

Sprawa nr 23/2020

Szczegółowy Opis Przedmiotu Zamówienia

„Dostawa sprzętu komputerowego oraz oprogramowania niezbędnego do realizacji e-USług wraz z usługą wdrożenia”

Spis treści

Wstęp	3
Ogólny zarys projektu	3
Słownik pojęć	4
Wymagania ogólne	6
Zakres 1 – Dostawa sprzętu i oprogramowania systemowego	7
Serwery	7
Macierz dyskowa - rozbudowa.....	8
Serwery – rozbudowa.....	8
Serwer NAS.....	8
Stanowiska robocze stacjonarne	9
Klawiatury z czytnikiem karty chipowej.....	10
Drukarki i karty chipowe.....	10
Modernizacja infrastruktury sieci teleinformatycznej.....	11
Przełączniki sieciowe TOR.....	11
Przełączniki sieciowe Access	12
Przełączniki sieciowe FC – 2 kpl.	15
Warunki ogólne	17
Parametry minimalne szafek RACK – 8 kpl.	18
Szafa RACK do serwerowni	18
Zabezpieczenie e-Uслуг	19
Firewall – UTM – 1 szt.....	19
Instalacja elementów w modernizowanej serwerowni zapasowej.....	25
System archiwizacji danych obrazowych	30
System monitorowania i zarządzania infrastrukturą serwerów.....	45
Licencje	47
Zakres 2 – Konfiguracja i uruchomienie sprzętu oraz oprogramowania systemowego	48
Serwery	48
Macierz dyskowa.....	48
Zabezpieczenie e-Uслуг	48
Firewall – UTM.....	48
Architektura Domeny	48
Architektura RDP	49
Usługi wspomagające	49
Zakres 3 – Przygotowanie i dostarczenie dokumentacji projektowej oraz powykonawczej	50
Gwarancja i wsparcie	51

Wstęp

Niniejszy dokument stanowi Szczegółowy Opis Przedmiotu Zamówienia (dalej SzOPZ lub OPZ) w zakresie dostawy i wdrożenia sprzętu oraz oprogramowania służącego uruchomieniu i zabezpieczeniu działania e-Uслуг w Szpitalu. Prezentowany poniżej ogólny opis organizacji serwerowni stanowi jedynie zarys całego rozwiązania – Wykonawca może zaproponować swoją wersję organizacji serwerowni o ile proponowane rozwiązanie gwarantowało będzie wyższy poziom bezpieczeństwa i lepsze wykorzystanie mocy obliczeniowej serwerów fizycznych przy czym nie może udostępniać mniejszej szybkości działania. Wszystkie parametry techniczne określone w niniejszym OPZ określają minimalne lub maksymalne (zgodnie z opisem) wymagania stawiane oferowanym urządzeniom i oprogramowaniu.

Ogólny zarys projektu

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

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

Niniejszy Przedmiot Zamówienia wykonany będzie w następujących terminach:

Lp.	Opis prac wykonanych w ramach zakresu	Maksymalny czas realizacji (dni robocze)
Zakres 1	Dostawa sprzętu i oprogramowania systemowego.	50 dni (od udzielenia zamówienia)
Zakres 2	Konfiguracja i uruchomienie sprzętu oraz oprogramowania systemowego.	90 dni (od udzielenia zamówienia)
Zakres 3	Przygotowanie oraz dostarczenie dokumentacji projektowej i powykonawczej.	Maksymalnie na dzień zakończenia realizacji zamówienia

Słownik pojęć

Na potrzeby niniejszego postępowania stosuje się następujące pojęcia i definicje:

1. **Dysfunkcja** – zbiorcze określenie dla nieprawidłowości rozumianych jako niezgodność z Dokumentacją lub też uciążliwość w pracy z Systemem.
2. **Kategoria Dysfunkcji** – kategoria, do której kwalifikowane jest Zgłoszenie Serwisowe dotyczące Dysfunkcji. Opisane szczegółowo w Załączniku nr 1 do niniejszego OPZ.
3. **Prace Serwisowe** – działania Wykonawcy mające na celu realizację Zgłoszenia Serwisowego.
4. **Naprawa** – modyfikacja Systemu usuwająca Dysfunkcję Systemu.
5. **Obejście** – tymczasowe rozwiązanie pozwalające na prawidłowe wykorzystanie oprogramowania bez usuwania wykrytego błędu przy zachowaniu integralności bazy danych.
6. **Realizacja Zgłoszenia Serwisowego** – zakończenie Prac Serwisowych, w wyniku których przywrócono Stan Funkcjonalności.
7. **Analiza** – dokumenty opracowane przez Wykonawcę, mające na celu doprecyzowanie sposobu realizacji wymagań Zamawiającego, zasad i metod realizacji Umowy oraz wskazanie i szczegółowe opisanie Produktów;
12. **Baza Danych** – zbiór wszystkich danych zewidencjonowanych za pomocą Systemu.
13. **Czas Roboczy** – czas pracy liczony w Dni Robocze, w którym świadczona jest pomoc telefoniczna przy eksploatacji Systemu.
14. **Dzień Roboczy** – dzień kalendarzowy od poniedziałku do piątku z wyłączeniem świąt i dni ustawowo wolnych od pracy.
15. **Dokumentacja** – dokument papierowy lub elektroniczny opisujący System i zasady użytkowania Systemu. Wszelka dokumentacja sporządzona przez Wykonawcę dostarczona i modyfikowana w wyniku realizacji umowy.
16. **Godziny robocze** – czas pracy liczony w Dni Robocze w godzinach 7:30 – 15:30.
17. **Konsultant** – osoba fizyczna posiadająca odpowiednie kwalifikacje uprawniające do realizowania Serwisu.
18. **Pomoc Telefoniczna** – świadczenie konsultacji telefonicznej dotyczące szeroko pojętej eksploatacji Systemu.
19. **Procedura** – schemat postępowania w jaki winien być realizowany określony fragment Przedmiotu Umowy.
20. **Serwer** – sprzęt komputerowy, na którym zainstalowana jest baza danych lub aplikacje wykorzystywane przez System.
21. **Serwis** – usługa o charakterze technicznym, organizacyjnym, doradczym i szkoleniowym, przeznaczona do zapewnienia stabilnej pracy Systemu.
22. **Stan Funkcjonalności** – stan Systemu, w którym nie występują Dysfunkcje.
23. **Upgrade** – nowa wersja Systemu związana ze stworzeniem nowej funkcjonalności.
24. **Update** – aktualizacja Systemu w wyniku zmian przepisów, związanych bezpośrednio i pośrednio z systemem ochrony zdrowia, w zakresie tej samej wersji Systemu.
25. **Wdrożenie** – opisane Umową świadczenia Wykonawcy mające na celu uruchomienie systemu serwerów wirtualnych w trybie HA.
26. **Wersja** – okresowa Publikacja Systemu uwzględniająca Naprawy i zmiany dokonane w okresie od poprzedniej Publikacji Systemu. Wydanie Wersji obejmuje również opis nowej Funkcjonalności Systemu.

