dla dysków twardych Hotplug 3,5”; * Zainstalowane 12 dysków 4TB SAS(NL-SAS) 12G | TAK |  | | |
|  | 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 i iSCSI boot; * Karta LAN 4x 1Gbit Base-T; możliwość wymiany zainstalowanych interfejsów LAN na interfejsy 4x 10Gbit SFP lub 2x 10Gbit Base-T bez potrzeby wymiany całego układu lub instalacji dodatkowych kart w slotach PCI Express | TAK |  | | |
|  | Kontrolery I/O:   * Kontroler SAS RAID 12G 0,1,10,5,50,6,60 z 1GB pamięci cache * Możliwość zainstalowania kontrolera RAID obsługującego dyski NVMe * Możliwość zainstalowania dwóch nośników flash o pojemności 64GB w konfiguracji RAID-1, rozwiązanie dedykowane dla hypervisora, niezajmujące zatok dla dysków hot-plug * Zainstalowana jedna karta dwuportowa FC 16Gb | TAK |  | | |
|  | Porty:   * Zintegrowana karta graficzna ze złączem VGA z tyłu serwera; * 1 port USB 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; | TAK |  | | |
|  | Zasilanie, chłodzenie:   * Redundantne zasilacze hotplug o sprawności 94% (tzw. klasa Platinum) o mocy 450W; * Redundantne wentylatory hotplug; | TAK |  | | |
|  | Zarządzanie:   * Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera; * 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;   + 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;   + Dostęp poprzez przeglądarkę Web, SSH;   + Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii;   + Zarządzanie alarmami (zdarzenia poprzez SNMP)   + Możliwość przejęcia konsoli tekstowej   + Możliwość zarządzania przez 6 administratorów jednocześnie   + Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM)   + Obsługa serwerów proxy (autentykacja)   + Obsługa VLAN   + Możliwość konfiguracji parametru Max. Transmission Unit (MTU)   + Wsparcie dla protokołu SSDP   + Obsługa protokołów TLS 1.0, TLS 1.1, TLS 1.2, SSL v3   + Obsługa protokołu LDAP   + Integracja z HP SIM   + Synchronizacja czasu poprzez protokół NTP   + 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 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; | TAK |  | | |
|  | Wspierane systemy operacyjne:   * Microsoft Windows Server 2016 oraz 2012 R2 * VMWare vSphere 6.5 oraz 6 * Suse Linux Enterprise Server 12 * Red Hat Enterprise Linux 6 oraz 7 | TAK |  | | |
|  | Gwarancja:   * 5 lat gwarancji producenta serwera w trybie on-site z gwarantowanym czasem usunięcia usterki do końca następnego dnia od zgłoszenia. * Uszkodzone dyski twarde nie muszą być zwracane organizacji serwisowej * Zgłaszanie usterek i awarii sprzętowych poprzez automatyczne założenie zgłoszenia w systemie helpdesk/servicedesk producenta sprzętu; * Firma serwisująca musi posiadać ISO 9001:2000 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 w trybie onsite z gwarantowanym skutecznym zakończeniem naprawy serwera najpóźniej w następnym dniu roboczym od zgłoszenia usterki (podać koszt na dzień składania oferty); | TAK |  | | |
|  | 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 – wymaganie oświadczenie wykonawcy lub producenta; | TAK |  | | |
|  | Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w UE – wymagane oświadczenie wykonawcy lub producenta; | TAK |  | | |
|  | 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; | TAK |  | | |
|  | 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; | TAK |  | | |
|  | Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera; | TAK |  | | |
|  | 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. | Warunek opcjonalny, dodatkowo punktowany:  - spełnione (TAK): 1pkt  - niespełnione (NIE): 0pkt |  | | |
|  | Sprzęt wyprodukowany na terenie Unii Europejskiej | Warunek opcjonalny, dodatkowo punktowany:  - spełnione (TAK): 1pkt  - niespełnione (NIE): 0pkt |  | | |
| 1. **Macierz dyskowa – 2 sztuki** | | | | | |
|  | System musi być dostarczony ze wszystkimi komponentami do instalacji w standardowej szafie rack 19” z zajętością maks. 4U 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 1U lub 2U pozwalająca umieścić do 24 dysków 2,5” typu hotplug dla dysków NL-SAS SAS i SSD oraz w rozmiarze 2U/3U dla 12 dysków 3,5” typu hotplug SAS, NL-SAS,SSD oraz 4U/5U gęstego upakowania dla 60 dysków typu hotplug SAS, NL-SAS,SSD; Wymaga się aby macierz umożliwiała jednoczesne podłączenie i użycie dowolnego rodzaju i kombinacji wyżej wymienionych półek dyskowych (tj. 12 HDD 3,5” + 24 HDD 2,5 + 60 HDD gęstego upakowania) | TAK |  | | |
|  | Pojemność dostarczonej macierzy (zainstalowane dyski):   * 7 szt. 1,2 TB SAS 12G 10 000 obr./min. * 9 szt. 8 TB NL-SAS 12G | TAK |  | | |
|  | Kontrolery macierzy muszą obsługiwać tryb pracy w układzie active-active lub mesh-active, macierz musi być dostarczona z zainstalowanymi minimum 2 kontrolerami; | TAK |  | | |
|  | Każdy z kontrolerów macierzy musi posiadać po minimum 16 GB pamięci podręcznej Cache – kontrolery muszą obsługiwać między sobą mechanizm lustrzanej kopii danych (cache mirror) przeznaczonych do zapisu; | TAK |  | | |
|  | 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 | TAK |  | | |
|  | W przypadku awarii zasilania dane nie zapisane na dyski, przechowywane w pamięci podręcznej Cache dla zapisów muszą być zabezpieczone metodą trwałego zapisu na dysk. | TAK |  | | |
|  | Kontrolery muszą posiadać możliwość ich wymiany bez konieczności wyłączania zasilania całego urządzenia; | TAK |  | | |
|  | Macierz musi obsługiwać wymianę kontrolera RAID bez utraty danych zapisanych na dyskach. | TAK |  | | |
|  | 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. | TAK |  | | |
|  | Kontrolery macierzy muszą być oparte o procesor wykonany w technologii wielordzeniowej z minimum 4 rdzeniami | TAK |  | | |
|  | Dla obsługi operacji blokowych I/O w sieci IP/FC SAN kontrolery macierzy muszą wspierać protokoły transmisji: FC 16Gb/s , iSCSI 10Gb/s | TAK |  | | |
|  | Kontrolery macierzy muszą obsługiwać do 130 grup dyskowych w całym rozwiązaniu, bez konieczności wymiany dostarczonych kontrolerów | TAK |  | | |
|  | Oferowana macierz musi mieć wyprowadzone 2 porty FC 16Gb/s do dołączenia serwerów bezpośrednio lub do dołączenia do sieci SAN, na każdy kontroler RAID. | TAK |  | | |
|  | Macierz musi umożliwiać wymianę portów do transmisji danych obsługujących protokoły: iSCSI 10Gb/s, SAS 12Gb/s, FC 8Gb/s, iSCSI 1Gb/s | TAK |  | | |
|  | 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. | TAK |  | | |
|  | Macierz musi umożliwiać dołożenie dodatkowych portów do transmisji danych obsługujących protokoły: iSCSI 10Gb/s, SAS 12Gb/s, FC 8Gb/s, iSCSI 1Gb/s, | TAK |  | | |
|  | 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. | TAK |  | | |
|  | Kontrolery macierzy obsługują funkcjonalność kompresji danych. | TAK |  | | |
|  | Obsługiwane poziomy RAID:   * Macierz musi zapewniać poziom zabezpieczenia danych na dyskach definiowany poziomami RAID:   + Raid-0   + Raid-1   + Raid-10   + Raid-5   + Raid-50   + Raid-6 | TAK |  | | |
|  | Oferowana macierz musi wspierać dyski hot-plug:   * + dyski elektroniczne SSD i mechaniczne HDD z interfejsami SAS12Gb/s   + dyski mechaniczne HDD o prędkości obrotowej 7,2 krpm, 10 krpm oraz 15k rpm, | TAK |  | | |
|  | Macierz musi obsługiwać mieszaną konfigurację dysków hot-plug SSD i HDD w rozmiarach 2,5” i 3,5” zainstalowanych w dowolnym module rozwiązania; | TAK |  | | |
|  | Wszystkie dyski wspierane przez oferowany model macierzy muszą być wykonane w technologii hot-plug i posiadać podwójne porty SAS obsługujące tryb pracy full-duplex | TAK |  | | |
|  | Macierz musi obsługiwać min. 60 dysków SAS SSD w całym rozwiązaniu, | TAK |  | | |
|  | 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 | TAK |  | | |
|  | 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) | TAK |  | | |
|  | Macierz musi pozwalać na zaszyfrowanie danych zapisanych na dostarczonych dyskach SSD SAS i HDD SAS minimum kluczem AES256-bit – jeżeli w tym celu niezbędne jest zakupienie dodatkowych licencji bądź komponentów sprzętowych to należy je dostarczyć wraz z macierzą | TAK |  | | |
|  | Macierz musi być wyposażona w system kopii migawkowych umożliwiających wykonanie minimum 2048 kopii migawkowych | TAK |  | | |
|  | Macierz musi umożliwiać zdefiniowanie min. 8000 woluminów (LUN) | TAK |  | | |
|  | Macierz powinna umożliwiać podłączenie logiczne z serwerami i stacjami poprzez min. 1024 ścieżek logicznych FC | TAK |  | | |
|  | 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 | TAK |  | | |
|  | 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 | TAK |  | | |
|  | Macierz musi posiadać wsparcie dla systemów operacyjnych : Microsoft Windows Server 2012R2, 2016, SuSE Linux Enterprise Server, Red Hat Linux Enterprise Server, HP-UNIX, IBM AIX, SUN Solaris, Vmware Vsphere; | TAK |  | | |
|  | 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. | TAK |  | | |
|  | 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. | TAK |  | | |
|  | 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 | TAK |  | | |
|  | Macierz musi obsługiwać mechanizm ochrony priorytetów obsługi wybranych zasobów – za taki mechanizm uznaje się funkcję typu ‘cache partitioning’ lub ‘storage partitioning’. | TAK |  | | |
|  | Macierz musi obsługiwać adresację IP v.4 i IP v.6 | TAK |  | | |
|  | 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 | TAK |  | | |
|  | 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. | TAK |  | | |
|  | 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 wyposażony w 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 | TAK |  | | |
|  | 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 | TAK |  | | |
|  | 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 | TAK |  | | |
|  | Macierz wspiera 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) – jeżeli funkcjonalność jest licencjonowana, wymagane jest dostarczenie odpowiedniej licencji. | TAK |  | | |
|  | Oprogramowanie do zarządzania musi być zintegrowane z systemem operacyjnym systemu pamięci masowej | TAK |  | | |
|  | Komunikacja z wbudowanym oprogramowaniem zarządzającym macierzą musi być możliwa w trybie graficznym np. poprzez przeglądarkę WWW oraz w trybie tekstowym. | TAK |  | | |
|  | 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 | TAK |  | | |
|  | 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 | TAK |  | | |
|  | Całe rozwiązanie musi być objęte minimum 60 miesięcznym okresem gwarancji z naprawą 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. | TAK |  | | |
|  | Uszkodzone dyski twarde nie podlegają zwrotowi organizacji serwisowej; | TAK |  | | |
|  | Serwis gwarancyjny musi obejmować dostęp do poprawek i nowych wersji oprogramowania wbudowanego, które są elementem zamówienia. | TAK |  | | |
|  | 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. | TAK |  | | |
|  | 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); | TAK |  | | |
|  | System musi zapewniać możliwość samodzielnego i automatycznego powiadamiania producenta i administratorów Zamawiającego o usterkach za pomocą wiadomości wysyłanych poprzez szyfrowany protokół. | TAK |  | | |
|  | Macierz musi pochodzić z oficjalnego kanału sprzedaży producenta w UE. Nie dopuszcza się użycia macierzy odnawianych, demonstracyjnych lub powystawowych | TAK |  | | |
|  | Urządzenie musi być wykonane zgodnie z europejskimi dyrektywami RoHS i WEEE stanowiącymi o unikaniu i ograniczaniu stosowania substancji szkodliwych dla zdrowia | TAK |  | | |
|  | Kontrolery macierzy obsługują funkcjonalność deduplikacji danych w trybie in-line | Warunek opcjonalny, dodatkowo punktowany:  - spełnione (TAK): 2pkt  - możliwość rozbudowy (OPCJA): 1pkt  - niespełnione (NIE): 0pkt |  | | |
|  | Każdy z kontrolerów macierzy posiada po minimum 32 GB pamięci podręcznej Cache | Warunek opcjonalny, dodatkowo punktowany:  - spełnione (TAK): 2pkt  - możliwość rozbudowy (OPCJA): 1pkt  - niespełnione (NIE): 0pkt |  | | |
|  | 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. | Warunek opcjonalny, dodatkowo punktowany:  - spełnione (TAK):2pkt  - możliwość rozbudowy (OPCJA): 1pkt  - niespełnione (NIE): 0pkt |  | | |
|  | Sprzęt wyprodukowany na terenie Unii Europejskiej | Warunek opcjonalny, dodatkowo punktowany:  - spełnione (TAK): 1pkt  - niespełnione (NIE): 0pkt |  | | |
| 1. **Szafa RACK – 1 sztuka** | | | | | |
|  | 42U pojemności użytecznej do instalacji urządzeń w pozycji poziomej | TAK |  | | |
|  | całkowita wysokość maksymalna 2000mm | TAK |  | | |
|  | całkowita głębokość maksymalna 1200mm | TAK |  | | |
|  | całkowita szerokość maksymalna 600mm | TAK |  | | |
|  | klasa ochrony IP20 | TAK |  | | |
|  | wyposażona w przednie drzwi perforowane, zamykane na zamek z kluczem, jednoskrzydłowe, możliwość montażu lewa/prawa strona, możliwość zdjęcia bez użycia narzędzi | TAK |  | | |
|  | wyposażona w tylne drzwi perforowane, dwuskrzydłowe dla ograniczenia przestrzeni serwisowej, zamykane na zamek z kluczem wspólny z zamkiem przednim, możliwość zdjęcia bez użycia narzędzi | TAK |  | | |
|  | wyposażona w zdejmowane panele boczne zabezpieczone w taki sam sposób jak drzwi | TAK |  | | |
|  | przystosowana do chłodzenia horyzontalnego przód-tył, pasywna – bez wentylatorów wspomagających | TAK |  | | |
|  | opcjonalne fabryczne zabezpieczenie teleskopowe przeciwko wywróceniu szafy do przodu (tzw. tilt protection) | TAK |  | | |
|  | udźwig gwarantowany szafy co najmniej 1000KG | TAK |  | | |
|  | wszystkie wolne „U” zaślepione zaślepkami w kolorze szafy | TAK |  | | |
|  | przystosowana do poprawnej instalacji dostarczonych serwerów rack wraz z ich fabrycznymi prowadnicami przewodów | TAK |  | | |
|  | zainstalowane 2 listwy zasilające 3 fazowe 3x8 gniazd | TAK |  | | |
|  | 5 lat gwarancji w miejscu użytkowania | TAK |  | | |
|  | Certyfikaty CE, EN, RoHS, WEEE | TAK |  | | |
| 1. **Switch FC – 4 sztuki** | | | | | |
|  | Wysokość przełącznika 1U w systemie montażu w szafie typu rack 19” wraz z kompletem szyn mocujących | TAK |  | | |
|  | 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 | TAK |  | | |
|  | 8 aktywnych portów | TAK |  | | |
|  | Zainstalowane moduły optyczne 8 szt. SFP 16Gbit/s, Short Wave Length (SWL), Multi Mode Fibre (MMF) | TAK |  | | |
|  | Obsługa trybów pracy portów FC: D\_port, F\_port, E\_port, M-Port | TAK |  | | |
|  | Obsługa funkcji POD (Ports on Demand) przydziału licencji dla aktywnych portów FC | TAK |  | | |
|  | Możliwość aktualizacji firmware’u switcha | TAK |  | | |
|  | Aktywne funkcje: Active Gateway, Webtools, Advanced Zoning, FullFabric (z obsługą do min. 128 przełączników FC) | TAK |  | | |
|  | Możliwość obsługi funkcjonalności (przez zakupienie odpowiednich licencji): Trunking, Extended Fabric, Fabric Vision | TAK |  | | |
|  | 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 | TAK |  | | |
|  | Sygnalizacja aktywnych i podłączonych portów na panelu przednim urządzenia | TAK |  | | |
|  | Zarządzanie poprzez przeglądarkę WWW z obsługą połączeń szyfrowanych 128-bit SSL oraz poprzez usługę SSH | TAK |  | | |
|  | Wsparcie dla protokołu SNMP v.3 | TAK |  | | |
|  | Osiem przewodów OM4 LC-LC o długości 5m | TAK |  | | |
|  | Gwarancja: 5 lat w miejscu instalacji, z gwarantowanym czasem naprawy do końca następnego dnia roboczego od zgłoszenia usterki | TAK |  | | |
| 1. **UPS – 4 sztuki** | | | | | |
|  | elementy umożliwiające montaż w szafie RACK | TAK |  | | |
|  | zajętość w szafie RACK nie więcej niż 3U | TAK |  | | |
|  | moc pozorna 5kVA | TAK |  | | |
|  | moc rzeczywista 4,5 kW | TAK |  | | |
|  | online (VFI) | TAK |  | | |
|  | podtrzymanie 4 minuty przy 100% obciążeniu | TAK |  | | |
|  | podtrzymanie 11,5 minuty przy 50% obciążeniu | TAK |  | | |
|  | 6x IEC 320 C13 (10A) | TAK |  | | |
|  | 4x IEC 320 C19 (16A) | TAK |  | | |
|  | 1x RJ45 | TAK |  | | |
|  | aplikacja do automatycznego zamykania wspieranych systemów operacyjnych w przypadku braku zasilania | TAK |  | | |
|  | wspierane i certyfikowane systemy operacyjne:   * Microsoft® Windows Server® 2012 R2, * Microsoft® Windows Server® 2016, * SUSE Linux Enterprise Server, * Red Hat Enterprise Linux, * VMware Infrastructure | TAK |  | | |
|  | zarządzanie przez SNMP | TAK |  | | |
|  | możliwość podłączenia dodatkowych modułów bateryjnych wydłużających czas potrzymania | TAK |  | | |
|  | automatyczny wewnętrzny bypass | TAK |  | | |
|  | bezprzerwowa wymiana baterii | TAK |  | | |
|  | wyświetlacz LCD na froncie urządzenia, umożliwiający zarządzanie i monitoring urządzenia | TAK |  | | |
|  | certyfikaty: CE, CB | TAK |  | | |
|  | 3 lata gwarancji door-to-door | TAK |  | | |
| 1. **System do wirtualizacji – 1 sztuka** | | | | | |
|  | Licencja dla 3 serwerów fizycznych posiadających po 2 procesory każdy z gwarancją utrzymania aktualnej wersji przez okres min. 5 lat | TAK | |  | |
|  | Warstwa wirtualizacji musi być zainstalowana bezpośrednio na sprzęcie fizycznym bez dodatkowych pośredniczących systemów operacyjnych | TAK | |  | |
|  | Rozwiązanie musi zapewnić możliwość obsługi wielu instancji systemów operacyjnych na jednym serwerze fizycznym i powinno się charakteryzować maksymalnym możliwym stopniem konsolidacji sprzętowej. | TAK | |  | |
|  | Pojedynczy klaster może się skalować do 64 fizycznych hostów (serwerów) z zainstalowaną warstwą wirtualizacji. | TAK | |  | |
|  | Oprogramowanie do wirtualizacji zainstalowane na serwerze fizycznym potrafi obsłużyć i wykorzystać procesory fizyczne wyposażone w 480 logicznych wątków oraz do 6TB pamięci fizycznej RAM. | TAK | |  | |