- 27. **Zgłoszenie Serwisowe** – Dysfunkcja, o której Wykonawca został powiadomiony drogą mailową.
- 28. **Administrator** – (ASI) Użytkownik konfigurujący i zarządzający Systemem i Infrastrukturą.
- 29. **Architektura systemu teleinformatycznego** – opis składników systemu teleinformatycznego, powiązań i relacji pomiędzy tymi składnikami.
- 30. **Czas dostarczenia rozwiązania** - Okres czasu od wysłania Zgłoszenia do usunięcia przyczyny problemu lub zastosowania Obejścia.
- 31. **Dostępność** – właściwość określająca, że zasób systemu teleinformatycznego jest możliwy do wykorzystania na żądanie, w założonym czasie, przez podmiot uprawniony do pracy w systemie teleinformatycznym .
- 32. **Integralność** – właściwość polegająca na tym, że zasób systemu teleinformatycznego nie został zmodyfikowany w sposób nieuprawniony .
- 33. **Moduł systemu** – kompletny zestaw narzędzi informatycznych obejmujących wszystkie warstwy architektury systemu, który dostarcza aplikację przeznaczoną dla użytkownika końcowego do realizacji określonych dziedzin działalności Zamawiającego.
- 34. **Oprogramowanie** – Każde dostarczane oprogramowanie niezbędne do działania Systemu.
- 35. **System** – łączne określenie dla oprogramowania i sprzętu – występującego u Zamawiającego, objętego wdrożeniem oraz umową serwisową z Wykonawcą, bez względu na nazwę handlową. Obejmujący platformę systemowo-sprzętową, oprogramowania niezbędne do działania e-Usług realizowanych w niniejszym zamówieniu dostarczanych przez Wykonawcę.
- 36. **System zewnętrzny** - Każdy System informatyczny niebędący przedmiotem Zamówienia a oddziaływujący lub komunikujący się z przedmiotem zamówienia.
- 37. **Użytkownik** - Osoba, która jest pracownikiem Zamawiającego, posiada swój unikalny login i hasło.
- 38. **Wykonawca** – wybrany w drodze zamówienia publicznego podmiot realizujący niniejszy przedmiot zamówienia.
- 39. **Zamawiający** – Uniwersytecki Szpital Kliniczny w Olsztynie
- 40. **Zdalny dostęp** – możliwość realizacji usług wsparcia, wdrożenia i gwarancji związanych z systemem z dowolnego miejsca za pośrednictwem bezpiecznego połączenia internetowego.

Wymagania ogólne

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

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

System musi umożliwiać definiowanie dowolnej ilości użytkowników.

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

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

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

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

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

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

Zakres 1 – Dostawa sprzętu i oprogramowania systemowego

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

Serwery

Serwery aplikacyjne – 3 kpl.

Parametr	Wymagania minimalne
Obudowa	RACK 19 cali (wraz z szynami montażowymi oraz ramieniem do prowadzenia kabli, umożliwiającymi serwisowanie serwera w szafie rack bez odłączania urządzenia), maksymalnie 2U
Procesor	Dwa procesory. Płyta główna wspierająca zastosowanie procesorów min. do 24 rdzeniowych. Min. 12-rdzeniowe ¹ klasy x86 - 64 bity, umożliwiające osiągnięcie wyniku min. 130 w teście SPECrate2017_int_base, dostępnym na stronie www.spec.org dla dwóch procesorów.
Dysk twardy	System wirtualizacji zainstalowany na nośnikach pracujących w trybie RAID-1, bez konieczności użycia dysków twardych. Wykonawca musi dostarczyć nośniki danych (min. 8GB każdy). Zastosowane rozwiązanie musi posiadać gwarancję producenta serwera.
Kontroler	Serwer wyposażony w 2-portowy kontroler sprzętowy FC16 wraz z kompatybilnymi wkładkami
Pamięć operacyjna	min. 384 GB DDR4 w modułach o pojemności 16 lub 32GB każdy.
Sloty rozszerzeń	2 aktywne gniazda PCI-Express generacji 3, w tym min. 1 slot x16
Interfejsy sieciowe	Minimum 2 wbudowane porty SFP+ min. 10Gb/s (wraz z wkładkami), min. 2 porty RJ-45 min. 1GB/s, min. jeden port zarządzania.
Karta graficzna	Zintegrowana karta graficzna
Porty	Min.: 3 x USB (co najmniej jeden z przodu obudowy); 1x VGA;
Chłodzenie	Zestaw redundantnych wentylatorów.
Karta/moduł zarządzający	Niezależna od systemu operacyjnego, zintegrowana z płytą główną serwera lub jako dodatkowa karta w slotcie PCI Express, posiadająca minimalną funkcjonalność: <ul style="list-style-type: none">• monitorowanie podzespołów serwera: temperatura, zasilacze, wentylatory, procesory, pamięć RAM, kontrolery macierzowe i dyski(fizyczne i logiczne), karty sieciowe• wsparcie dla agentów zarządzających oraz możliwość pracy w trybie bezagentowym – bez agentów zarządzania instalowanych w systemie operacyjnym z generowaniem alertów SNMP• dostęp do karty zarządzającej możliwy poprzez:<ul style="list-style-type: none">– dedykowany port RJ45– przez współdzielony port zintegrowanej karty sieciowej serwera• dostęp do karty możliwy<ul style="list-style-type: none">– z poziomu przeglądarki webowej (GUI)– z poziomu linii komend– poprzez interfejs IPMI 2.0• wbudowane narzędzia diagnostyczne

¹ Parametr ważny z uwagi na docelowe wykorzystanie serwerów

	<ul style="list-style-type: none"> • zdalna konfiguracji serwera (BIOS) i instalacji systemu operacyjnego • wbudowany mechanizm logowania zdarzeń serwera i karty zarządzającej w tym włączanie/wyłączanie serwera, restart, zmiany w konfiguracji, logowanie użytkowników • przesyłanie alertów poprzez e-mail oraz przekierowanie SNMP • obsługa zdalnego serwera logowania (remote syslog) • wirtualna zdalna konsola, tekstowa i graficzna, z dostępem do myszy i klawiatury i możliwością podłączenia wirtualnych napędów FDD, CD/DVD i USB i wirtualnych folderów • monitorowanie zasilania oraz zużycia energii przez serwer w czasie rzeczywistym • zdalna aktualizacja oprogramowania (firmware) • możliwość równoczesnej obsługi przez min. 2 administratorów • wsparcie dla Microsoft Active Directory • obsługa SSL i SSH • wsparcie dla IPv4 oraz IPv6, obsługa SNMP v3 • możliwość autokonfiguracji sieci karty zarządzającej (DHCP)
Gwarancja	Z czasem reakcji NBD. Usługa wsparcia technicznego musi być świadczona przez serwis producenta oferowanych urządzeń.

Macierz dyskowa - rozbudowa

Rozbudowa macierzy dyskowej Zamawiającego (EMC Unity 300) o dodatkowe dyski – min. 8 szt. NLSAS 12Gb/s, min. 6TB, prędkość obrotowa min. 7200 rpm, bufor: min. 128 MB. Oferowane dyski muszą znajdować się na liście dysków kompatybilnych z macierzą.

Serwery – rozbudowa

Dodatkowy RAM, karty FC – zestaw.

Zamawiający posiada obecnie 4 serwery (2x Dell R620 oraz 2x Dell R630), które zamierza rozbudować o pamięć RAM oraz dodatkowe karty sieciowe:

- 4x Dual Port 16Gb Fibre Channel HBA, LowProfile - zestaw
- 4x Dual Port 10Gb DA/SFP+ Server Adapter, LowProfile - zestaw
- 8x Przełącznik 10GbE SR SFP+ zgodny ze standardami 10Gb i 1Gb do serwerowych kart sieciowych
- 24x Memory Upgrade - 32GB - 4Rx4 DDR3 RDIMM 1333MHz
- 24x Memory Upgrade - 32GB - 2Rx4 DDR4 RDIMM 2133MHz

Serwer NAS

Sprzętowy serwer NAS – 1 kpl.

Parametr	Wymagania minimalne
Obudowa	Rack max. 3U, szyny montażowe w zestawie
Pamięć RAM	min. 8 GB RAM – możliwość rozszerzenia do min. 32 GB

Dyski zainstalowane	12 dysków przeznaczonych do pracy w serwerach NAS o pojemności min. 4TB każdy. Cache SSD M.2 min 32 GB.
Interfejsy sieciowe	Min: 4 x Gigabit; Min. 2 x 10GbE SFP+ z odpowiednimi wkładkami 10Gb
Porty	Min. 2x USB w tym min. 1x USB 3.0
Obsługa RAID	Pojedynczy dysk, JBOD, RAID 0, 1, 5, 6, 10. Możliwość skonfigurowania Global Spare Disk.
Funkcje RAID	Możliwość zwiększania pojemności i migracja między poziomami RAID online.
Wspierane systemy operacyjne	Microsoft Windows Server 2016, Linux, Vmware
Protokoły	CIFS, AFP, NFS, FTP, iSCSI, SSH, SNMP
Wirtualizacja	Możliwość uruchomienia maszyn wirtualnych bezpośrednio na macierzy bez konieczności posiadania zewnętrznych wirtualizatorów
iSCSI	Wbudowany inicjator i target iSCSI
Replikacja	Replikacja między urządzeniami w czasie rzeczywistym
Kontroler domeny	Możliwość podłączenia do kontrolera domeny Microsoft i obsługi uprawnień do udziałów na poziomie grup domeny
Liczba iSCSI LUN	Min. 64
Liczba udziałów	Min. 100
Liczba jednoczesnych połączeń	Min. 250
Zasilanie	Redundantne 2 szt.
Chłodzenie	Min 4 wentylatory