|  | Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych 1-128 procesorowych. | TAK | |  | |
|  | Oprogramowanie do wirtualizacji musi zapewniać możliwość stworzenia dysku maszyny wirtualnej o wielkości do 62 TB. | TAK | |  | |
|  | Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością przydzielenia do 4 TB pamięci operacyjnej RAM. | TAK | |  | |
|  | Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 1-10 wirtualnych kart sieciowych. | TAK | |  | |
|  | Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 32 porty szeregowe. | TAK | |  | |
|  | Rozwiązanie musi umożliwiać łatwą i szybką rozbudowę infrastruktury o nowe usługi bez spadku wydajności i dostępności pozostałych wybranych usług. | TAK | |  | |
|  | Rozwiązanie powinno w możliwie największym stopniu być niezależne od producenta platformy sprzętowej. | TAK | |  | |
|  | Polityka licencjonowania musi umożliwiać przenoszenie licencji na oprogramowanie do wirtualizacji pomiędzy serwerami. | TAK | |  | |
|  | Rozwiązanie musi wspierać następujące systemy operacyjne: MS-DOS 6.22, Windows 3.1, Windows 95, Windows 98, Windows XP, Windows Vista , Windows NT 4.0, Windows 2000, Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows 7, Windows 8, SLES 11, SLES 10, SLES 9, SLES 8, RHEL 6, RHEL 5, RHEL 4, RHEL 3, Solaris 11 ,Solaris 10, Solaris 9, Solaris 8, OS/2 Warp 4.0, NetWare 6.5, NetWare 6, NetWare 5, OEL 4, OEL 5, Debian, CentOS, FreeBSD, Asianux, Mandriva, Ubuntu 14, Ubuntu 12, SCO OpenServer, SCO Unixware, Mac OS X. | TAK | |  | |
|  | Rozwiązanie musi umożliwiać przydzielenie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera w celu osiągnięcia maksymalnego współczynnika konsolidacji. | TAK | |  | |
|  | Rozwiązanie musi umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie zarezerwowane na dyskach lokalnych serwera lub na macierzy. | TAK | |  | |
|  | Rozwiązanie powinno posiadać centralną konsolę graficzną do zarządzania maszynami wirtualnymi i do konfigurowania innych funkcjonalności. Centralna konsola graficzna powinna mieć możliwość działania zarówno, jako aplikacja na maszynie fizycznej lub wirtualnej, jak i jako gotowa, wstępnie skonfigurowana maszyna wirtualna tzw. virtual appliance. | TAK | |  | |
|  | Rozwiązanie musi zapewnić możliwość bieżącego monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej (np. wykorzystanie procesorów, pamięci RAM, wykorzystanie przestrzeni na dyskach/wolumenach) oraz przechowywać i wyświetlać dane maksymalnie sprzed roku. | TAK | |  | |
|  | Oprogramowanie do wirtualizacji powinno zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych (tzw. snapshot) na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy. | TAK | |  | |
|  | Oprogramowanie do wirtualizacji musi zapewnić możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi. | TAK | |  | |
|  | Oprogramowanie do wirtualizacji oraz oprogramowanie zarządzające musi posiadać możliwość integracji z usługami katalogowymi Microsoft Active Directory. | TAK | |  | |
|  | Rozwiązanie musi zapewniać mechanizm bezpiecznego uaktualniania warstwy wirtualizacyjnej (hosta, maszyny wirtualnej) bez potrzeby wyłączania wirtualnych maszyn. | TAK | |  | |
|  | System musi posiadać funkcjonalność wirtualnego przełącznika (virtual switch) umożliwiającego tworzenie sieci wirtualnej w obszarze hosta i pozwalającego połączyć maszyny wirtualne w obszarze jednego hosta, a także na zewnątrz sieci fizycznej. Pojedynczy przełącznik wirtualny powinien mieć możliwość konfiguracji do 4000 portów. | TAK | |  | |
|  | Pojedynczy wirtualny przełącznik musi posiadać możliwość przyłączania do niego dwóch i więcej fizycznych kart sieciowych, aby zapewnić bezpieczeństwo połączenia ethernetowego w razie awarii karty sieciowej. | TAK | |  | |
|  | Wirtualne przełączniki musza obsługiwać wirtualne sieci lokalne (VLAN). | TAK | |  | |
|  | Rozwiązanie musi zapewnić wbudowany, bezpieczny mechanizm do automatycznego tworzenia kopii zapasowych, odtwarzania wskazanych maszyn wirtualnych. Mechanizm ten musi umożliwiać również odtwarzanie pojedynczych plików z kopii zapasowej oraz zapewnia stosowanie deduplikacji dla kopii zapasowych. Mechanizm zapewnia możliwość wykonywania spójnych kopii zapasowych serwerów aplikacyjnych (Microsoft SQL Server, Microsoft Exchange Server, Microsoft SharePoint Server) oraz replikację kopii zapasowych. | TAK | |  | |
|  | Rozwiązanie musi zapewniać mechanizm replikacji wskazanych maszyn wirtualnych w obrębie klastra serwerów fizycznych. | TAK | |  | |
|  | Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy serwerami fizycznymi. Mechanizmpowinien umożliwiać 4 lub więcej takich procesów przenoszenia jednocześnie. | TAK | |  | |
|  | Musi zostać zapewniona odpowiednia redundancja i taki mechanizm (wysokiej dostępności HA) , aby w przypadku awarii lub niedostępności serwera fizycznego wybrane przez administratora i uruchomione nim wirtualne maszyny zostały uruchomione na innych serwerach z zainstalowanym oprogramowaniem wirtualizacyjnym. | TAK | |  | |
| 1. **System bazodanowy – 1 sztuka** | | | | | |
|  | Licencje na motor bazy danych typu Oracle Standard Edition lub kompatybilny umożliwiająca uruchomienie na 2 fizycznych procesorów klasy Intel x86 (po 1 w 2 serwerach spiętych w klaster). | TAK |  | | |
|  | Licencja dożywotnia | TAK |  | | |
|  | Usługa asysty technicznej i konserwacji producenta na okres minimum 60 miesięcy | TAK |  | | |
|  | Dostępność oprogramowania na współczesne 64-bitowe platformy Unix (HP-UX dla Itanium, Solaris dla procesorów SPARC/x86-64, IBM AIX), Intel Linux 64-bit, MS Windows 64-bit. Identyczna funkcjonalność serwera bazy danych na ww. platformach. | TAK |  | | |
|  | Niezależność platformy systemowej dla oprogramowania klienckiego / serwera aplikacyjnego od platformy systemowej bazy danych. | TAK |  | | |
|  | Możliwość przeniesienia (migracji) struktur bazy danych i danych pomiędzy ww. platformami bez konieczności rekompilacji aplikacji bądź migracji środowiska aplikacyjnego. | TAK |  | | |
|  | Przetwarzanie transakcyjne wg reguł ACID (Atomicity, Consistency, Independency, Durability) z zachowaniem spójności i maksymalnego możliwego stopnia współbieżności. Mechanizm izolowania transakcji powinien pozwalać na spójny odczyt modyfikowanego obszaru danych bez wprowadzania blokad, z kolei spójny odczyt nie powinien blokować możliwości wykonywania zmian. Oznacza to, że modyfikowanie wierszy nie może blokować ich odczytu, z kolei odczyt wierszy nie może ich blokować do celów modyfikacji. Jednocześnie spójność odczytu musi gwarantować uzyskanie rezultatów zapytań odzwierciedlających stan danych z chwili jego rozpoczęcia, niezależnie od modyfikacji przeglądanego zbioru danych. | TAK |  | | |
|  | Wsparcie dla wielu ustawień narodowych i wielu zestawów znaków (włącznie z Unicode). | TAK |  | | |
|  | Możliwość migracji 8-bitowego zestawu znaków bazy danych (np MS Windows CP 1252, ISO 8859-2) do Unicode. | TAK |  | | |
|  | Skalowanie rozwiązań opartych o architekturę trójwarstwową: możliwość uruchomienia wielu sesji bazy danych przy wykorzystaniu jednego połączenia z serwera aplikacyjnego do serwera bazy danych. | TAK |  | | |
|  | Brak formalnych ograniczeń na liczbę tabel i indeksów w bazie danych oraz na ich rozmiar (liczbę wierszy). | TAK |  | | |
|  | Wsparcie dla procedur i funkcji składowanych w bazie danych. Język programowania powinien być językiem proceduralnym, blokowym (umożliwiającym deklarowanie zmiennych wewnątrz bloku), oraz wspierającym obsługę wyjątków. W przypadku, gdy wyjątek nie ma zadeklarowanej obsługi wewnątrz bloku, w razie jego wystąpienia wyjątek powinien być automatycznie propagowany do bloku nadrzędnego bądź wywołującej go jednostki programu. | TAK |  | | |
|  | Możliwość kompilacji procedur składowanych w bazie danych do postaci kodu binarnego. | TAK |  | | |
|  | Możliwość deklarowania wyzwalaczy (triggerów) na poziomie instrukcji DML (INSERT, UPDATE, DELETE) wykonywanej na tabeli, poziomie każdego wiersza modyfikowanego przez instrukcję DML oraz na poziomie zdarzeń bazy danych (np. próba wykonania instrukcji DDL, start serwera, stop serwera, próba zalogowania użytkownika, wystąpienie specyficznego błędu w serwerze). Ponadto mechanizm wyzwalaczy powinien umożliwiać oprogramowanie obsługi instrukcji DML (INSERT, UPDATE, DELETE) wykonywanych na tzw. niemodyfikowalnych widokach (views). | TAK |  | | |
|  | W przypadku, gdy w wyzwalaczu na poziomie instrukcji DML wystąpi błąd zgłoszony przez motor bazy danych bądź ustawiony wyjątek w kodzie wyzwalacza, wykonywana instrukcja DML musi być automatycznie wycofana przez serwer bazy danych, zaś stan transakcji po wycofaniu musi odzwierciedlać chwilę przed rozpoczęciem instrukcji w której wystąpił ww. błąd lub wyjątek. | TAK |  | | |
|  | Baza danych powinna umożliwiać na wymuszanie złożoności hasła użytkownika, czasu życia hasła, sprawdzanie historii haseł, blokowanie konta przez administratora bądź w przypadku przekroczenia limitu nieudanych logowań. | TAK |  | | |
|  | Przywileje użytkowników bazy danych powinny być określane za pomocą przywilejów systemowych (np. prawo do podłączenia się do bazy danych - czyli utworzenia sesji, prawo do tworzenia tabel itd.) oraz przywilejów dostępu do obiektów aplikacyjnych (np. odczytu / modyfikacji tabeli, wykonania procedury). Baza danych powinna umożliwiać nadawanie ww. przywilejów za pośrednictwem mechanizmu grup użytkowników / ról bazodanowych. W danej chwili użytkownik może mieć aktywny dowolny podzbiór nadanych ról bazodanowych. | TAK |  | | |
|  | Możliwość wykonywania i katalogowania kopii bezpieczeństwa bezpośrednio przez serwer bazy danych. Możliwość zautomatyzowanego usuwania zbędnych kopii bezpieczeństwa przy zachowaniu odpowiedniej liczby kopii nadmiarowych - stosownie do założonej polityki nadmiarowości backup'ów. Możliwość integracji z powszechnie stosowanymi systemami backupu (Legato, Veritas, Tivoli, Data Protector itd). Wykonywanie kopii bezpieczeństwa powinno być możliwe w trybie offline oraz w trybie online. | TAK |  | | |
|  | Możliwość wykonywania kopii bezpieczeństwa w trybie online (hot backup). | TAK |  | | |
|  | Odtwarzanie powinno umożliwiać odzyskanie stanu danych z chwili wystąpienia awarii bądź cofnąć stan bazy danych do punktu w czasie. W przypadku odtwarzania do stanu z chwili wystąpienia awarii odtwarzaniu może podlegać cała baza danych bądź pojedyncze pliki danych. | TAK |  | | |
|  | W przypadku, gdy odtwarzaniu podlegają pojedyncze pliki bazy danych, pozostałe pliki baz danych mogą być dostępne dla użytkowników. | TAK |  | | |
|  | Wsparcie dla typu danych DICOM obsługiwanego wewnętrznie przez serwer bazy danych. | TAK |  | | |
|  | Możliwość zakładania w tabelach kolumn typu obsługującego standard DICOM. | TAK |  | | |
|  | Możliwość przeszukiwania zakładania indeksów na grupie atrybutów metadanych składowanych w kolumnach przechowujących dane w formacie DICOM. | TAK |  | | |
|  | Możliwość przeszukiwania metadanych  \* wszystkich bądź niektórych atrybutów,  \* możliwość zakładania indeksów na wybranych atrybutach,  \* możliwość wyszukiwania pełnotekstowego,  \* możliwość nawigacji zgodnej z hierarchią atrybutów. | TAK |  | | |
|  | Składowanie metadanych DICOM i treści DICOM odbywa się wewnątrz bazy danych. | TAK |  | | |
|  | Operowanie na danych DICOM za pomocą konstrukcji języka SQL, procedur składowanych, dostęp za pomocą Java API. | TAK |  | | |
|  | Wbudowane mechanizmy konwersji treści DICOM do formatów JPEG, GIF, MPEG, AVI. | TAK |  | | |
|  | Możliwość budowy klasta typu active-active opartego o maksymalnie 2 węzły (maksymalnie 2 x 1 CPU) | TAK |  | | |
|  | Możliwość zwiększenia przepustowości bazy danych poprzez uruchomienie dodatkowych serwerów obsługujących tą samą bazę danych (w klastrze). | TAK |  | | |
|  | Zwiększenie bądź zmniejszenie liczby serwerów obsługujących klastrową bazę danych nie może powodować konieczności reorganizacji fizycznej (zmiana organizacji plików danych) oraz logicznej struktury baz danych (tabel / indeksów). | TAK |  | | |
|  | Unieruchomienie jednego z serwerów bazy danych nie może powodować braku dostępu do jakiejkolwiek części danych – baza danych musi być nadal dostępna za pośrednictwem funkcjonujących dalej serwerów | TAK |  | | |
|  | Możliwość kontynuacji pracy użytkowników podłączonych do serwera klastrowej bazy danych, który uległ awarii. Powinna istnieć możliwość przeniesienia sesji na inny serwer oraz automatycznego powiadomienia aplikacji o wykonaniu przełączenia. | TAK |  | | |
|  | Obraz bazy danych (metadane, obiekty bazy danych, stan danych) w klastrowej bazie danych musi być niezależny od serwera do którego zostało nawiązane połączenie. | TAK |  | | |
| 1. **Oprogramowanie antywirusowe – 1 sztuka** | | | | | |
|  | Licencja na 180 stanowisk na okres 36 miesięcy (3 lata) | TAK |  | | |
|  | Pełne wsparcie dla systemu Windows XP SP3/Vista/Windows 7/Windows8/Windows 8.1/Windows 8.1 Update/10 | TAK |  | | |
|  | Wsparcie dla 32- i 64-bitowej wersji systemu Windows. | TAK |  | | |
|  | Wersja programu dla stacji roboczych Windows dostępna zarówno w języku polskim jak i angielskim. | TAK |  | | |
|  | Pomoc w programie (help) i dokumentacja do programu dostępna w języku polskim. | TAK |  | | |
|  | Skuteczność programu potwierdzona nagrodami VB100 i AV-comparatives | TAK |  | | |
| **Ochrona antywirusowa i antyspyware** | | | | | |
|  | Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami. | TAK |  | | |
|  | Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp. | TAK |  | | |
|  | Wbudowana technologia do ochrony przed rootkitami. | TAK |  | | |
|  | Wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji. | TAK |  | | |
|  | Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. | TAK |  | | |
|  | Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu. | TAK |  | | |
|  | System ma oferować administratorowi możliwość definiowania zadań w harmonogramie w taki sposób, aby zadanie przed wykonaniem sprawdzało czy komputer pracuje na zasilaniu bateryjnym i jeśli tak – nie wykonywało danego zadania. | TAK |  | | |
|  | Możliwość utworzenia wielu różnych zadań skanowania według harmonogramu (w tym: co godzinę, po zalogowaniu i po uruchomieniu komputera). Każde zadanie ma mieć możliwość uruchomienia z innymi ustawieniami (czyli metody skanowania, obiekty skanowania, czynności, rozszerzenia przeznaczone do skanowania, priorytet skanowania). | TAK |  | | |
|  | Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym. | TAK |  | | |
|  | Możliwość określania poziomu obciążenia procesora (CPU) podczas skanowania „na żądanie” i według harmonogramu. | TAK |  | | |
|  | Możliwość skanowania dysków sieciowych i dysków przenośnych. | TAK |  | | |
|  | Skanowanie plików spakowanych i skompresowanych. | TAK |  | | |
|  | Możliwość umieszczenia na liście wyłączeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach. | TAK |  | | |
|  | Wykluczenie ze skanowania musi odbywać się nie tylko po nazwie pliku ale również ma być możliwe użycie symbolu wieloznacznego „\*” zastępującego dowolne znaki w ścieżce. | TAK |  | | |
|  | Administrator ma możliwość dodania wykluczenia po tzw. HASH’u zagrożenia, wskazującego bezpośrednio na określoną infekcję a nie konkretny plik. | TAK |  | | |
|  | Możliwość automatycznego wyłączenia komputera po zakończonym skanowaniu. | TAK |  | | |
|  | Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji programu. | TAK |  | | |
|  | Użytkownik musi posiadać możliwość tymczasowego wyłączenia ochrony na czas co najmniej 10 min lub do ponownego uruchomienia komputera. | TAK |  | | |
|  | W momencie tymczasowego wyłączenia ochrony antywirusowej użytkownik musi być poinformowany o takim fakcie odpowiednim powiadomieniem i informacją w interfejsie aplikacji. | TAK |  | | |
|  | Ponowne włączenie ochrony antywirusowej nie może wymagać od użytkownika ponownego uruchomienia komputera. | TAK |  | | |
|  | Możliwość przeniesienia zainfekowanych plików i załączników poczty w bezpieczny obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej. | TAK |  | | |
|  | Wbudowany konektor dla programów MS Outlook, Outlook Express, Windows Mail i Windows Live Mail (funkcje programu dostępne są bezpośrednio z menu programu pocztowego). | TAK |  | | |
|  | Skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu MS Outlook, Outlook Express, Windows Mail i Windows Live Mail. | TAK |  | | |
|  | Skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP "w locie" (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego). | TAK |  | | |
|  | Automatyczna integracja skanera POP3 i IMAP z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji. | TAK |  | | |
|  | Możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail. | TAK |  | | |
|  | Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie. | TAK |  | | |
|  | Blokowanie możliwości przeglądania wybranych stron internetowych. Listę blokowanych stron internetowych określa administrator. Program musi umożliwić blokowanie danej strony internetowej po podaniu na liście całej nazwy strony lub tylko wybranego słowa występującego w nazwie strony. | TAK |  | | |
|  | Możliwość zdefiniowania blokady wszystkich stron internetowych z wyjątkiem listy stron ustalonej przez administratora. | TAK |  | | |
|  | Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji. | TAK |  | | |
|  | Program ma umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS. | TAK |  | | |
|  | Program ma zapewniać skanowanie ruchu HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe. | TAK |  | | |