Stanowiska robocze stacjonarne

Terminal – 50 kpl.:

Parametr	Wymagania minimalne
Procesor/Chipset	Odpowiednie dla urządzeń typu terminal, min. 600 pkt. w teście PassMark - CPU Mark
Karta graficzna	Odpowiednie dla urządzeń typu terminal, min. 100 pkt. w teście PassMark - G3D Mark
Ekran	min. 21 cali, Full HD 1920 x 1080 @ 60 Hz, proporcje: 16:9, Powłoka antyodblaskowa/matowa
System operacyjny	Dostosowany do urządzeń typu cienki klient w najnowszej wersji
Wspierane protokoły	min.: Citrix ICA, HDX 3D & 3D Pro, Microsoft RDP 8.0
Pamięć masowa	Min. 8GB
Pamięć RAM	Min. 2GB DDR3
Sieć	10/100/1000 Ethernet, możliwość dołączenia dedykowanej wewnętrznej karty bezprzewodowej – 802.11 a/b/g/n
Porty	min. 4 USB 2.0, 1 RJ45, 1 złącze do podłączenia zewnętrznego komputera PC, 1 DisplayPort/HDMI (do podłączenia drugiego monitora), kamera HD, wbudowane głośniki i mikrofon

Akcesoria w zestawie	Mysz przewodowa laserowa USB, Podstawka stała lub z regulacją wysokości, złącze VESA. <u>Klawiatura przewodowa USB z czytnikiem kart chipowych.</u>
Moc pobierana	<65W
Zasilanie:	220-240V @ 50Hz
Waga	max. 7kg
Temperatura pracy	min. 10° do 40° C
Certyfikaty	TÜV-GS, EN 60950 RF Interference: FCC Class B, Ergonomics CE, VCCI, RoHS Compliant lub równoważne
CD/DVD	napęd DVD-RW/BD-RW USB

Klawiatury z czytnikiem karty chipowej

Klawiatury z czytnikiem kart inteligentnych – 230 szt.

Parametr	Wymagania minimalne
Typ	Klasyczna
Łączność	Przewodowa
Interfejs	USB
Rodzaje wejść / wyjść	USB 2.0 – min. 1 szt
Kolor	Czarny
Długość przewodu	min. 1,8 m
Obsługiwane systemy	Windows, Linux
Dodatkowe informacje	<u>Wbudowany czytnik kart inteligentnych zgodny z dostarczonymi kartami inteligentnymi</u> , Podpórka pod nadgarstki, Odporność na zachłapanie

Drukarki i karty chipowe

Zestaw Drukarka kart chipowych (1 kpl.) + karty chipowe (1000 szt.)

Parametr	Wymagania minimalne
Rodzaj druku:	termotransferowy
Typ zadruku:	Jednostronny i dwustronny
Wydruk:	Monochromatyczny i kolorowy
Dostępne interfejsy:	min. USB
Dodatkowe opcje:	koder kart chipowych
Grubość kart:	min. 30 mil (ok. 0,75mm)
Moduł RFID:	TAK
Pojemność podajnika:	Min. 100
Rozdzielczość:	Min. 300 dpi
Prędkość druku:	Min. 100 kart/h
Waga:	Max 8 kg

Do drukarki należy dołączyć min. 2 komplety zestawów materiałów pozwalających na uruchomienie drukarki i zadrukowanie min. 1000 kart chipowych dwustronnie (przy założeniu pokrycia 5% powierzchni karty każdym kolorem).

Specyfikacja kart chipowych:

- Pamięć EEPROM min. 64 kB
- RSA do 2048 bitów, AES, 3DES
- Możliwość integracji ze środowiskiem PKCS#11 i Microsoft® CSP
- Możliwość uruchomienia usługi podpisu elektronicznego, uwierzytelniania i szyfrowania
- Common Criteria EAL 4+ i EAL 5+ zgodne z SSD typ 2 i 3
- Wykonana z materiału o podwyższonej trwałości PET-F
- Obsługa Middleware PKCS#11 i CSP dla środowisk: Windows, Mac, Linux
- Interfejs bezstykowy Mifare 1kb (13,56 MHz)
- **Karta dualna**
- Karta biała – do zadruku.

Modernizacja infrastruktury sieci teleinformatycznej

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

Przełączniki sieciowe TOR

Przełączniki rdzeniowe – 2 kpl.

Parametr	Wymagania minimalne
Obudowa	1U do montażu w szafie RACK 19" wraz z kompletem szyn/uchwytów montażowych
Porty	48xSFP+, 2xQSFP+ port konsoli, porty do stakowania, port zarządzania, port USB
Wydajność przełącznika	Min. 4GB RAM, min. 12MB buforu pakietów, Min. 1.6Tbps, 1.2Gpps, opóźnienie przełączania max. 900 ns
Zasilanie	Zasilacze redundantne, hot-swap, max 400W
Chłodzenie	Redundantne wentylatory, hot-swap
Obsługiwane protokoły warstwy 2	802.1D Compatible 802.1p L2 Prioritization 802.1Q VLAN Tagging 802.1s MSTP 802.1w RSTP 802.1t RPVST+ 802.3ad Link Aggregation with LACP VLT (Virtual Link Trunking) VLT Enhancements VLT Proxy Gateway RVPST over VLT iSCSI over VLT RSPAN over VLT 802.1Qbb Priority-Based Flow Control Data Center Bridging eXchange (DCBx)
Obsługiwane protokoły IP	IPv4 : ICMP, ARP, Proxy ARP, DNS (client), Ethernet Transmission, Path MTU Discovery, NTPv4, CIDR, IP Fragment Filtering, DHCP (server and relay), VRRP, DHCP Option 82 (Relay),

	IPv6: Stateless Address AutoConfig, ICMPv6, Ethernet Transmission, Jumbo grams, Global Unicast Address Format, Transmission of IPv6 Packets over Ethernet Networks, IPv6 Router Alert Option, IPv6 Scoped Address Architecture, IPv6 Addressing Architecture
Zarządzanie	SNMPv1/2 SSHv2 FTP, TFTP, SCP Syslog RADIUS 802.1X Netconf APIs CLI sFlow lub inny kompatybilny protokół monitorowania
Akcesoria	Kable zasilające, wkładki SFP+ jednomodowe (lub w razie konieczności wielomodowe – należy dostosować do dostarczanych urządzeń-serwerów) min. 1,3km – obsadzone wszystkie porty, szyny do montażu w szafie Rack, śruby mocujące.

Przełączniki sieciowe Access

Przełączniki dostępne 48P – 2 kpl.

Parametr	Wymagania minimalne
Obudowa	Do montażu w szafie Rack 19", o wysokości nie więcej niż 1U, wraz z kompletem odpowiednich szyn, wyposażona w zintegrowany zasilacz HotPlug.
Porty	Minimum 48 portów GigabitEthernet w standardzie BaseT minimum 2 zintegrowane porty 10Gb Ethernet SFP+, minimum 2 porty do łączenia przełączników w stos, minimum 1 port USB do konfiguracji przełącznika, 1 port RJ45 do portu konsoli wraz z odpowiednim kablem RJ45-RS232 lub USB.
Wydajność przełącznika	minimum 32000 adresów MAC switch fabric capacity min. 200 Gbps (w trybie full-duplex) forwarding rate min. 160 Mbps pamięć flash min. 256MB bufor pamięci dla pakietów minimum 4MB pamięć procesora minimum 1GB obsługa minimum 2000 wirtualnych sieci możliwość połączenia w stos do min. 8 urządzeń tego samego typu przepustowość stosu minimum 84 Gbps full duplex wsparcie dla agregacji LACP (802.3ad) - minimum 32 grupy do 8 portów na grupę
Zgodność z protokołami	802.1AB LLDP 802.1D Bridging, Spanning Tree 802.1p Ethernet Priority (User Provisioning and Mapping)

	802.1Q VLAN Tagging, Double VLAN Tagging, GVRP 802.1S Multiple Spanning Tree (MSTP) 802.1v Protocol-based VLANs 802.1W Rapid Spanning Tree (RSTP) BPDU guard, BPDU filtering 802.1X Network Access Control, Auto VLAN 802.2 Logical Link Control 802.3ac Frame Extensions for VLAN Tagging 802.3ad Link Aggregation with LACP 802.3AX LAG Load Balancing 802.3az Energy Efficient Ethernet (EEE) 802.3x Flow Control ANSI LLDP-MED (TIA-1057) MTU 9216 B
Zarządzanie siecią i bezpieczeństwo	Funkcjonalność warstwy 3: RIPv2, QoS. 1155 SMIv1 1157 SNMPv1 1212 Concise MIB Definitions 1213 MIB-II 1215 SNMP Traps 1492 TACACS+ 1573 Evolution of Interfaces 1867 HTML/2.0 Forms with file upload extensions 1901 Community-based SNMPv2 1907 SNMPv2 MIB 1908 Coexistence between SNMPv1/v2 2068 HTTP/1.1 2233 Interfaces Group using SMIv2 2246 TLS v1 2295 Transport Content Negotiation 2296 Remote Variant Selection 2346 AES Cipher suites for TLS 2576 Coexistence between SNMPv1/v2/v3 2580 Conformance Statements for SMIv2 2666 Identification of Ethernet chipsets 2818 HTTP over TLS 2819 RMON MIB (groups 1, 2, 3, 9) 2856 Text Conv. For High Capacity Data Types 2865 RADIUS 2866 RADIUS Accounting 2868 RADIUS Attributes for Tunnel Prot. 3410 Internet Standard Mgmt. Framework 3411 SNMP Management Framework 3412 Message Processing and Dispatching 3413 SNMP Applications 3414 User-based security model 3415 View-based control model 3416 SNMPv2 3417 Transport Mappings

	3418 SNMP MIB 3580 802.1X with RADIUS 4251 SSH Protocol 4252 SSH Authentication 4253 SSH Transport 4254 SSH Connection Protocol 4419 SSH Transport Layer Protocol 4521 LDAP Extensions 6101 SSL 6398 IP Router Alert (Obsoletes RFC 2665)
Warunki pracy	- Wydajność pracy zasilaczy na poziomie min. 80% - temperatura pracy w zakresie od 0 do 45°C - wilgotność dla trybu pracy do 80%
Funkcjonalność	Musi wspierać funkcjonalność wirtualnej agregacji portów umożliwiającą: - terminowanie pojedynczej wiązki EtherChannel/LACP wyprowadzonej z urządzenia zewnętrznego (serwera, przełącznika) na 2 niezależnych urządzeniach - budowę topologii sieci bez pętli z pełnym wykorzystaniem agregowanych łączy - umożliwiać wysokodostępny mechanizm kontroli dla 2 niezależnych urządzeń
Certyfikaty i standardy	Zamawiający wymaga aby oferowany przełącznik: - posiadał deklarację CE - był zgodny z standardem RoHS lub równoważnym
Komponenty dodatkowe	Do każdego przełącznika należy dostarczyć komponenty kompatybilne z przełącznikami: - 4 x wkładki 10GbE SFP+ jednomodowe
Gwarancja	Gwarancja czasu życia (Limited Lifetime warranty) obejmująca: - przełącznik - zasilacze i wiatraki - bezterminowy dostęp do nowych wersji oprogramowania

Przełącznik dostępowy 24p – 1 kpl.