|  | Możliwość zgłoszenia witryny z podejrzeniem phishingu z poziomu graficznego interfejsu użytkownika w celu analizy przez laboratorium producenta. | TAK |  | | |
|  | Administrator ma mieć możliwość zdefiniowania portów TCP, na których aplikacja będzie realizowała proces skanowania ruchu szyfrowanego. | TAK |  | | |
|  | Program musi posiadać funkcjonalność która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika. | TAK |  | | |
|  | Procesy zweryfikowane jako bezpieczne mają być pomijane podczas procesu skanowania na żądanie oraz przez moduły ochrony w czasie rzeczywistym. | TAK |  | | |
|  | Użytkownik musi posiadać możliwość przesłania pliku celem zweryfikowania jego reputacji bezpośrednio z poziomu menu kontekstowego. | TAK |  | | |
|  | W przypadku gdy stacja robocza nie będzie posiadała dostępu do sieci Internet ma odbywać się skanowanie wszystkich procesów również tych, które wcześniej zostały uznane za bezpieczne. | TAK |  | | |
|  | Wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne (heurystyka) i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji (zaawansowana heurystyka). Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej i/lub obu metod jednocześnie. | TAK |  | | |
|  | Możliwość automatycznego wysyłania nowych zagrożeń (wykrytych przez metody heurystyczne) do laboratoriów producenta bezpośrednio z programu (nie wymaga ingerencji użytkownika). Użytkownik musi mieć możliwość określenia rozszerzeń dla plików, które nie będą wysyłane automatycznie, oraz czy próbki zagrożeń mają być wysyłane w pełni automatycznie czy też po dodatkowym potwierdzeniu przez użytkownika. | TAK |  | | |
|  | Do wysłania próbki zagrożenia do laboratorium producenta aplikacja nie może wykorzystywać klienta pocztowego wykorzystywanego na komputerze użytkownika. | TAK |  | | |
|  | Możliwość wysyłania wraz z próbką komentarza dotyczącego nowego zagrożenia i adresu e-mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia. | TAK |  | | |
|  | Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe. | TAK |  | | |
|  | Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta. | TAK |  | | |
|  | Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby użytkownik siedzący przy komputerze przy próbie dostępu do konfiguracji był proszony o podanie hasła. | TAK |  | | |
|  | Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet, gdy posiada ona prawa lokalnego lub domenowego administratora. Przy próbie deinstalacji program musi pytać o hasło. | TAK |  | | |
|  | Hasło do zabezpieczenia konfiguracji programu oraz deinstalacji musi być takie samo. | TAK |  | | |
|  | Program ma mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku jakiejś aktualizacji – poinformować o tym użytkownika i administratora wraz z listą niezainstalowanych aktualizacji. | TAK |  | | |
|  | Program ma mieć możliwość definiowania typu aktualizacji systemowych o braku, których będzie informował użytkownika w tym przynajmniej: aktualizacje krytyczne, aktualizacje ważne, aktualizacje zwykle oraz aktualizacje o niskim priorytecie. Ma być możliwość dezaktywacji tego mechanizmu. | TAK |  | | |
|  | Po instalacji programu, użytkownik ma mieć możliwość przygotowania płyty CD, DVD lub pamięci USB, z której będzie w stanie uruchomić komputer w przypadku infekcji i przeskanować dysk w poszukiwaniu wirusów. | TAK |  | | |
|  | System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma umożliwiać pełną aktualizację baz sygnatur wirusów z Internetu lub z bazy zapisanej na dysku. | TAK |  | | |
|  | System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma pracować w trybie graficznym. | TAK |  | | |
|  | Program ma umożliwiać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM , urządzeń przenośnych oraz urządzeń dowolnego typu. | TAK |  | | |
|  | Funkcja blokowania nośników wymiennych bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ urządzenia, numer seryjny urządzenia, dostawcę urządzenia, model. | TAK |  | | |
|  | Program musi mieć możliwość utworzenia reguły na podstawie podłączonego urządzenia, dana funkcjonalność musi pozwalać na automatyczne wypełnienie właściwości urządzenia dla tworzonej reguły. | TAK |  | | |
|  | Program ma umożliwiać użytkownikowi nadanie uprawnień dla podłączanych urządzeń w tym co najmniej: dostęp w trybie do odczytu, pełen dostęp, ostrzeżenie brak dostępu do podłączanego urządzenia. | TAK |  | | |
|  | Program ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika. | TAK |  | | |
|  | W momencie podłączenia zewnętrznego nośnika aplikacja musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika. | TAK |  | | |
|  | Użytkownik ma posiadać możliwość takiej konfiguracji programu aby skanowanie całego nośnika odbywało się automatycznie lub za potwierdzeniem przez użytkownika | TAK |  | | |
|  | Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS). | TAK |  | | |
|  | Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów: | TAK |  | | |
|  | tryb automatyczny z regułami gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika, | TAK |  | | |
|  | tryb interaktywny, w którym to program pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie, | TAK |  | | |
|  | tryb oparty na regułach gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika, | TAK |  | | |
|  | tryb uczenia się, w którym program uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach. | TAK |  | | |
|  | Tryb inteligentny – w którym program będzie powiadamiał wyłącznie o szczególnie podejrzanych zdarzeniach. | TAK |  | | |
|  | Tworzenie reguł dla modułu HIPS musi odbywać się co najmniej w oparciu o: aplikacje źródłowe, pliki docelowe, aplikacje docelowe, elementy docelowe rejestru systemowego. | TAK |  | | |
|  | Użytkownik na etapie tworzenia reguł dla modułu HIPS musi posiadać możliwość wybrania jednej z trzech akcji: pytaj, blokuj, zezwól. | TAK |  | | |
|  | Oprogramowanie musi posiadać zaawansowany skaner pamięci. | TAK |  | | |
|  | Program musi być wyposażona w mechanizm ochrony przed exploitami w popularnych aplikacjach np. czytnikach PDF, aplikacjach JAVA itp. | TAK |  | | |
|  | Program ma być wyposażony we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której został zainstalowany w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesach i połączeniach. | TAK |  | | |
|  | Funkcja generująca taki log ma oferować przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla programu i mogą stanowić dla niego zagrożenie bezpieczeństwa. | TAK |  | | |
|  | Program ma oferować funkcję, która aktywnie monitoruje i skutecznie blokuje działania wszystkich plików programu, jego procesów, usług i wpisów w rejestrze przed próbą ich modyfikacji przez aplikacje trzecie. | TAK |  | | |
|  | Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń dostępna z Internetu. | TAK |  | | |
|  | Możliwość utworzenia kilku zadań aktualizacji (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z własnymi ustawieniami. | TAK |  | | |
|  | Możliwość określenia maksymalnego czasu ważności dla bazy danych sygnatur, po upływie czasu i braku aktualizacji program zgłosi posiadanie nieaktualnej bazy sygnatur. | TAK |  | | |
|  | Program musi posiadać funkcjonalność tworzenia lokalnego repozytorium aktualizacji. | TAK |  | | |
|  | Program musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji za pomocą wbudowanego w program serwera http | TAK |  | | |
|  | Program musi być wyposażona w funkcjonalność umożliwiającą tworzenie kopii wcześniejszych aktualizacji w celu ich późniejszego przywrócenia (rollback). | TAK |  | | |
|  | Program wyposażony tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne, zapora sieciowa). | TAK |  | | |
|  | Program ma być w pełni zgodny z technologią CISCO Network Access Control. | TAK |  | | |
|  | Aplikacja musi posiadać funkcjonalność, która automatycznie wykrywa aplikacje pracujące w trybie pełno ekranowym. | TAK |  | | |
|  | W momencie wykrycia trybu pełno ekranowego aplikacja ma wstrzymać wyświetlanie wszelkich powiadomień związanych ze swoją pracą oraz wstrzymać swoje zadania znajdujące się w harmonogramie zadań aplikacji. | TAK |  | | |
|  | Użytkownik ma mieć możliwość skonfigurowania programu tak aby automatycznie program włączał powiadomienia oraz zadania pomimo pracy w trybie pełnoekranowym po określonym przez użytkownika czasie. | TAK |  | | |
|  | Program ma być wyposażony w dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, pracy zapory osobistej, modułu antyspamowego, kontroli stron Internetowych i kontroli urządzeń, skanowania na żądanie i według harmonogramu, dokonanych aktualizacji baz wirusów i samego oprogramowania. | TAK |  | | |
|  | Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu. | TAK |  | | |
|  | Program musi posiadać możliwość utworzenia z poziomu interfejsu aplikacji dziennika diagnostycznego na potrzeby pomocy technicznej. | TAK |  | | |
|  | Program musi posiadać możliwość aktywacji poprzez podanie konta administratora licencji, podanie klucza licencyjnego oraz możliwość aktywacji programu offline. | TAK |  | | |
|  | Możliwość podejrzenia licencji za pomocą, której program został aktywowany. | TAK |  | | |
|  | W trakcie instalacji program ma umożliwiać wybór komponentów, które mają być instalowane. Instalator ma zezwalać na wybór co najmniej następujących modułów do instalacji: ochrona antywirusowa i antyspyware, kontrola dostępu do urządzeń, zapora osobista, ochrona poczty, ochrona protokołów, kontrola dostępu do stron internetowych, , Obsługa technologii Microsoft NAP. | TAK |  | | |
|  | W programie musi istnieć możliwość tymczasowego wstrzymania polityk wysłanych z poziomu serwera zdalnej administracji. | TAK |  | | |
|  | Wstrzymanie polityk ma umożliwić lokalną zmianę ustawień programu na stacji końcowej. | TAK |  | | |
|  | Funkcja wstrzymania polityki musi być realizowana tylko przez określony czas po którym automatycznie zostają przywrócone dotychczasowe ustawienia. | TAK |  | | |
|  | Administrator ma możliwość wstrzymania polityk na 10 min, 30 min, 1 godzinę i 4 godziny | TAK |  | | |
|  | Aktywacja funkcji wstrzymania polityki musi obsługiwać uwierzytelnienie za pomocą hasła lub konta użytkownika. | TAK |  | | |
|  | Program musi posiadać opcję automatycznego skanowania komputera po dokonaniu zmian z użyciem opcji wstrzymania polityki. | TAK |  | | |
|  | Aplikacja musi posiadać funkcję ręcznej aktualizacji komponentów programu. | TAK |  | | |
|  | Możliwość zmiany konfiguracji programu z poziomu dedykowanego modułu wiersza poleceń. Zmiana konfiguracji jest w takim przypadku autoryzowana bez hasła lub za pomocą hasła do ustawień zaawansowanych. | TAK |  | | |
|  | Program musi posiadać możliwość definiowana stanów aplikacji, jakie będą wyświetlane użytkownikowi np. powiadomień o wyłączonych mechanizmach ochrony czy stanie licencji. | TAK |  | | |
|  | Administrator musi mieć możliwość dodania własnego komunikatu do stopki powiadomień, jakie będą wyświetlane użytkownikowi na pulpicie. | TAK |  | | |
| **Ochrona przed spamem** | | | | | |
|  | Ochrona antyspamowa dla programów pocztowych MS Outlook, Outlook Express, Windows Mail oraz Windows Live Mail. | TAK |  | | |
|  | Program ma umożliwiać uaktywnienie funkcji wyłączenia skanowania baz programu pocztowego po zmianie zawartości skrzynki odbiorczej. | TAK |  | | |
|  | Pełna integracja z programami pocztowymi MS Outlook, Outlook Express, Windows Mail oraz Windows Live Mail – antyspamowe funkcje programu dostępne są bezpośrednio z paska menu programu pocztowego. | TAK |  | | |
|  | Automatyczne wpisanie do białej listy wszystkich kontaktów z książki adresowej programu pocztowego. | TAK |  | | |
|  | Możliwość ręcznej zmiany klasyfikacji wiadomości spamu na pożądaną wiadomość i odwrotnie oraz ręcznego dodania wiadomości do białej i czarnej listy z wykorzystaniem funkcji programu zintegrowanych z programem pocztowym. | TAK |  | | |
|  | Możliwość definiowania swoich własnych folderów, gdzie program pocztowy będzie umieszczać spam. | TAK |  | | |
|  | Możliwość zdefiniowania dowolnego Tag-u dodawanego do tematu wiadomości zakwalifikowanej jako spam. | TAK |  | | |
|  | Program ma umożliwiać współpracę w swojej domyślnej konfiguracji z folderem „Wiadomości śmieci” obecnym w programie Microsoft Outlook. | TAK |  | | |
|  | Program ma umożliwiać funkcjonalność, która po zmianie klasyfikacji wiadomości typu spam na pożądaną zmieni jej właściwość jako „nieprzeczytana” oraz w momencie zaklasyfikowania wiadomości jako spam na automatyczne ustawienie jej właściwości jako „przeczytana”. | TAK |  | | |
|  | Program musi posiadać funkcjonalność wyłączenia modułu antyspamowego na określony czas lub do czasu ponownego uruchomienia komputera. | TAK |  | | |
| **Zapora osobista (personal firewall)** | | | | | |
|  | Zapora osobista ma pracować jednym z 4 trybów: | TAK |  | | |
|  | tryb automatyczny – program blokuje cały ruch przychodzący i zezwala tylko na znane, bezpieczne połączenia wychodzące, jednocześnie umożliwia utworzenie dodatkowych reguł przez administratora | TAK |  | | |
|  | tryb interaktywny – program pyta się o każde nowe nawiązywane połączenie i automatycznie tworzy dla niego regułę (na stałe lub tymczasowo), | TAK |  | | |
|  | tryb oparty na regułach – użytkownik/administrator musi ręcznie zdefiniować reguły określające jaki ruch jest blokowany a jaki przepuszczany, | TAK |  | | |
|  | tryb uczenia się – umożliwia zdefiniowanie przez administratora określonego okresu czasu w którym oprogramowanie samo tworzy odpowiednie reguły zapory analizując aktywność sieciową danej stacji. | TAK |  | | |
|  | Program musi akceptować istniejące reguły w zaporze systemu Windows, zezwalające na ruch przychodzący. | TAK |  | | |
|  | Możliwość tworzenia list sieci zaufanych. | TAK |  | | |
|  | Możliwość dezaktywacji funkcji zapory sieciowej poprzez trwałe wyłączenie | TAK |  | | |
|  | Możliwość określenia w regułach zapory osobistej kierunku ruchu, portu lub zakresu portów, protokołu, aplikacji i adresu komputera zdalnego. | TAK |  | | |
|  | Możliwość wyboru jednej z 3 akcji w trakcie tworzenia reguł w trybie interaktywnym: zezwól, zablokuj i pytaj o decyzję. | TAK |  | | |
|  | Możliwość powiadomienia użytkownika o nawiązaniu określonych połączeń oraz odnotowanie faktu nawiązania danego połączenia w dzienniku zdarzeń. | TAK |  | | |
|  | Możliwość zapisywania w dzienniku zdarzeń związanych z zezwoleniem lub zablokowaniem danego typu ruchu. | TAK |  | | |
|  | Możliwość zdefiniowania wielu niezależnych zestawów reguł dla każdej sieci, w której pracuje komputer w tym minimum dla strefy zaufanej i sieci Internet. | TAK |  | | |
|  | Wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych*.* | TAK |  | | |
|  | Program musi umożliwiać ochronę przed przyłączeniem komputera do sieci botnet. | TAK |  | | |
|  | Wykrywanie zmian w aplikacjach korzystających z sieci i monitorowanie o tym zdarzeniu. | TAK |  | | |
|  | Program ma oferować pełne wsparcie zarówno dla protokołu IPv4 jak i dla standardu IPv6. | TAK |  | | |
|  | Możliwość tworzenia profili pracy zapory osobistej w zależności od wykrytej sieci. | TAK |  | | |
|  | Administrator ma możliwość sprecyzowania, który profil zapory ma zostać zaaplikowany po wykryciu danej sieci | TAK |  | | |
|  | Profile mają możliwość automatycznego przełączania, bez ingerencji użytkownika lub administratora. | TAK |  | | |
|  | Autoryzacja stref ma się odbywać min. w oparciu o: zaaplikowany profil połączenia, adres serwera DNS, sufiks domeny, adres domyślnej bramy, adres serwera WINS, adres serwera DHCP, lokalny adres IP, identyfikator SSID, szyfrowaniu sieci bezprzewodowej lub jego braku, aktywności połączenia bezprzewodowego lub jego braku, konkretny interfejs sieciowy w systemie. | TAK |  | | |
|  | Podczas konfiguracji autoryzacji sieci, administrator ma mieć możliwość definiowania adresów IP dla lokalnego połączenia, adresu IP serwera DHCP, adresu serwera DNS oraz adresu IP serwera WINS zarówno z wykorzystaniem adresów IPv4 jak i IPv6 | TAK |  | | |
|  | Opcje związane z autoryzacją stref mają oferować opcje łączenia (np. lokalny adres IP i adres serwera DNS) w dowolnej kombinacji celem zwiększenia dokładności identyfikacji danej sieci. | TAK |  | | |
|  | Program musi możliwość ustalenia tymczasowej czarnej listy adresów IP, które będą blokowane podczas próby połączenia. | TAK |  | | |
|  | Program musi posiadać kreator, który umożliwia rozwiązać problemy z połączeniem. Musi on działać w oparciu o: | TAK |  | | |
|  | rozwiązanie problemów z aplikacją lokalną którą wskazujemy z listy. Dana reguła będzie mogła obowiązywać przez określony okres czasu. | TAK |  | | |
|  | rozwiązywanie problemów z połączeniem z urządzeniem zdalnym na podstawie adresu IP, dana reguła będzie mogła obowiązywać przez określony okres czasu. | TAK |  | | |
| **Kontrola dostępu do stron internetowych** | | | | | |
|  | Aplikacja musi być wyposażona w zintegrowany moduł kontroli odwiedzanych stron internetowych. | TAK |  | | |
|  | Moduł kontroli dostępu do stron internetowych musi posiadać możliwość dodawania różnych użytkowników, dla których będą stosowane zdefiniowane reguły. | TAK |  | | |
|  | Dodawanie użytkowników musi być możliwe w oparciu o już istniejące konta użytkowników systemu operacyjnego. | TAK |  | | |
|  | Profile mają być automatycznie aktywowane w zależności od zalogowanego użytkownika. | TAK |  | | |