Parametr	Wymagania minimalne
Obudowa	Do montażu w szafie RACK (wraz z szynami/uchwyty), wysokość nie więcej niż 1U, wyposażona w zintegrowany zasilacz, konstrukcja bez wentylatorów
Porty	Minimum 24 porty GigabitEthernet w standardzie BaseT minimum 2 zintegrowane porty 10Gb Ethernet SFP+.
Wydajność przełącznika	Szybkość przełączania: min. 50 Gb/s Prędkość przekazywania: min. 38 mln pakietów na sekundę Liczba adresów MAC: min. 16 tys. Pamięć buforu pakietów: min. 1 MB
Zasilanie	Pobór mocy (maks.): 20 W Zasilanie w BTU/godz.: max. 60

Funkcjonalność	<p>Obsługa wartości 802.1p i DSCP IP</p> <p>Obsługa planowania kolejek według ścisłych priorytetów i konfigurowanego protokołu Weighted Round Robin (WRR)</p> <p>Obsługa do min. 2000 sieci VLAN opartych na portach.</p>
Obsługiwane standardy	<p>IEEE 802.3ac — etykietowanie VLAN</p> <p>IEEE 802.3ad — agregacja łączy z obsługą statycznych grup LAG</p> <p>IEEE 802.1W — protokół Rapid Spanning Tree</p> <p>IEEE 802.1D — protokół Spanning Tree</p> <p>IEEE 802.1Q — sieci VLAN oparte na portach</p> <p>IEEE 802.1v — sieci VLAN oparte na protokołach</p> <p>IEEE 802.1p — priorytet Ethernet z przydzielaniem i mapowaniem użytkowników</p> <p>IEEE 802.1X — uwierzytelnianie oparte na portach</p> <p>IEEE 802.3x — sterowanie przepływem</p> <p>RFC 826 — ARP</p> <p>RFC 1155 — SMIv1</p> <p>RFC 1157 — SNMP</p> <p>RFC 1213 — MIB II</p> <p>RFC 3164 — protokół dziennika Syslog BSD</p> <p>RFC 3416 — baza informacji o zarządzaniu (MIB) dla SNMP</p> <p>RFC 768 — UDP</p> <p>RFC 783 — TFTP</p> <p>RFC 791 — IP</p> <p>RFC 792 — ICMP</p> <p>RFC 793 — TCP</p> <p>RFC 1123 — wymagania dotyczące hostów internetowych</p> <p>RFC 1042 — standard transmisji datagramów IP w sieciach IEEE802</p> <p>RFC 1071 — obliczanie internetowej sumy kontrolnej</p>
Komponenty dodatkowe	Do przełącznika należy dostarczyć kompatybilne z przełącznikiem 4 x wkładki 10GbE SFP+ jednomodowe (min. 3 km)
Dodatkowe możliwości przełącznika	<p>Identyfikacja IGMPv2</p> <p>GARP</p> <p>Ramki jumbo do 9k</p> <p>Obsługa protokołu IPv6</p> <p>Obsługa aktualizacji oprogramowania wewnętrznego i konfiguracji za pośrednictwem połączenia USB</p> <p>Automatyczne aktualizowanie oprogramowania wewnętrznego i konfiguracji z serwera TFTP/USB</p> <p>Port konsoli</p> <p>Protokoły LLDP i LLDP-MED</p>

Przełączniki sieciowe FC – 2 kpl.

Parametr	Wymagania minimalne
Typ urządzenia	Przełącznik FC w technologii FC 16 Gb/s, musi posiadać możliwość pracy portów FC z prędkościami min. 16, 8 Gb/s z funkcją autonegocjacji prędkości. Przełącznik FC musi być wykonany w tzw.

	architekturze „non-blocking” uniemożliwiającej blokowanie się ruchu wewnątrz przełącznika przy pełnej prędkości pracy wszystkich portów
Ilość portów	minimum 24 sloty na moduły FC. Wszystkie wymagane funkcje muszą być dostępne dla wszystkich portów FC przełącznika. Przełącznik musi być dostarczony wraz z minimum 12 modułami SFP FC 16 Gb/s. Należy dostarczyć również 12 kabli OM4 LC-LC o długości min. 3m max. 15m.
Opóźnienie	Przełącznik musi zapewniać opóźnienie przy przesyłaniu ramek FC między dowolnymi portami nie większe niż 700ns. Przepustowość min. 380 Gb/s
Obsługiwane porty	D_Port (ClearLink Diagnostic Port), E_Port, F_Port, M_Port (Mirror Port);
Obudowa	wysokość maksymalnie 1U i szerokość 19” oraz zapewniać techniczną możliwość montażu w szafie 19”. Szyny do montażu w szafie rack.
Chłodzenie	musi posiadać nadmiarowe wentylatory N+1.
Obsługiwane mechanizmy	<ul style="list-style-type: none"> • musi posiadać mechanizm balansowania ruchu między grupami połączeń tzw. „trunk” oraz obsługiwać grupy połączeń „trunk” o różnych długościach. • musi udostępniać usługę Name Server Zoning - tworzenia stref (zon) w oparciu bazę danych nazw serwerów. • musi posiadać możliwość wymiany i aktywacji wersji firmware’u (zarówno na wersję wyższą jak i na niższą) w czasie pracy urządzenia, bez wymogu ponownego uruchomienia urządzeń w sieci SAN. • musi zapewniać sprzętową obsługę zoningu na podstawie portów i adresów WWN • musi wspierać mechanizm balansowania ruchem w połączeniach wewnątrz wielodomenowych sieci fabric w oparciu OXID. • Możliwość wymiany w trybie „na gorąco”: minimum w odniesieniu do modułów portów Fibre Channel (SFP). • Wsparcie dla N_Port ID Virtualization (NPIV). Obsługa co najmniej 255 wirtualnych urządzeń na pojedynczym porcie przełącznika.
Kontrola dostępu / bezpieczeństwo	<ul style="list-style-type: none"> • Obsługa ACL definiująca urządzenia (przełączniki i urządzenia końcowe) uprawnione do pracy w sieci Fabric • Możliwość autentykacji przełączników z listy kontroli dostępu w sieci Fabric za pomocą protokołów DH-CHAP i FCAP • Możliwość uwierzytelnienia (autentykacji) urządzeń końcowych z listy kontroli dostępu w sieci Fabric za pomocą protokołu DH-CHAP • Kontrola dostępu administracyjnego definiująca możliwość zarządzania przełącznikiem tylko z określonych urządzeń oraz portów • Szyfrowanie połączenia z konsolą administracyjną, SSHv2, • Wskazanie nadrzędnych przełączników odpowiedzialnych za bezpieczeństwo w sieci typu Fabric. • Konta użytkowników definiowane w środowisku RADIUS lub LDAP • Szyfrowanie komunikacji za pomocą SSL/HTTPS • Obsługa SNMP v3