|  | Aplikacja musi posiadać możliwość filtrowania url w oparciu o co najmniej 140 kategorii i pod kategorii. | TAK |  | | |
|  | Podstawowe kategorie w jakie aplikacja musi być wyposażona to: materiały dla dorosłych, usługi biznesowe, komunikacja i sieci społecznościowe, działalność przestępcza, oświata, rozrywka, gry, zdrowie, informatyka, styl życia, aktualności, polityka, religia i prawo, wyszukiwarki, bezpieczeństwo i szkodliwe oprogramowanie, zakupy, hazard, udostępnianie plików, zainteresowania dzieci, serwery proxy, alkohol i tytoń, szukanie pracy, nieruchomości, finanse i pieniądze, niebezpieczne sporty, nierozpoznane kategorie oraz elementy niezaliczone do żadnej kategorii. | TAK |  | | |
|  | Moduł musi posiadać także możliwość grupowania kategorii już istniejących. | TAK |  | | |
|  | Lista adresów url znajdujących się w poszczególnych kategoriach musi być na bieżąco aktualizowana przez producenta. | TAK |  | | |
|  | Użytkownik musi posiadać możliwość wyłączenia integracji modułu kontroli dostępu do stron internetowych. | TAK |  | | |
|  | Aplikacja musi posiadać możliwość określenia uprawnień dla dostępu do kategorii url – zezwól, zezwól i ostrzeż, blokuj. | TAK |  | | |
|  | Program musi posiadać także możliwość dodania komunikatu i grafiki w przypadku zablokowania określonej w regułach witryny. | TAK |  | | |
| **Administracja zdalna** | | | | | |
|  | Serwer administracyjny musi oferować możliwość instalacji na systemach Windows Server 2003, 2008, 2012 oraz systemach Linux. | TAK |  | | |
|  | Musi istnieć możliwość pobrania ze strony producenta serwera zarządzającego w postaci gotowej maszyny wirtualnej w formacie OVA (Open Virtual Appliance). | TAK |  | | |
|  | Serwer administracyjny musi wspierać instalację w oparciu o co najmniej bazy danych MS SQL i MySQL. | TAK |  | | |
|  | Serwer administracyjny musi oferować możliwość wykorzystania już istniejącej bazy danych MS SQL lub MySQL użytkownika. | TAK |  | | |
|  | Administrator musi posiadać możliwość pobrania wszystkich wymaganych elementów serwera centralnej administracji i konsoli w postaci jednego pakietu instalacyjnego lub każdego z modułów oddzielnie bezpośrednio ze strony producenta. | TAK |  | | |
|  | Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW niezależnie od platformy sprzętowej i programowej. | TAK |  | | |
|  | Narzędzie administracyjne musi wspierać połączenia poprzez serwer proxy występujące w sieci. | TAK |  | | |
|  | Narzędzie musi być kompatybilne z protokołami IPv4 oraz IPv6. | TAK |  | | |
|  | Podczas logowania administrator musi mieć możliwość wyboru języka w jakim zostanie wyświetlony panel zarządzający. | TAK |  | | |
|  | Zmiana języka panelu administracyjnego nie może wymagać zatrzymania lub reinstalacji oprogramowania zarządzającego. | TAK |  | | |
|  | Komunikacja z konsolą powinna być zabezpieczona się za pośrednictwem protokołu SSL. | TAK |  | | |
|  | Narzędzie do administracji zdalnej musi posiadać moduł pozwalający na wykrycie niezarządzanych stacji roboczych w sieci. | TAK |  | | |
|  | Serwer administracyjny musi posiadać mechanizm instalacji zdalnej agenta na stacjach roboczych. | TAK |  | | |
|  | Jeden centralny serwer centralnego zarządzania bez względu na wielkość sieci. | TAK |  | | |
|  | Instalacja serwera administracyjnego powinna oferować wybór trybu pracy serwera w sieci w przypadku rozproszonych sieci –serwer pośredniczący (proxy) lub serwer centralny. | TAK |  | | |
|  | Serwer proxy musi pełnić funkcję pośrednika pomiędzy lokalizacjami zdalnymi a serwerem centralnym. | TAK |  | | |
|  | Serwer proxy musi być wyposażony we własną bazę danych, w której będą przechowywane dane z agentów na wypadek braku połączenia z serwerem centralnym. | TAK |  | | |
|  | Serwer administracyjny musi oferować możliwość instalacji modułu do zarządzania urządzeniami mobilnymi – MDM. | TAK |  | | |
|  | Serwer administracyjny musi oferować możliwość instalacji serwera http proxy pozwalającego na pobieranie aktualizacji baz sygnatur oraz pakietów instalacyjnych na stacjach roboczych bez dostępu do Internetu. | TAK |  | | |
|  | Serwer http proxy musi posiadać mechanizm zapisywania w pamięci podręcznej (cache) najczęściej pobieranych elementów. | TAK |  | | |
|  | Komunikacja pomiędzy poszczególnymi modułami serwera musi być zabezpieczona za pomocą certyfikatów. | TAK |  | | |
|  | Serwer administracyjny musi oferować możliwość utworzenia własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy. | TAK |  | | |
|  | Centralna administracja musi pozwalać na zarządzanie programami zabezpieczającymi na stacjach roboczych z systemami Windows, Mac OS X oraz Linux oraz serwerach Windows. | TAK |  | | |
|  | Centralna administracja musi pozwalać na zarządzanie programami zabezpieczającymi na urządzeniach mobilnych z systemem Android. | TAK |  | | |
|  | Centralna konfiguracja i zarządzanie ochroną antywirusową, antyspyware’ową, zaporą osobistą i kontrolą dostępu do stron internetowych zainstalowanymi na stacjach roboczych w sieci. | TAK |  | | |
|  | Zarządzanie oprogramowaniem zabezpieczającym na stacjach roboczych musi odbywać się za pośrednictwem dedykowanego agenta. | TAK |  | | |
|  | Administrator musi posiadać możliwość zarządzania za pomocą dedykowanego agenta stacjami nie posiadającymi zainstalowanego programu zabezpieczającego. | TAK |  | | |
|  | Agent musi przekazywać informacje na temat stanu systemu operacyjnego do serwera administracji zdalnej | TAK |  | | |
|  | .Agent musi posiadać możliwość pobrania listy zainstalowanego oprogramowania firm trzecich na stacji roboczej z możliwością jego odinstalowania. | TAK |  | | |
|  | Serwer administracyjny musi oferować możliwość wymuszenia połączenia agenta do serwera administracyjnego z pominięciem domyślnego czasu oczekiwania na połączenie. | TAK |  | | |
|  | Instalacja agenta musi odbywać się przy wykorzystaniu repozytorium producenta. Repozytorium powinno zawierać aktualne wersje agentów bez względu na rodzaj systemu operacyjnego. | TAK |  | | |
|  | Instalacja agenta nie może wymagać określenia typu systemu (32 lub 64 – bitowy) oraz jego rodzaju (Windows, Mac, itp) a dobór odpowiedniego pakietu musi być w pełni automatyczny. | TAK |  | | |
|  | Instalacja klienta na urządzeniach mobilnych musi być dostępna za pośrednictwem portalu WWW udostępnionego przez moduł MDM z poziomu urządzenia użytkownika. | TAK |  | | |
|  | W przypadku braku zainstalowanego klienta na urządzeniu mobilnym musi istnieć możliwość jego pobrania ze sklepu Google Play. | TAK |  | | |
|  | Administrator musi posiadać możliwość utworzenia listy zautoryzowanych urządzeń mobilnych, które mogą zostać podłączone do serwera centralnej administracji. | TAK |  | | |
|  | Serwer administracyjny musi oferować możliwość zablokowania, odblokowania, wyczyszczenia zawartości, zlokalizowania oraz uruchomienia syreny na zarządzanym urządzaniu mobilnym. Funkcjonalność musi wykorzystywać połączenie internetowe, nie komunikację za pośrednictwem wiadomości SMS. | TAK |  | | |
|  | Serwer administracyjny musi oferować możliwość utworzenia polityk konfiguracji dla aplikacji zabezpieczającej na urządzeniu mobilnym. | TAK |  | | |
|  | Administrator musi posiadać możliwość utworzenia dodatkowych użytkowników/administratorów Serwer centralnego zarządzania do zarządzania stacjami roboczymi. | TAK |  | | |
|  | Administrator musi posiadać możliwość utworzenia użytkownika wbudowanego lub zintegrowanego z grupą z usługi Active Directory. | TAK |  | | |
|  | Administrator musi posiadać wymuszenia dwufazowej autoryzacji podczas logowania do konsoli zarządzającej | TAK |  | | |
|  | Dwu fazowa autoryzacja musi się odbywać za pomocą wiadomości SMS lub haseł jednorazowych generowanych na urządzeniu mobilnym za pomocą dedykowanej aplikacji. | TAK |  | | |
|  | Serwer administracyjny musi oferować możliwość utworzenia zestawów uprawnień dotyczących zarządzania poszczególnymi grupami komputerów, politykami, instalacją agenta, raportowania, zarządzania licencjami, zadaniami, itp. | TAK |  | | |
|  | Administrator musi posiadać możliwość nadania dwóch typów uprawnień do każdej z funkcji przypisanej w zestawie uprawnień: tylko do odczytu, odczyt/zapis. | TAK |  | | |
|  | Administrator musi posiadać możliwość przypisania kilku zestawów uprawnień do jednego użytkownika. | TAK |  | | |
|  | Użytkownik musi posiadać możliwość zmiany hasła dla swojego konta bez konieczności logowania się do panelu administracyjnego. | TAK |  | | |
|  | Serwer administracyjny musi posiadać możliwość konfiguracji czasu bezczynności po jakim użytkownik zostanie automatycznie wylogowany. | TAK |  | | |
|  | Dostępne zadania muszą być podzielone na dwie grupy: zadania klienta oraz zadania serwera. | TAK |  | | |
|  | Zadania serwera obejmujące zadanie instalacji agenta, generowania raportów oraz synchronizacji grup. | TAK |  | | |
|  | Zadania klienta muszą być wykonywane za pośrednictwem agenta na stacji roboczej. | TAK |  | | |
|  | Agent musi posiadać mechanizm pozwalający na zapis zadania w swojej pamięci wewnętrznej w celu ich późniejszego wykonania bez względu na stan połączenia z serwerem centralnej administracji. | TAK |  | | |
|  | Serwer administracyjny musi w przejrzysty sposób informować administratora o elementach zadań jakie są wymagane do jego uruchomienia a w przypadku jego braku wskazywać brakujące elementy konfiguracji. | TAK |  | | |
|  | Instalacja zdalna programu zabezpieczającego za pośrednictwem agenta musi odbywać się z repozytorium producenta lub z pakietu dostępnego w Internecie lub zasobie lokalnym. | TAK |  | | |
|  | Serwer administracyjny musi oferować możliwość wyboru parametrów pakietu instalacyjnego zależnych od systemu operacyjnego oraz licencji na program zabezpieczający. | TAK |  | | |
|  | Serwer administracyjny musi oferować możliwość deinstalacji programu zabezpieczającego firm trzecich lub jego niepełnej instalacji podczas instalacji nowego pakietu. | TAK |  | | |
|  | Serwer administracyjny musi oferować możliwość wysłania komunikatu lub polecenia na stacje kliencką. | TAK |  | | |
|  | Serwer administracyjny musi oferować możliwość utworzenia jednego zadania dla kilku klientów lub grupy. | TAK |  | | |
|  | Serwer administracyjny musi oferować możliwość uruchomienia zadania automatycznie zgodnie z harmonogramem, po wystąpieniu nowego dziennika zdarzeń lub umieszczeniu nowego klienta w grupie dynamicznej. | TAK |  | | |
|  | Serwer administracyjny musi oferować możliwość utworzenia grup statycznych i dynamicznych komputerów. | TAK |  | | |
|  | Grupy dynamiczne tworzone na podstawie szablonu określającego warunki jakie musi spełnić klient aby zostać umieszczony w danej grupie. Przykładowe warunki: Adresy sieciowe IP, Aktywne zagrożenia, Stan funkcjonowania/ochrony, Wersja systemu operacyjnego, itp. | TAK |  | | |
|  | Serwer administracyjny musi oferować możliwość utworzenia polityk dla programów zabezpieczających i modułów serwera centralnego zarządzania. | TAK |  | | |
|  | Serwer administracyjny musi oferować możliwość przypisania polityki dla pojedynczego klienta lub dla grupy komputerów. Serwer administracyjny musi oferować możliwość przypisania kilku polityk z innymi priorytetami dla jednego klienta. | TAK |  | | |
|  | Edytor konfiguracji polityki musi być identyczny jak edytor konfiguracji ustawień zaawansowanych w programie zabezpieczającym na stacji roboczej. | TAK |  | | |
|  | Serwer administracyjny musi oferować możliwość nadania priorytetu „Wymuś” dla konkretnej opcji w konfiguracji klienta. Opcja ta nie będzie mogła być zmieniona na stacji klienckiej bez względu na zabezpieczenie całej konfiguracji hasłem lub w przypadku jego braku. | TAK |  | | |
|  | Serwer administracyjny musi oferować możliwość ukrycia graficznego interfejsu użytkownika na stacji klienckiej i jego uruchomienia tylko przez administratora. | TAK |  | | |
|  | Serwer administracyjny musi umożliwiać wyświetlenie polityk do których przynależy dana stacja robocza oraz ich edycję z poziomu właściwości samego klienta | TAK |  | | |
|  | Serwer administracyjny musi oferować możliwość utworzenia własnych raportów lub skorzystanie z predefiniowanych wzorów. | TAK |  | | |
|  | Serwer administracyjny musi oferować możliwość utworzenia raportów zawierających dane zebrane przez agenta ze stacji roboczej i serwer centralnego zarządzania. | TAK |  | | |
|  | Serwer administracyjny musi oferować możliwość wyboru formy przedstawienia danych w raporcie w postaci tabeli, wykresu lub obu elementów jednocześnie. | TAK |  | | |
|  | Serwer administracyjny musi oferować możliwość wyboru jednego z kilku typów wykresów: kołowy, pierścieniowy, liniowy, słupkowy, punktowy, itp. | TAK |  | | |
|  | Serwer administracyjny musi oferować możliwość określenia danych jakie powinny znajdować się w poszczególnych kolumnach tabeli lub na elementach wykresu oraz ich odfiltrowania i posortowania. | TAK |  | | |
|  | Serwer administracyjny musi być wyposażona w mechanizm importu oraz eksportu szablonów raportów. | TAK |  | | |
|  | Serwer administracyjny powinien posiadać Panel kontrolny z raportami administratora, pozwalający na szybki dostępu do najbardziej interesujących go danych. Panel ten musi oferować możliwość modyfikacji jego elementów. | TAK |  | | |
|  | Serwer administracyjny musi oferować możliwość wygenerowania raportu na żądanie, zgodnie z harmonogramem lub umieszczenie raportu na Panelu kontrolnym dostępnym z poziomu interfejsu konsoli WWW. | TAK |  | | |
|  | Raport generowany okresowo może zostać wysłany za pośrednictwem wiadomości email lub zapisany do pliku w formacie PDF, CSV lub PS. | TAK |  | | |
|  | Serwer administracyjny musi oferować możliwość skonfigurowania czasu automatycznego odświeżania raportu na panelu kontrolnym oraz umożliwiać jego odświeżenie na żądanie. | TAK |  | | |
|  | Serwer administracyjny musi oferować możliwość tworzenia wielu zakładek panelu, w których będą widoczne wybrane przez administratora elementy monitorujące. | TAK |  | | |
|  | Serwer administracyjny musi oferować możliwość maksymalizacji wybranego elementu monitorującego. | TAK |  | | |
|  | Raport na panelu kontrolnym musi być w pełni interaktywny pozwalając przejść do zarządzania stacją/stacjami, której raport dotyczy. | TAK |  | | |
|  | Serwer administracyjny musi oferować możliwość utworzenia własnych powiadomień lub skorzystanie z predefiniowanych wzorów. | TAK |  | | |
|  | Powiadomienia muszą dotyczyć zmiany ilości klientów danej grupy dynamicznej, wzrostu liczby grupy w stosunku do innej grupy, pojawienia się dziennika zagrożeń lub skanowania lub stanu obiektu serwer centralnego zarządzania. | TAK |  | | |
|  | Administrator musi posiadać możliwość wysłania powiadomienia za pośrednictwem wiadomości email lub komunikatu SNMP. | TAK |  | | |
|  | Serwer administracyjny musi oferować możliwość konfiguracji własnej treści komunikatu w powiadomieniu. | TAK |  | | |
|  | Serwer administracyjny musi oferować możliwość agregacji identycznych powiadomień występujących w zadanym przez administratora okresie czasu. | TAK |  | | |
|  | Serwer administracyjny musi oferować możliwość podłączenia serwera administracji zdalnej do portalu zarządzania licencjami dostępnego na serwerze producenta. | TAK |  | | |
|  | Serwer administracyjny musi oferować możliwość dodania licencji do serwera zarządzania na podstawie klucza licencyjnego lub pliku offline licencji. | TAK |  | | |
|  | Serwer administracyjny musi posiadać możliwość dodania dowolnej ilości licencji obejmujących różne produkty. | TAK |  | | |
|  | Serwer administracyjny musi oferować możliwość weryfikacji identyfikatora publicznego licencji, ilości wykorzystanych stanowisk, czasu wygaśnięcia, wersji produktu, na który jest licencja oraz jej właściciela. | TAK |  | | |
|  | Narzędzie administracyjne musi być wyposażone w mechanizm wyszukiwania zarządzanych komputerów na podstawie co najmniej nazwy komputera, adresu IPv4 i IPv6 lub wyszukania konkretnej nazwy zagrożenia. | TAK |  | | |
|  | Serwer administracyjny musi być wyposażona w machizm autodopasowania kolumn w zależności od rozdzielczości urządzenia na jakim jest wyświetlana. | TAK |  | | |
|  | Administrator musi mieć możliwość określenia zakresu czasu w jakim dane zadanie będzie wykonywane (sekundy, minuty, godziny, dni, tygodnie). | TAK |  | | |
|  | Serwer administracji musi umożliwić granulację uprawnień dla Administratorów w taki sposób, aby każdemu z nich możliwe było przyznanie oddzielnych uprawnień do poszczególnych grup komputerów, polityk lub zadań. | TAK |  | | |
|  | Konfiguracja zestawów uprawnień musi umożliwiać przypisanie praw tylko do odczytu, odczytu i użycia, oraz prawo do zapisania zmian w ramach danego zadania lub polityki w konsoli ERA. | TAK |  | | |
|  | Konsola webowa musi umożliwiać stronicowanie w widoku komputerów w celu ograniczenia liczby wyświetlanych maszyn na jednej stronie. | TAK |  | | |
|  | Administrator musi mieć możliwość podłączenia do stacji roboczej z użyciem protokołu RDP bezpośrednio z poziomu konsoli ERA. | TAK |  | | |
|  | Serwer musi wspierać wysyłanie logów do systemu SIEM IBM qRadar | TAK |  | | |
|  | Musi istnieć mechanizm, umożliwiający dodawanie reguł do istniejących już w module firewalla lub harmonogramie. Takie reguły można umieścić na początku lub końcu istniejącej listy. | TAK |  | | |
|  | Konsola administracyjna musi umożliwiać dodanie własnego logotypu do interfejsu webowego. | TAK |  | | |