Zarządzanie	Przełącznik FC musi posiadać możliwość konfiguracji przez interfejs CLI oraz przez przeglądarkę internetową z interfejsem graficznym. Przełącznik FC musi mieć możliwość instalacji jednomodowych SFP umożliwiających bezpośrednie połączenie (bez dodatkowych urządzeń pośredniczących) z innymi przełącznikami na odległość minimum 10km. Przełącznik FC musi zapewnić możliwość jego zarządzania przez zintegrowany port Ethernet, RS232 oraz inband IP-over-FC. Przełącznik FC musi zapewniać wsparcie dla standardu zarządzającego SMI-S v1.1 (powinien zawierać agenta SMI-S zgodnego z wersją standardu v1.1). Przełącznik FC musi zapewniać możliwość nadawania adresu IP dla zarządzającego portu Ethernet za pomocą protokołu DHCP
Zasilanie	Maksymalny pobór mocy: 90W
Gwarancja	z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 24x7x365 poprzez ogólnopolską linię telefoniczną producenta.

Warunki ogólne

Wykonawca połączy dostarczane przełączniki sieciowe z pozostałymi segmentami sieci za pomocą światłowodów. Zamawiający wymaga aby wszystkie dostarczane terminale zostały podłączone do sieci LAN w wyznaczonych w załączniku 2 do niniejszego OPZ punktach. Za podłączenie terminali do sieci odpowiedzialny jest Wykonawca. W celu prawidłowego oszacowania oferty w zakresie wymaganej modernizacji sieci zaleca się wykonać wizję lokalną.

Jeśli do prawidłowego działania dostarczonych urządzeń wymagana będzie modernizacja sieci miedzianej, należy ją wykonać w standardzie min. cat. 6.; sieci światłowodowe należy modernizować za pomocą kabli min. 12J singlemode ze złączami LC. Podczas modernizacji Wykonawca nie będzie uprawniony do prowadzenia prac budowlanych.

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

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

- patchcordsy światłowodowe LC-LC [chyba że dostarczany sprzęt wymaga inaczej] - do PD o długości około 1m; [30 szt.]
- patchcordsy światłowodowe LC-LC [chyba że dostarczany sprzęt wymaga inaczej] - do serwerowni o długości około 3m, 5m i 10m [po 20 szt. każdej długości],
- patchcordsy miedziane do PD – o długości około 0,5m i 1m; [po 50 szt. obydwu długości]
- patchcordsy do podłączenia gniazd abonenckich – o długości około 2m [100 szt.] 5m [25 szt.], 10m [10 szt.]

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

Parametry minimalne szafek RACK – 8 kpl.

Szafki muszą być zainstalowane w miejsce obecnie wykorzystywanych (kable i urządzenia należy przenieść z 2 szafek – obecnych; do jednej – instalowanej).

Parametr	Wymagania minimalne
Wysokość	16U
Szerokość całkowita	600 mm
Głębokość całkowita	600 mm
Szerokość szyn montażowych	19 cali
Ilość belek nośnych	Dwie belki nośne 19 cali z regulacją położenia
Otwory kablowe i wentylacyjne	otwory kablowe w postaci zaślepek oraz po min. 3 otwory wentylacyjne w płycie górnej i dolnej
Obciążenie dopuszczalne	Min. 120 kg
Klasa ochrony	Min. IP 20
Dodatkowe cechy	Możliwość demontażu płyty górnej i dolnej, osłon bocznych oraz drzwi przy kompletnie wyposażonej szafce, przymocowanej do ściany. Wymagany bez narzędziowy montaż drzwi, osłon bocznych. Dwie osłony boczne, demontaż osłon bocznych możliwy po otwarciu drzwi przednich lub z własnym zamkiem. Osłona tylna z możliwością demontażu

Szafa RACK do serwerowni

Szafy do zapasowej serwerowni – 2 kpl.