1. **Moduł e-Konsultacje – 1 sztuka**

Opis:

E-Usługa polegająca na pozyskaniu przez pacjenta specjalistycznej porady lekarskiej na żądany temat, bez konieczności wychodzenia z domu, w sposób zdalny przez Internet. Usługa umożliwiać ma konsultacje pisemne lub video-konsultacje według ustalonego terminarza. Zarówno pacjent jak i lekarz mają mieć dostęp do wyników pacjenta i historii leczenia. Moduł e-konsultacji umożliwiać ma zadawanie pytań / zgłaszanie uwag przez pacjentów poprzez wewnętrzny system komunikacji. Proces e-konsultacji ma zostać wsparty systemem powiadomień indywidualnych dla Pacjentów (SMS/email) o dostępności odpowiedzi na zadane przez Pacjenta pytanie.

Usługa umożliwiać ma także przeprowadzenie wideokonferencji z lekarzem w celu wykonania konsultacji medycznej on-line. W trakcie wideo konsultacji, lekarz ma mieć dostęp do udostępnionej na portalu dokumentacji medycznej (wyników badań, karty informacyjnej, obrazów diagnostycznych..). Konsultacje on-line obrazu i dźwięku mają mieć możliwość odbywania się w jakości HD oraz niższej, w zależności od podłączonej stacji nadawczej i możliwości sieci pacjenta. Wideo konsultacje realizowane mają być zdalnie i mają obsługiwać do kilkunastu jednoczesnych połączeń i mogą być realizowane z dedykowanych terminali, telefonów, tabletów, komputerów PC, pozwalając na udostępnienie np. obrazu z pulpitu roboczego. Usługa zapewniać ma bezpieczną transmisję danych zgodną z obecnie panującymi standardami i wymogami prawnymi.

**Model kluczowych kroków procesu:**

1. Pacjent loguje się do e-Portalu.
2. Pacjent wybiera typ konsultacji: pisemna lub wideokonferencja.
3. Po wybraniu konsultacji pisemnych:
   1. pacjent zadaje pytanie i kończy pracę z systemem
   2. lekarza analizuje pytanie i wpisuje odpowiedź
   3. e-Portal wysyła powiadomienie do pacjenta o dostępnej odpowiedzi
   4. pacjent ponownie loguje się do e-Portalu i czyta odpowiedź; następnie kontynuuje konsultacje lub kończy pracę z systemem.
4. Po wybraniu wideokonferencji:
   1. Pacjent wyszukuje i wybiera właściwego lekarza, który ma możliwość udzielania konsultacji w trybie telekonferencji
   2. System uruchamia komunikator i łączy z wybranym lekarzem
   3. Lekarz udziela konsultacji
   4. Lekarz i pacjent kończą pracę z systemem

|  |  |  |  |
| --- | --- | --- | --- |
| **OPIS PRZEDMIOTU ZAMÓWIENIA** | | | |
| **Lp** | **Oznaczenie produktu zamówienia** | **Wymóg graniczny (TAK / NIE) lub informacja o wyborze punktowanym** | **Wymóg spełniony (TAK / NIE / OPCJA – w wybranych polach)** |
| 1. **Moduł e-Konsultacje – 1 sztuka** | | | |
| 11.1 | Moduł umożliwia konsultacje pisemne, gromadzone w powiązaniu z rekordem medycznym pacjenta między lekarzem a pacjentem. Umożliwia zadawanie pytań / zgłaszanie uwag przez pacjentów poprzez wewnętrzny system komunikacji. | Warunek opcjonalny, dodatkowo punktowany:  - spełnione (TAK): 1pkt  - niespełnione (NIE): 0pkt |  |
| 11.2 | W części szpitalnej i poradni użytkownicy korzystają z wbudowanej w system kontrolki do komunikacji z pacjentem. | Warunek opcjonalny, dodatkowo punktowany:  - spełnione (TAK): 1pkt  - niespełnione (NIE): 0pkt |  |
| 11.3 | Pacjent może zwęzić konsultacje do wybranej poradni i lekarza na podstawie odbytych wizyt. | TAK |  |
| 11.4 | Wiadomość wysłana z portalu przez zalogowanego pacjenta będzie dostępna w systemie HIS dla osoby podanej w konfiguracji funkcjonalności. | Warunek opcjonalny, dodatkowo punktowany:  - spełnione (TAK): 1pkt  - niespełnione (NIE): 0pkt |  |
| 11.5 | Do wiadomości wysłanej przez pacjenta możliwa będzie generacja jednej odpowiedzi (dostępnej następnie do podglądu przez pacjenta na portalu). | TAK |  |
| 11.6 | Pacjent zostanie poinformowany za pomocą maila o odpowiedzi na pytanie. | TAK |  |
| 11.7 | Pacjent będzie miał dostęp do historii konsultacji pisemnych. | TAK |  |
| 11.8 | Wspólny moduł administracyjny dla e-Portalu oraz systemu HIS umożliwia administrację funkcjami e-Portalu oraz wspólnymi słownikami. | Warunek opcjonalny, dodatkowo punktowany:  - spełnione (TAK): 1pkt  - niespełnione (NIE): 0pkt |  |
| **Minimalny zakres funkcjonalności w module administracyjnym:** | | | |
| 11.9 | W nagłówku portalu może zostać umieszczone logo jednostki medycznej. | TAK |  |
| **Moduł administracyjny umożliwia administratorowi na definiowanie przynajmniej następujących parametrów e-usług e-Portalu pacjenta:** | | | |
| 11.10 | umożliwia konfigurację szablonu wiadomości, jakie System będzie automatycznie wysyłał do pacjentów: przypomnienia o wizycie, przypomnienie o potwierdzeniu wizyty, anulowanie niepotwierdzonej wizyty | Warunek opcjonalny, dodatkowo punktowany:  - spełnione (TAK): 1pkt  - niespełnione (NIE): 0pkt |  |
| 11.11 | Umożliwia wskazanie E-mail: adres serwera i parametry SMTP (serwer poczty wychodzącej). | Warunek opcjonalny, dodatkowo punktowany:  - spełnione (TAK): 1pkt  - niespełnione (NIE): 0pkt |  |
| 11.12 | Umożliwia ustawienie opcji: czas generowania wiadomości - w momencie wykonania akcji w Systemie lub wyrażenie cron. | Warunek opcjonalny, dodatkowo punktowany:  - spełnione (TAK): 1pkt  - niespełnione (NIE): 0pkt |  |
| 11.13 | 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” | Warunek opcjonalny, dodatkowo punktowany:  - spełnione (TAK): 1pkt  - niespełnione (NIE): 0pkt |  |
| 11.14 | Czas blokady konta - Opcja pozwala na określenie czasu (w minutach), na jaki konto pacjenta zostanie zablokowane, po tym jak wykorzysta limit nieudanych prób logowania. | Warunek opcjonalny, dodatkowo punktowany:  - spełnione (TAK): 1pkt  - niespełnione (NIE): 0pkt |  |
| 11.15 | Adres internetowy do powiadomień - Opcja określa widziany adres e-mail w powiadomieniach wysyłanych pacjentowi. | Warunek opcjonalny, dodatkowo punktowany:  - spełnione (TAK): 1pkt  - niespełnione (NIE): 0pkt |  |
| **Ogólne wymagania odnośnie instalacji i bezpieczeństwa** | | | |
| 11.16 | Serwer WWW powinien być udostępniony (chroniony) za dodatkowym serwerem proxy. | TAK |  |
| 11.17 | ePortal będzie wyposażony w certyfikat SSL. Będzie posiadał odpowiednią nazwę domenową. | TAK |  |
| 11.18 | Zamawiający zapewni Wykonawcy do instalacji wymagany certyfikat SSL. | TAK |  |
| 11.19 | Dostarczony certyfikat będzie pochodził od uzgodnionych z Wykonawcą dostawców, minimum: GeoTrust (min. QuickSSL Premium) lub Thawte (min. SSL 123) Będzie posiadał okres ważności certyfikatu minimum 5 lata | TAK |  |

1. **Moduł e-Wyniki – 1 sztuka**

Opis:

E-usługa ma umożliwić odbiór dokumentacji medycznej przez pacjenta tj. wyników badań, obrazów, itp. metodą zdalną za pośrednictwem Internetu**.** Wyniki badań udostępniane online pacjentom mają dotyczyć zarówno elementów dokumentacji jak i wyników obrazowych z systemu PACS (konieczna integracja z obecnie istniejącym systemem obsługującym diagnostykę obrazową w Szpitalu – NetRAAD firmy Compugroup Medical Polska sp.z o.o.).

Pacjent korzystając z funkcjonalności e-Portalu będzie mógł się zalogować, wybrać na podstawie różnych kryteriów (jednostka wykonująca, nazwa badania, status) interesujące go wyniki odczytać, pobrać lub wydrukować. Proces ma być wsparty systemem powiadomień indywidualnych dla Pacjentów (SMS/email) o dostępności wyników do odbioru.

**Model kluczowych kroków procesu:**

1. W pracowni szpitala zostaje wykonane badanie. System zarządzania dokumentacją medyczną generuje informację dla e-Portalu o dostępnym wyniku badania.
2. E-Portal wysyła dostępnymi kanałami powiadomienie dla pacjenta o możliwości pobrania wyniku badania; informacja może być przekazana bezpośrednio w e-Portalu, za pośrednictwem maila lub SMS.
3. Pacjent loguje się do portalu.
4. Pacjent wyszukuje badanie, którego wynik został udostępniony.
5. Pacjent uruchamia drukowanie wyniku lub pobranie go w postaci pliku.
6. E-Portal pobiera dane wyniku z bazy danych systemu i zależnie od wyboru użytkownika: generuje wydruk lub startuje pobieranie pliku z wynikiem.
7. Pacjent kończy pracę z systemem

|  |  |  |  |
| --- | --- | --- | --- |
| **OPIS PRZEDMIOTU ZAMÓWIENA** | | | |
| **Lp** | **Oznaczenie produktu zamówienia** | **Wymóg graniczny (TAK / NIE) lub informacja o wyborze punktowanym** | **Wymóg spełniony (TAK / NIE / OPCJA – w wybranych polach)** |
| 1. **Moduł e-Wyniki – 1 sztuka** | | | |
| 12.1 | Aplikacja umożliwia przeglądanie wyników badań i obrazów diagnostycznych w formacie DICOM/JPG przez pacjenta metodą zdalną za pośrednictwem Internetu. | Warunek opcjonalny, dodatkowo punktowany:  - spełnione (TAK): 1pkt  - niespełnione (NIE): 0pkt |  |
| 12.2 | Pacjent korzystając z przygotowanej witryny internetowej może się zalogować, wybrać na podstawie różnych kryteriów ( jednostka wykonująca, nazwa badania, status) interesujące go wyniki odczytać, pobrać lub wydrukować. | TAK |  |
| 12.3 | Wyniki mogą być prezentowane jako lista lub hierarchicznie z podziałem na jednostki wykonujące. | TAK |  |
| 12.4 | Możliwość prezentowania wyników badań tylko i wyłącznie skonsultowanych podczas porady pacjenta. | TAK |  |
| 12.5 | Możliwość konfiguracji okresu widoczności danego wyniku na liście wyników pacjenta. | TAK |  |
| 12.6 | Pełna integracja z Elektronicznym Rekordem Medycznym Pacjenta systemu szpitalnego, korzystanie z tego samego źródła danych, wspólnego modułu administracyjnego oraz słowników. | Warunek opcjonalny, dodatkowo punktowany:  - spełnione (TAK): 1pkt  - niespełnione (NIE): 0pkt |  |
| 12.7 | Pacjent ma możliwość załączenia zeskanowanych załączników. Lekarz po stronie systemu medycznego HIS działającego w intranecie może zdecydować które z załączników dołączyć do dokumentacji medycznej wizyty. | Warunek opcjonalny, dodatkowo punktowany:  - spełnione (TAK): 1pkt  - niespełnione (NIE): 0pkt |  |

1. **Wdrożenie modułów e-Wyniki i e-Konsultacje oraz wdrożenie nowego systemu serwerowego i bazodanowego wraz z dostosowaniem do niego aplikacji medycznej**
2. **Opis stanu bieżącego**

Zamawiający użytkuje obecnie system klasy HIS (system medyczny) o nazwie CGM CLININET, którego producentem jest CompuGroup Medical Polska sp. z.o.o. (CGM) . Zamawiający posiada licencję na system CGM CLININET, oraz licencje na bazę danych Sybase ASE, na której opiera się działanie systemu HIS.

Lista modułów posiadanych przez Zamawiającego :

1. **HIS (system medyczny):**
   1. Izba przyjęć
   2. Oddział
   3. Apteka Centralna
   4. Poradnia
   5. Diagnostyka
   6. Blok Operacyjny
   7. Administracja
   8. Recepcja
   9. Recepcja szpitala
   10. JPK
   11. SIK (System Informowania Kierownictwa)
   12. STER-Rozliczenia
   13. SAKPro
   14. PACS / RIS (NetRAAD)
   15. e-Rejestracja
   16. Mobilna wersja modułu Oddział
   17. Program do zarządzania księgą jakości ISO

System jest uruchomiony i wdrożony w następujących jednostkach organizacyjnych Zamawiającego:

* oddział chorób wewnętrznych
* oddział leczenia jednego dnia dla dzieci
* oddział hematologiczny
* oddział chirurgii urazowo-ortopedycznej
* oddział chorób płuc
* oddział ginekologiczny
* oddział pediatryczny
* apteka szpitalna
* sterylizatornia
* dział anestezjologii
* blok operacyjny
* dział diagnostyki obrazowej
* pracownie diagnostyczne i zabiegowe
* izba przyjęć szpitala
* poradnia nocnej i świątecznej opieki zdrowotnej
* przychodnia gruźlicy i chorób płuc
* przychodnia specjalistyczna
* zakład opiekuńczo – leczniczy
* oddział medycyny paliatywnej
* hospicjum domowe
* dział nadzoru i kontroli wewnętrznej

Na bieżąco jest wykorzystywany przez następujące kategorie użytkowników:

* Lekarzy
* Pielęgniarki
* Pracowników rozliczeń
* Sekretarki medyczne
* Administratorzy
* Pozostali użytkownicy

System jest częściowo zintegrowany z następującymi systemami użytkowanymi przez Zamawiającego:

* GEM (system kadrowo – płacowy)

1. **Krótki opis przedmiotu zamówienia**

Przedmiotem tej części zamówienia jest instalacja modułów e-Konsultacje i e-Wyniki będących jednym ze składników tego zamówienia, integracja ich z systemem medycznym oraz migracja użytkowanego systemu medycznego na wydajny silnik bazy danych, celem podniesienia wydajności, bezpieczeństwa 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 w konfiguracji funkcjonalnej jaka istniała u Zamawiającego oraz uruchomienia systemu we wszystkich użytkowanych obecnie przez Zamawiającego aspektach to jest:

* System musi być uruchomiony w zakresie wszystkich modułów oraz we wszystkich lokalizacjach wymienionych w punkcie I. „Opis stanu bieżącego” tego dokumentu.
* 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.
* Wykonawca jest zobowiązany do uruchomienia pełnego zakresu integracji z systemami opisanymi w rozdziale „Opis stanu bieżącego”. Koszt ewentualnej modyfikacji integrowanych systemów stanowi koszt Wykonawcy i jest on w pełni odpowiedzialny za uruchomienie pełnych funkcjonalności integracji po wykonaniu migracji.

Dodatkowo system medyczny po migracji musi posiadać następujące funkcjonalności:

* system jest zintegrowany z Elektroniczną Platformą Gromadzenia, Analizy i Udostępnienia Zasobów Cyfrowych o Zdarzeniach Medycznych (P1) w zakresie zgodnym z zapisami ustawy z dnia 28 kwietnia 2011 roku o systemie informacji w ochronie zdrowia.
* system jest dostosowany do prowadzenia i wymiany elektronicznej dokumentacji medycznej zgodnie z zapisami ustawy z dnia 28 kwietnia 2011 roku o systemie informacji w ochronie zdrowia. W szczególności dostosowane zostaną dokumenty określone w Art.. 13a ustawy, wskazane w Rozporządzeniu Ministra Zdrowia z dnia 8 maja 2018 r. w sprawie rodzajów elektronicznej dokumentacji medycznej. Kolejne dokumenty dostosowywane będą wraz z publikacją kolejnych aktów prawnych. Terminy wdrożenia poszczególnych elementów elektronicznej dokumentacji medycznej zostały określone w Art. 56 ustawy z dnia 28 kwietnia 2011 roku o systemie informacji w ochronie zdrowia.

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

* Dostarczenia i instalacji systemów operacyjnych oraz specjalistycznego oprogramowania do wirtualizacji będącego częścią tego zamówienia na serwerach zakupionych w ramach tego zamówienia
* Dostarczenia i instalacji wydajnego silnika bazy danych wraz z umową utrzymania i wsparcia na okres 60 miesięcy zakupionego w ramach tego zamówienia.
* 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,
* Przedstawienia planu, harmonogramu migracji i projektu technicznego migracji do akceptacji Zamawiającego
* 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.
* Przeszkolenia administratorów Zamawiającego z nowej konfiguracji systemu oraz struktury bazy danych.
* Przeniesienia wszystkich danych z użytkowanego systemu CGM CLININET na nową instancję bazy danych.
* Wykonania testów potwierdzających poprawne funkcjonowanie wszystkich modułów aplikacji oraz potwierdzającymi prawidłowość działania raportów, wydruków i integracji z innymi systemami.
* Przeszkolenia użytkowników w zakresie w jakim modyfikacji uległ interfejs graficzny użytkownika i/lub przebieg procesów w systemie.
* Przedstawienie raportu z migracji zawierającego raporty z testów oraz potwierdzenie kompletnego przeniesienia danych pomiędzy systemami bazodanowymi.
* Uruchomienia i wdrożenia systemu medycznego na nowej wydajnej bazie danych wraz z asystą uruchomieniową w zakresie w jakim modyfikacji uległ interfejs graficzny użytkownika i/lub przebieg procesów w systemie.

1. **Organizacja prac projektowych**

W celu efektywnego prowadzenia prac projektowych w ramach Migracji bazy HIS zostaną powołane odpowiednie struktury projektowe, zarówno po stronie Wykonawcy, jak również po stronie Zamawiającego. Powołana zostanie struktura organizacyjna Projektu, w skład której wejdą:

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

**Kierownictwo Projektu**

W skład operacyjnego Kierownictwa wchodzi Kierownik Projektu ze strony Zamawiającego oraz Kierownik Projektu ze strony Wykonawcy. Wykonawca i Zamawiający są zobowiązani do wskazania osób pełniących role Kierownika Projektu.

Obowiązki Kierownika Projektu ze strony Wykonawcy:

1. Wyznaczenie osób upoważnionych do realizacji przedmiotu umowy.
2. Lista osób upoważnionych zostanie przekazana Kierownikowi Projektu 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. Tworzenie planów etapów i ewentualnych planów awaryjnych.
5. Tworzenie harmonogramu projektu
6. Zgłaszanie, zatwierdzanie gotowości do odbioru usług Kierownikowi Projektu ze strony Zamawiającego.
7. Zgłaszanie potrzeby konsultacji i doradztwa w zakresie realizacji projektu.
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 usług.
10. Zapewnienie odpowiedniego zastępstwa na czas swojej nieobecności z poinformowaniem Kierownika Projektu ze strony Zamawiającego.
11. Przedkładanie informacji Kierownikowi Projektu ze strony Zamawiającego zgodnie z jego potrzebami.
12. Przedkładanie wniosków, sugestii i propozycji Kierownikowi Projektu ze strony Zamawiającego zgodnie z potrzebami.
13. Realizowanie we współpracy z Kierownikiem ze strony Zamawiającego wszystkich zadań związanych z procesem zarządzania Projektem.
14. Kontrola zakresu Projektu.
15. Zarządzanie ryzykiem.
16. Wspólna z Kierownikiem Projektu ze strony Zamawiającego kontrola terminowej i zgodnej z budżetem realizacji Projektu, w szczególności w obszarach prac wykonywanych przez pracowników Wykonawcy.
17. Wspólne z Kierownikiem Projektu ze strony Zamawiającego rozwiązywane istotnych kwestii pojawiających się podczas prac projektowych; nadzór nad Liderami Zespołów Projektowych.
18. Koordynacja przeprowadzenia odbioru prac w Projekcie. W przypadku powstania kwestii spornych między stronami zaangażowanymi w realizację Projektu Kierownik powinien być stroną rozstrzygającą o najlepszym rozwiązaniu.

Obowiązki Kierownika Projektu 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 ze strony Wykonawcy.
4. Zatwierdzaniu planów etapów i ewentualnych planów awaryjnych.
5. Zatwierdzaniu harmonogramu projektu
6. Przyjmowanie i akceptacja protokołów odbioru z realizacji etapów przedmiotu umowy.
7. Prawo i obowiązek formalnego zgłoszenia żądania zmiany, jeżeli uzna, że dla zapewnienia prawidłowej realizacji przedmiotu umowy konieczne jest podjęcie działań mających wpływ na ustalony zakres prac.
8. Przegląd, zgłaszanie uwag, akceptacja oraz odbiór poszczególnych Etapów Umowy od Wykonawcy.
9. Zarządzanie i kontrola zakresu Projektu - wspólne z Kierownikiem Projektu ze strony Wykonawcy zarządzanie zakresem prac realizowanych w ramach Projektu.
10. Zarządzanie jakością - w rozumieniu jakości realizacji Projektu oraz jakości dostarczanych produktów prac, w ścisłej współpracy z Kierownikiem Projektu 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 Projektowymi Zamawiającego i Kierownikiem Projektu ze strony Wykonawcy.
14. Zapewnienie zasobów ze strony Zamawiającego koniecznych do terminowego i zgodnego z założeniami wykonania prac.

Prace Wykonawcy powinny być zorganizowane w ramach następującej struktury:

1. Zespół ds. migracji HIS
2. Zespół ds. testów
3. Zespół ds. audytu systemu

Do obowiązków Lidera Zespołu Projektowego 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 Projektu 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 Projektu.
8. Opiniowanie prac z zakresu pracy Zespołu wykonanych przez Wykonawcę.

**Opis sposobu zarządzania ryzykiem w projekcie**

Kierownik projektu ze strony Wykonawcy opracuje i przedstawi Kierownikowi Projektu ze strony Zamawiającego do akceptacji rejestr zagrożeń i środków zaradczych, gdzie identyfikowane i kategoryzowane są poszczególne czynniki ryzyka za pomocą poziomu wpływu na projekt, prawdopodobieństwa wystąpienia, priorytetu, daty powstania i zamknięcia, właściciela ryzyka, opisu ryzyka, kategorii, wymaganych środków zaradczych, statusu. Rejestr ten będzie na bieżąco w ramach potrzeb aktualizowany.

**Opis sposobu komunikacji Wykonawcy z Zamawiającym**

Podczas przeprowadzenia migracji bazy danych systemu HIS będą obowiązywały następujące założenia dotyczące wzajemnej współpracy Zamawiającego i Wykonawcy:

1. Komunikacja między uczestnikami Projektu po stronie Wykonawcy i Zamawiającego będzie się odbywać na poziomie Kierowników Projektów obu stron oraz Kierowników 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 projektu będzie poczta elektroniczna, kontakt telefoniczny i telekonferencje, z zastrzeżeniem, że jeżeli podczas rozmowy podjęte zostaną istotne ustalenia projektowe powinny one zostać potwierdzone poprzez e-mail.
3. Prace wspólne specjalistów po obu stronach (spotkania w ramach analizy przedwdrożeniowej, testy odbiorcze, szkolenia) będą 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 będą organizowane w miarę bieżących potrzeb na życzenie Zamawiającego. Wykonawca będzie odpowiedzialny za przedstawienie raportu o bieżącym zaawansowaniu prac i informacji o zagrożeniach w realizacji projektu oraz sposobach rozwiązywania tych problemów. Spotkania dotyczące kontroli realizacji Projektu również będą potwierdzone notatką ze spotkania podpisaną przez Strony.
5. Zgłoszenie zagadnienia wymagającego decyzji Kierownika Projektu przez Wykonawcę powinno zachować formę pisemną.

**Zgłoszenie zmiany w projekcie**

Potrzeba wprowadzenia zmian może wynikać między innymi z:

1. Potrzeb, które zostały błędnie zdefiniowane, nie zostały zdefiniowane lub uległy zmianie w trakcie przebiegu projektu. W szczególności dotyczy to potrzeby zmian lub rozszerzeń funkcjonalności systemu - związanych z dopasowaniem funkcjonalności systemu do specyficznych potrzeb Zamawiającego w zakresie realizacji procesów biznesowych.
2. Zaakceptowanego sposobu neutralizacji ryzyka projektowego.
3. Wprowadzenia w trakcie wdrożenia zmian organizacyjnych u Zamawiającego, które mają wpływ na zatwierdzony sposób realizacji procesów biznesowych.
4. Konieczności wprowadzenia zmian w zatwierdzonych etapach przedmiotu umowy.

Potrzebę zmiany mają prawo i obowiązek zgłosić kierownicy projektu ze strony Zamawiającego i Wykonawcy, jeżeli uzna, że dla zapewnienia prawidłowej realizacji przedmiotu umowy konieczne jest podjęcie działań mających wpływ na ustalony zakres prac.

Żądanie zmiany jest dokumentowane przez zgłaszającego za pomocą formularza żądania zmiany. Wykonawca w terminie 5 dni roboczych dokonuje analizy zmiany na projekt i przedstawia ją Kierownikowi Projektu ze strony Zamawiającego. Po zapoznaniu z analizą Kierownik projektu Zamawiającego ma prawo przyjąć bądź odrzucić zmianę. W przypadku sporów sprawę rozstrzyga Kierownik Projektu. Zmiany dotyczące harmonogramu projektu i kosztów projektu muszą być zatwierdzone przez Kierownika Projektu.

1. **Harmonogram prac projektowych**

Harmonogram realizacji Projektu migracji bazy danych podzielony będzie na następujące etapy:

**Etap I –** obejmować będzie:

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

Punkt ten będzie zawierał następujące elementy:

* Uruchomienie projektu po stronie Wykonawcy w terminie 2 dni od podpisania umowy.
* Przedstawienie harmonogramu prac projektowych (do 5 dni od podpisania umowy).
* Powołanie struktury projektowej po stronie Wykonawcy i przedstawienie jej Zamawiającemu do 5 dni od podpisania umowy.

Przedstawienia planu migracji oraz projektu technicznego migracji zawierającego następujące elementy:

* Harmonogram procesu migracji danych
* Analizę ryzyka związanego z procesem migracji wraz z planami odpowiedzi minimalizującymi ich wystąpienie.
* Opis konfiguracji obecnego systemu
* Opis konfiguracji docelowego systemu
* Szczegółowy opis procesu migracji danych ze szczególnym uwzględnieniem sposobów w jaki Wykonawca chce zapewnić:
* Kompletność i wiarygodność danych podlegających migracji
* Bezpieczeństwo danych podlegających migracji
* Zabezpieczenie ciągłości pracy Zamawiającego
* Integrację z innymi systemami
* Przebieg i szczegółowy opis procedury testowej poprawności migracji
* Szablon raportu z migracji systemu.

Odbiór punktu - podpisanie protokołu odbioru.

**2. Dostawę sprzętu i licencji oprogramowania** zakupionego w ramach projektu w terminie nie dłuższym niż do **14 grudnia 2018 roku**. Punkt będzie obejmował następujące elementy:

* Dostawę następującego sprzętu oraz licencji oprogramowania (zakupionych w ramach tego projektu):
  + serwery aplikacyjne
  + serwery bazodanowe
  + serwer backupowy
  + macierze dyskowe
  + UPSy
  + Switche FC
  + Szafa RACK
  + moduły e-Konsultacje i e-Wyniki
  + system wirtualizacji
  + system bazodanowy
* Odbiór punktu - podpisanie protokołu odbioru.

3. **Instalację zakupionego w ramach projektu oprogramowania na zakupionym w ramach projektu sprzęcie** w terminie nie dłuższym niż do **01 marca 2019 roku**. Punkt będzie obejmował następujące elementy:

* Instalację i konfigurację oprogramowania:
  + moduły e-Konsultacje i e-Wyniki
  + system wirtualizacji
  + system bazodanowy
* Odbiór punktu - podpisanie protokołu odbioru.

**4. Wykonanie procesu migracji** bazy danych systemu medycznego na wydajną bazę danych, uruchomienie i wdrożenie systemu w nowej konfiguracji w terminie nie dłuższym niż do **30 września 2019 roku**. Punkt będzie obejmował następujące elementy:

* 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.
* Przeniesienia wszystkich danych z użytkowanego systemu medycznego na nową instancję bazy danych.
* Wykonania testów potwierdzających poprawne funkcjonowanie wszystkich modułów systemu medycznego oraz wykonanie testów potwierdzające prawidłowość działania raportów, wydruków i integracji z innymi systemami.
* 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.
* Przeszkolenia użytkowników w zakresie w jakim modyfikacji uległ interfejs graficzny użytkownika i/lub przebieg procesów w systemie.
* Przedstawienie raportu z migracji zawierającego raporty z testów oraz potwierdzenie przeniesienia danych pomiędzy systemami.
* 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.
* Odbiór punktu - podpisanie protokołu odbioru.

**ETAP II –** Obejmować będzie wykonanie dalszej optymalizacji Systemu mającej na celu przyspieszenie jego działania w terminie nie dłuższym niż do **31 października 2019 roku.**

Odbiór punktu - podpisanie protokołu odbioru.

1. **Gwarancja**

**Wykonawca** udziela gwarancji i zapewnia serwis na wykonane prace migracyjne oraz poprawne funkcjonowanie wszystkich modułów zainstalowanych przed migracją w systemie medycznym wraz z instalacją wymaganych prawnie aktualizacji i poprawek na okres 60 miesięcy od daty podpisania końcowego protokołu odbioru.

1. **Analiza przedwdrożeniowa**

W zakresie analizy przedwdrożeniowej Wykonawca zobowiązany będzie do:

1. Przeprowadzenia audytu istniejącego rozwiązania celem identyfikacji i inwentaryzacji konfiguracji elementów niestandardowych systemu HIS użytkowanego przez Zamawiającego w szczególności:
2. Raportów
3. Wydruków
4. Formularzy
5. Integracji z innymi systemami
6. Bieżącej konfiguracji systemu HIS
7. Konfiguracji procedur backupu systemu HIS

Wszystkie elementy wynikające z audytu zostaną 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 przenoszenie wybranych raportów i wydruków. Decyzja w tym zakresie jest wyłączną kompetencją Zamawiającego

1. Opracowania planu migracji – Plan migracji będzie opisywał proces migracji danych z obecnie użytkowanej bazy do wydajnej bazy danych dostarczanej w ramach tego zamówienia i będzie zawierał 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 systemu HIS
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 a nową wydajną dostarczaną zgodnie ze specyfikacją 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 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 zmieniać danych ani struktury danych jak i samych baz danych obecnie użytkowanego systemu medycznego 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 w projekcie technicznym migracji.

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

1. **System HIS**

Wykonawca jest zobowiązany do odtworzenia w nowym środowisku wszystkie funkcjonalności systemu posiadanego przez Zamawiającego w następujących obszarach:

1. System po migracji musi zachować pełną funkcjonalność użytkowaną obecnie przez Zamawiającego
2. System po migracji na wydajną bazę danych ma zachować możliwość użytkowania wszystkich wydruków, raportów oraz formularzy używanych obecnie przez Zamawiającego. Wykonawca w ramach etapu analizy przedwdrożeniowej wykona inwentaryzację tych elementów. Wykonawca ma obowiązek przeniesienia wszystkich tych elementów w ramach procesu migracji. Rezygnacja z przeniesienia jest wyłącznym prawem Zamawiającego.
3. System musi być uruchomiony i wdrożony we wszystkich komórkach organizacyjnych wymienionych w rozdziale „Opis stanu bieżącego” tego dokumentu.
4. 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. Wymagania dla procesu szkoleń przedstawione są w akapicie „Szkolenie personelu w przypadku zmiany interfejsu graficznego lub przebiegu procesu”
5. Wykonawca jest zobowiązany do uruchomienia pełnego zakresu integracji z systemami opisanymi w rozdziale „Opis stanu bieżącego”. Koszt ewentualnej modyfikacji integrowanych systemów stanowi koszt Wykonawcy i jest on w pełni odpowiedzialny za uruchomienie pełnych funkcjonalności integracji po wykonaniu migracji w momencie startu produkcyjnego systemu po migracji.
6. **Przebieg procesu migracji**

W procesie planowania i realizowania migracji danych 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”

**2.** **Pobranie danych do struktur pośrednich** – czynność dotyczy 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, ustalana jest przyczyna błędu. Jeżeli przyczyna leży w złym pobraniu danych z systemu źródłowego proces wraca do kroku „Pobranie danych do struktur pośrednich”. Jeżeli problem dotyczy błędu w procedurach importu danych należy 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 powinna być  wykonywana na pełnych danych. Dopuszcza się w niektórych szczególnie wymagających obszarach (ze względu na ilość 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 przewiduje się wykorzystanie następujących metod sprawdzania poprawności jej wykonania:

1. **Szczegółowa weryfikacja zapis po zapisie**

Jest możliwa tylko 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 w niektórych przypadkach przygotować  zestawienia tabelaryczne danych z nowego systemu eksportowanie do arkusza kalkulacyjnego lub wydrukowane. Wtedy porównanie polega na zaznaczeniu każdego poprawnego zapisu na wydruku lub w arkuszu.

1. **Porównanie skryptami**

Weryfikacja polegająca 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 powinien być automatycznie wygenerowany.

1. **Wyrywkowa kontrola danych przez użytkowników**

Weryfikacja przeprowadzana przez użytkowników docelowych Systemu, mających dostęp do nowego środowiska testowego Systemu oraz Systemu źródłowego. Polega 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**

Polega na uruchomieniu i porównaniu wybranych raportów/wydruków wygenerowanych z Systemu testowego oraz Systemu źródłowego.

1. **Weryfikacja statystyczna**

Polega na stworzeniu 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 zostaną zrealizowane minimum następujące testy:

* Testy funkcjonalne
* Testy integracji

**6. Migracja docelowa produkcyjna**  – właściwa migracja, po której rozpoczyna się produkcyjną pracę w nowym Systemie. W przypadku braku stwierdzonych istotnych problemów w trakcie wcześniejszych kroków procesu migracji Zamawiający podejmuje decyzję o przeprowadzeniu procesu migracji do nowego, docelowego Systemu opartego o wydajną bazę danych. Wykonawca po procesie migracji jest zobowiązanych 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 zostaną przekazane Zamawiającemu.

Wykonawca przeprowadzać będzie migracje w siedzibie Zamawiającego. W przypadku, gdy nie będzie to możliwe, Wykonawca zobowiązany będzie 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 będzie się odbywać protokolarnie upoważnionemu przedstawicielowi Wykonawcy, a prace związane z obróbką pozyskanych danych odbywać się będą 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 |
| ZSN.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. ) |
| ZSN.002 | W procesie migracji zostaną przeniesione wszystkie dane historyczne zgormadzone i przetwarzane obecnie przez Zamawiającego w systemie HIS |
| ZSN.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. |
| ZSN.004 | Wykonawca wykona 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. |
| ZSN.005 | Proces migracji nie może zaburzyć wzajemnych powiązań logicznych danych . Wzajemne relacje pomiędzy danymi w systemie muszą być zachowane. |
| ZSN.006 | Migracja musi być przeprowadzona w dwóch etapach:   * migracja testowa * migracja produkcyjna. |
| ZSN.007 | Warunkiem możliwości wykonania migracji produkcyjnej jest akceptacja przez Zamawiającego wyników migracji testowej na podstawie raportu z testów migracji przedstawionego przez Wykonawcę. |
| ZSN.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 |

1. **Szkolenie personelu w przypadku zmiany interfejsu graficznego lub przebiegu procesu**

Zamawiający wymaga, by w przypadku zmiany elementów interfejsu graficznego systemu (układ pól, inny układ formularzy itp.) i/lub przebiegu procesu (kolejność wykonywania działań, sposób i kolejność wywoływania formularzy itp. ) ulegną zmianie w wyniku migracji Wykonawca jest zobowiązany w tych obszarach przeszkolić wszystkich użytkowników systemu. Jeżeli w ramach postepowania Wykonawca zaproponuję zmianę producenta oprogramowania systemu HIS szkolenie to powinno dotyczyć całości personelu Zamawiającego użytkującego system HIS. Szkolenia te muszą się zakończyć przed startem produkcyjnym systemu na nowej wydajnej bazie danych po migracji. Poprzez szkolenie personelu Zamawiający rozumie:

* + - 1. Szkolenia dla użytkowników końcowych Szpitalnego Systemu Informatycznego HIS . Szkolenia mają być przeprowadzone w siedzibie Zamawiającego w uzgodnionych terminach tak by nie zakłóciły one bieżącej pracy. Za zgodą Zamawiającego dopuszczalne jest szkolenie poza siedzibą Zamawiającego. W takim przypadku Wykonawca ponosi koszty transportowe i zakwaterowania uczestników szkolenia. Szkolenie musi wyczerpywać zakres funkcjonalności niezbędnych do realizacji zadań wynikających z ról pracownika i nie może być krótsze niż 6 godz. Szkolenia powinny się odbywać w grupach max 12 osobowych. Wykonawca jest zobowiązany zapewnić sprzęt niezbędny do realizacji szkolenia. Zamawiający udostępni Wykonawcy salę szkoleniową na okres szkoleń.
      2. Szkolenia liderów poszczególnych modułów funkcjonalnych. Zamawiający oczekuje, że Wykonawca przeprowadzi pogłębione szkolenie dla użytkowników, którzy jako liderzy modułów będą stanowili wsparcie dla pozostałych użytkowników. Należy przewidzieć, że dla każdego z modułów Zamawiający wyznaczy po 2 liderów. Szkolenie ma trwać minimum 2 dni robocze (dodatkowe poza szkoleniem użytkowników ).

1. **Proces odbiorowy**

W ramach projektu dostarczane będą następujące typy produktów:

* Produkt typu dokument (np. plan migracji, dokumentacja powykonawcza)
* Produkt typu licencje.
* Produkt typu szkolenia
* Produkt typu System (system po migracji)
* Produkt typu Optymalizacja system po migracji

Odbiory poszczególnych produktów/etapów będą przeprowadzone zgodnie z założeniami opisanymi poniżej.

**Odbiór produktu typu dokument**

Zakłada się następujący przebieg procedury odbiorowej produktu typu dokument

* Wykonawca przedstawi zamawiającemu produkty typu dokument w postaci edytowalnego pliku   
  w formacie DOC.
* Zamawiający naniesie swoje uwagi do dokumentu w trybie zmian w postaci dokumentu lub przedstawi jej w postaci odrębnego pliku zawierającego listę uwag i przekaże je Wykonawcy w terminie 5 dni roboczych od dnia przekazania dokumentu (dzień przekazania nie jest uwzględniany w czasie Zamawiającego). Na życzenie Wykonawcy może być na tym etapie zorganizowana telekonferencja wyjaśniająca uwagi Zamawiającego.
* Wykonawca w terminie do 5 dni roboczych jest zobowiązany przekazać Zamawiającemu poprawiony dokument w wersji 2.
* Zamawiający weryfikuje ustosunkowanie się do uwag przez Wykonawcę i ewentualnie przedstawia ponownie swoje uwagi z zastrzeżeniem, że będą się one odnosić do wcześniej zgłoszonych zastrzeżeń lub nowo przedstawionych fragmentów dokumentacji.
* Jeżeli dokument w wersji 2 nie uwzględnia w wystarczającym stopniu uwag Zamawiającego organizowana jest narada jakości, na której Zamawiający wraz z Wykonawcą szczegółowo omawiają możliwość i sposób realizacji uwag oraz określają termin dostarczenia kompletnego dokumentu.
* Po dostarczeniu dokumentu w wersji 3 Zamawiający podejmuje decyzje o jego odbiorze lub odrzuceniu.
* Odbiór produktu typu dokument potwierdza się protokołem odbioru podpisanym przez obie strony
* Zamawiający zastrzega sobie prawo odbioru warunkowego dokumentu, w którym stwierdzono wady ale nie są one na tyle istotne by wstrzymywać przebieg prac projektowych. W takim przypadku w protokole odbioru produktu zawierane są klauzule wskazujące listę wad do usunięcia wraz ze wskazaniem terminu dostarczenia produktu bez wad.
* Zamawiający zastrzega sobie prawo nie wnoszenia uwag do dokumentu i jego odrzucenia w przedstawionej formie jeżeli jakość dokumentu będzie rażąco niska. Poprzez rażąco niską jakość Zamawiający rozumie brak wszystkich elementów wymaganych w SIWZ lub wymaganych na podstawie uzgodnień projektowych lub bardzo niskiej jakości opis tych elementów np. jedno lub kilku zdaniowy bardzo ogólny opis.

**Odbiór produktu typu migracja systemu**

Proces odbioru produktu migracja systemu będzie przebiegał następująco

* Wykonawca po przeprowadzaniu procesu migracji testowej systemu na wydajną bazę danych przedstawia raport z migracji wg szablonu uzgodnionego na etapie analizy przedwdrożeniowej oraz zgłasza gotowość systemu do testów funkcjonalnych. Raport z migracji musi dokumentować poprawność przeprowadzenia procesu migracji testowej w szczególności kompletność przeniesionych danych.
* Testy funkcjonalne wykonywane są na podstawie dokumentacji testowej zatwierdzonej na etapie analizy przedwdrożeniowej z zastrzeżeniem, że dokumentacja ta będzie uwzględniała pełny przebieg kluczowych dla Zamawiającego procesów biznesowych. Jako pełny przebieg rozumie się testowanie zarówno ścieżek pozytywnych jak i negatywnych dla procesów.
* Testy funkcjonalne wykonywane są na dokumentacji testowej opracowanej w ramach etapu I
* Za realizację testów odpowiada Wykonawca przy współudziale Zamawiającego. Zamawiający zastrzega sobie prawo samodzielnej realizacji testów przy lub bez obecności Wykonawcy. W przypadku realizacji testów bez obecności wykonawcy, Zamawiający zobowiązuje się do opisu wykrytych błędów w sposób umożliwiający odtworzenie błędu Wykonawcy (opis powtarzalnej ścieżki dojścia do błędu wraz z zestawem danych testowych). Informacje takie będę przekazane w dokumencie będącym protokołem z sesji odbytych testów systemu przez Zamawiającego.
* Jeżeli w procesie testowania uwidocznione zostały błędy uniemożliwiające odbiór systemu w ramach raportu z testów są one uwidaczniane w tym raporcie wraz z ustaleniem terminu przeprowadzanie II tury testów. Kryteria odbiorowe dla poszczególnych rodzajów testów określone są w rozdziale „Testy”
* Wykonawca w uzgodnionym terminie przedstawia system do II tury testów. W ramach II tury testów weryfikowane są scenariusze dla których stwierdzono występowanie błędów w ramach I tury. Zamawiający zastrzega sobie prawo wykonania testów regresji dla scenariuszy testowych które przebiegły poprawnie w II turze.
* Każda tura testów kończy się raportem z testów przedstawionym Zamawiającemu.
* W przypadku spełniania warunków odbioru testów funkcjonalnych migracji systemu Zamawiający i Wykonawca podpisują protokół odbioru testów funkcjonalnych migracji .
* W przypadku pozytywnej weryfikacji raportu z migracji i testów funkcjonalnych migracji Zamawiający podejmuje decyzję o realizacji migracji produkcyjnej.
* Po przeprowadzaniu uruchomienia produkcyjnego systemu po migracji w terminie nie wcześniej niż po 5 dniach, Wykonawca przedstawi raport z migracji produkcyjnej systemu wg szablonu uzgodnionego na etapie analizy przedwdrożeniowej. Raport będzie zawierał raporty z wydajności systemu sprzed i po migracji systemu. Raporty te powinny umożliwiać porównanie:
  + Czasu zapisu do bazy danych systemu dla tych samych lub porównywalnych danych
  + Czasu odpowiedzi bazy danych na zapytania systemu dla tych samych lub porównywalnych zapytań.
* Na podstawie raportu z migracji produkcyjnej systemu Zamawiający dokona odbioru migracji systemu poprzez podpisanie protokołu odbioru.
* Odbiór migracji systemu zostanie potwierdzony protokołem odbioru podpisanym przez obie strony
* Zamawiający zastrzega sobie prawo odbioru warunkowego migracji systemu, w którym stwierdzono wady ale nie są one na tyle istotne by wstrzymywać przebieg prac projektowych. W takim przypadku w protokole odbioru migracji zawierane są klauzule wskazujące listę wad do usunięcia wraz ze wskazaniem terminu dostarczenia produktu bez wad.

**Odbiór produktu typu szkolenia**

Produkt szkolenia będzie odbierany każdorazowo przekazanych do akceptacji Zamawiającego oraz listy obecności uczestników szkolenia. Pracownicy Zamawiającego mają obowiązek podpisania listy obecności na szkoleniu. Wykonawca odpowiada za zorganizowanie sprzętu niezbędnego do przeprowadzenia szkolenia. Zamawiający udostępni Wykonawcy salę szkoleniową z dostępem do sieci internet. Wykonawca zobowiązany jest zapewnić każdemu uczestnikowi komplet materiałów szkoleniowych minimum w formie plików na nośniku elektronicznym lub wskazania lokalizacji z której można takie pliki pobrać samodzielnie. Na podstawie materiałów szkoleniowych i listy obecności podpisywany jest przez strony protokół odbioru szkolenia.

**Odbiór produktów typu licencje**

Odbiór produktów typu licencje będzie następował na podstawie protokołu przekazania licencji po wcześniejszym sprawdzeniu kompletności dostawy.

**Odbiór produktu typu Optymalizacja system po migracji**

Pomiaru dokonujemy dla produkcyjnej wersji systemu medycznego w stanie po optymalizacji migracji

**Odbiór etapu / umowy**

Dla każdego z etapów Projektu określona jest lista produktów dostarczanych w ramach etapu. Odbiór etapu może nastąpić jedynie jeżeli odebrane są wszystkie produktu dla danego etapu minimum na poziomie odbioru warunkowego z zastrzeżeniem, że w momencie odbioru Etapu II wszystkie produkty poprzedniego etapu powinny uzyskać status odbioru bezwarunkowego.

1. **Testy**

W ramach realizacji przedmiotu umowy Wykonawca zobowiązany jest przeprowadzić zestaw testów potwierdzających poprawność wykonania migracji. W skład testów realizowanych w ramach procesu migracji systemu HIS 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 w punkcie „Opis stanu bieżącego”.

**Dokumentacja testowa**

Dokumentacja testowa zostanie opracowana przez Wykonawcę na etapie analiz przedwdrożeniowej. Dokumentacja testowe będzie obejmowała następujące rodzaje dokumentów:

* Plan testów
* Scenariusz testowe
* Przypadki testowe
* Dane do testów

Plan i scenariusze będą zgodne z powszechnie stosowanymi zasadami i praktykami.

Plan testów określać będzie w szczególności:

* Ogólne zasady przeprowadzania testów,
* opis środowiska testowego;
* kolejność wykonywania scenariuszy testowych;
* klasyfikację wykrytych problemów testowych;
* kryteria sukcesu dla poszczególnych kategorii testów.

Scenariusze będą zapewniać pokrycie wszystkich procesów systemu HIS kluczowych dla działalności Zamawiającego. Każdy scenariusz określać będzie:

* dane, które muszą być wprowadzone do systemu przed uruchomieniem scenariusza;
* kolejność czynności, wykonywanych w czasie testu oraz dane, wprowadzane do systemu w czasie testu;
* oczekiwaną reakcję systemu na wykonane czynności i wprowadzone dane.

Przypadki testowe i dane testowe w tym wszelkie materiały eksploatacyjne dostarczone będą przez Wykonawcę. Zamawiający zobowiązany jest do współpracy z Wykonawcą przy przygotowywaniu scenariuszy testowych i danych testowych, przeprowadzaniu testów oraz przygotowaniu wyników testów.

Zamawiający dopuszcza przeprowadzenie testów automatycznych, o ile w planie testów zostanie wyspecyfikowany zakres tych testów i uzyska on akceptację Zamawiającego.

Testy będą przeprowadzone przez w terminie przewidzianym w harmonogramie, zgodnie z zaakceptowanym planem testów.

Testy zostaną wykonane z użyciem środowiska testowego migracji chyba, że plan testów będzie przewidywał inaczej, na bazie reprezentatywnej próbki danych eksploatacyjnych. Zakres testów nie może wykraczać poza merytoryczny zakres projektu. Test może zostać przerwany, jeżeli z jakiejkolwiek przyczyny nie może być kontynuowany (np. poważny błąd w oprogramowaniu lub awaria systemu). Test taki powinien zostać powtórzony lub kontynuowany w innym terminie po obustronnym uzgodnieniu.

W ramach procesu testowania mogą wystąpić następujące kategorie błędów

|  |  |
| --- | --- |
| **Poziom istotności** | **Opis** |
| A/Krytyczny | Zatrzymanie działania Produktu lub błąd uniemożliwiający realizację kluczowego procesu w tym także obniżenie wydajności, które w praktyce uniemożliwia jego realizację i nie jest możliwe wskazanie obejścia błędu. |
| B /Wysoki | Zatrzymanie działania Produktu lub realizację kluczowego procesu w tym także obniżenie wydajności, które w praktyce uniemożliwia jego realizację ale jest możliwe wskazanie obejścia błędu. Obejście umożliwia weryfikację funkcjonalności występujących „za” błędem. |
| C /Średni | Zakłócenie pracy Produktu wpływające na weryfikację poprawności przebiegu kluczowego procesu |
| D/Niski | Zakłócenie pracy Produktu niewpływające na weryfikację poprawności przebiegu kluczowego procesu , w tym błędy kosmetyczne interfejsu. |

**Kryteria Akceptacji Testów**

**Kryteria akceptacji dla scenariuszy i przypadków testowych**

Wynik testu dla Scenariusza Testowego uznaje się za pozytywny, gdy wyniki testów dla wszystkich Przypadków Testowych zawartych w Scenariuszu Testowym są pozytywne. Wynik testu dla Scenariusza Testowego uznaje się za negatywny, gdy wynik testu dla któregokolwiek Przypadku Testowego zawartego w Scenariuszu testowym jest negatywny.

Wynik testu dla Przypadku Testowego uznaje się za pozytywny, gdy opis oczekiwanego rezultatu zamieszczony w polu „Oczekiwany wynik" jest ‘zgodny’ z faktycznie uzyskanym wynikiem po zakończeniu Przypadku Testowego.

Wynik testu dla Przypadku Testowego uznaje się za negatywny, gdy opis oczekiwanego rezultatu zamieszczony w polu „Oczekiwany wynik" jest ‘nie zgodny’ z faktycznie uzyskanym wynikiem po zakończeniu Przypadku Testowego. W przypadku, gdy występująca niezgodność jest wynikiem błędnie opisanego Przypadku Testowego, wówczas wynik testu może być uznany za prawidłowy, a błędny opis Przypadku Testowego musi zostać poprawiony przez Wykonawcę. Sytuacja taka musi znaleźć odzwierciedlenie w raporcie z Testów Akceptacyjnych.

**Kryteria zakończenia testów sukcesem**

Testy są wykonane na podstawie Scenariuszy Testowych zaakceptowanych przez Zamawiającego.

Testy uznaje się za zakończone z sukcesem, gdy:

* przeprowadzono testy z wykorzystaniem zaplanowanych Scenariuszy Testowych,
* brak niezakończonych Scenariuszy Testowych z powodu wystąpienia Incydentu/ów z klasą istotności B/Wysoki, C/Średni i D/Niski, których liczba wykracza poza dopuszczalny limit
* na moment zakończenia Testów Akceptacyjnych brak jest Incydentów z klasą istotności A/Krytyczny

W przypadku wystąpienia Incydentu, który uniemożliwia wykonanie wszystkich zaplanowanych przypadków Testowych i/lub Scenariuszy Testowych, a który nie wynika z winy Wykonawcy, wówczas zakres testów może zostać zmieniony (wyłączenie przypadków i/lub scenariuszy) na podstawie decyzji podjętej przez Zamawiającego.

W przypadku Scenariuszy Testowych zakończonych negatywnie, w których wystąpiły Incydenty o klasie istotności B/Wysoki, C/Średni lub D/Niski, wynik ich zakończenia może zostać uznany za pozytywny na podstawie decyzji podjętej przez Kierownika Projektu ze strony Zamawiającego.

Testy uznaje się za zakończone z wynikiem negatywnym, gdy po ich zrealizowaniu otrzymano następujące wyniki:

* istnieje przynajmniej jeden niezakończony Scenariusz Testowy z powodu wystąpienia Incydentu/ów z klasą istotności A/Krytyczny,
* istnieją niezakończone Scenariusze Testowe z powodu wystąpienia Incydentu/ów z klasą istotności B/Wysoki i C/Średni, których liczba wykracza poza dopuszczalny limit, w takim przypadku Scenariusze te nie mogą zostać uznane za zakończone pozytywnie.

W przypadku zakończenia Testów z wynikiem negatywnym, zostanie ustalony plan powtórzenia testów. Wybór scenariuszy do II tury testów zostanie przeprowadzony według następujących zasad:

* Scenariusze Testowe, które otrzymały wynik negatywny z powodu wystąpienie Incydentu/ów.
* Scenariusze Testowe dla funkcjonalności powiązanych z funkcjonalnością Scenariusza Testowego, w którym wystąpiły Incydenty.

Zamawiający zastrzega sobie prawo przeprowadzenia testów regresji dla scenariuszy z wynikiem pozytywnym.

**Kryteria akceptacji testów funkcjonalnych**

Dopuszczalna liczba otwartych Incydentów na zakończenie Testów Funkcjonalnych migracji

|  |  |
| --- | --- |
| Kategoria błędu | Dopuszczalna liczba przypadków testowych  z błędem |
| A/Krytyczny | 0 |
| B/Wysoki | 0 |
| C/Średni | 2 |
| D/Niski | 10 |

**Kryteria akceptacji testów wydajnościowych**

Minimalny średni czas reakcji Systemu wynosi 1 sekunda.

**Kryteria akceptacji testów integracji**

Raport testów ma wykazać, że generowane z nowej wersji systemu pliki wymiany (pliki XML, dokumenty HL7, widoki na bazie danych) posiadają identyczną strukturę i zawartość dla takiego samego zakresu danych jak w dotychczas używanym systemie HIS.

..........................dnia ................. 2018 roku ................................................................

podpis osoby(osób) uprawnionych

do reprezentowania Wykonawcy