Parametr	Wymagania minimalne
Wysokość	Min. 36U
Szerokość całkowita	Min. 800 mm
Głębokość całkowita	1200 mm
Szerokość szyn montażowych	Standard 19 cali
Ilość belek nośnych	Dwie pary belek nośnych 19 cali o płynnej regulacji położenia
Wykonanie drzwi przednich	Błaszane, jednoskrzydłowe, perforowane (prześwit ok. 80%) z zamkiem z klamką, możliwość zmiany kierunku otwierania drzwi
Kąt otwarcia drzwi przednich	Min. 180°
Wykonanie drzwi tylnych	Błaszane, perforowane (prześwit ok. 80%) z zamkiem trzypunktowym z klamką
Ściągane panele boczne	dwie osłony boczne, pełne z zamkami
Możliwość łączenia szaf	możliwość łączenia szaf w układy szeregowo oraz zabudowy typu Data Box
Otwory kablowe	w płycie dolnej i górnej o szerokości min. 60 mm,
Obciążenie dopuszczalne	Min. 1100 kg
Wykończenie powierzchni: szkielet, osłony, drzwi	Malowane farbą proszkową o grubej strukturze

Wykończenie powierzchni: belki nośne, ceowniki	Alucynk
Klasa ochrony	IP 20 zgodnie z normą PN-EN 60529 lub równoważną
Wyposażenie dodatkowe	Zestaw gniazd wyjściowych PDU o prądzie nominalnym 16A podłączany do gniazda wyjściowego IEC-320-C19 w zasilaczu awaryjnym UPS, obudowa 1U do montażu w szafie Rack (19") z możliwością montażu w wielu położeniach z 12 szt. gniazd IEC-320-C13 (10A) i 1 szt. IEC-320-C19 (16A) (z 2 bezpiecznikami nadprądowymi), z zaciskami zabezpieczającymi przed przypadkowym wyciągnięciem kabla zasilającego na gniazdkach wejściowych i wyjściowych. Stopki poziomujące, Zestaw przewodów uziemiających, Numeracja jednostek U na belkach nośnych

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

Zabezpieczenie e-Uслуг

Firewall – UTM – 1 zestaw

Platforma służąca zabezpieczeniu dostępu do systemów szpitalnych oraz do innych usług zainstalowanych u Zamawiającego, pozwalająca na filtrowanie ruchu z/do internetu do/z sieci LAN. Platforma musi umożliwiać kontrolę w warstwie aplikacji oraz umożliwiać zdalny dostęp do sieci LAN zamawiającego jednostkom zewnętrznym. W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.

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

Dla elementów systemu bezpieczeństwa wykonawca musi zapewnić wszystkie poniższe funkcjonalności:

OBSŁUGA SIECI

1. Urządzenie ma posiadać wsparcie dla protokołu IPv4 oraz IPv6 co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, firewalla, systemu IPS oraz usług sieciowych takich jak np. DHCP.

ZAPORA KORPORACYJNA (Firewall)

2. Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection.

3. Urządzenie ma obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT.
4. Urządzenie ma dawać możliwość ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge).
5. Interface (GUI) do konfiguracji firewalla ma umożliwiać tworzenie odpowiednich reguł przy użyciu prekonfigurowanych obiektów. Przy zastosowaniu takiej technologii osoba administrująca ma mieć możliwość określania parametrów pojedynczej reguły (adres źródłowy, adres docelowy etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie.
6. Administrator musi mieć możliwość budowania reguł firewalla na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, użytkownika bądź grupy bazy LDAP, pola DSCP nagłówka pakietu, godziny oraz dnia nawiązywania połączenia.
7. Administrator ma możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł na firewall'u.
8. Edytor reguł na firewallu ma posiadać wbudowany analizator reguł, który eliminuje sprzeczności w konfiguracji reguł lub wskazuje na użycie nieistniejących elementów (obiektów).
9. Firewall ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę lokalną, zewnętrzny serwer RADIUS, LDAP (wewnętrzny i zewnętrzny) lub przy współpracy z uwierzytelnieniem Windows 2k (Kerberos).

INTRUSION PREVENTION SYSTEM (IPS)

10. System detekcji i prewencji włamań (IPS) ma być zaimplementowany w jądrze systemu i ma wykrywać włamania oraz anomalie w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe.
11. Moduł IPS musi być opracowany przez producenta urządzenia. Nie dopuszcza się aby moduł IPS pochodził od zewnętrznego dostawcy.
12. Moduł IPS musi zabezpieczać przed co najmniej 10 000 ataków i zagrożeń.
13. Administrator musi mieć możliwość tworzenia własnych sygnatur dla systemu IPS.
14. Moduł IPS ma nie tylko wykrywać ale również usuwać szkodliwą zawartość w kodzie HTML oraz Javascript żądanej przez użytkownika strony internetowej.
15. Urządzenie ma mieć możliwość inspekcji ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, FTPS, POP3S oraz SMTPS.
16. Administrator urządzenia ma mieć możliwość konfiguracji jednego z trybów pracy urządzenia, to jest: IPS, IDS lub Firewall dla wybranych adresów IP (źródłowych i docelowych), użytkowników, portów (źródłowych i docelowych) oraz na podstawie pola DSCP.
17. Urządzenie ma posiadać moduł wykrywania typu i wersji oprogramowania sieciowego, którego ruch jest filtrowany przez urządzenie. Moduł skanujący musi działać na urządzeniu. Nie dopuszcza się stosowania rozwiązania z agentem instalowanym na komputerach w sieci. Moduł ma nie tylko wykrywać oprogramowanie ale również wykrywać i informować o lukach i podatnościach występujących w wykrytym oprogramowaniu.
18. Urządzenie musi posiadać analizę typu sandbox przeprowadzaną w chmurze producenta która zlokalizowana jest na terenie Unii Europejskiej. Nie dopuszcza się aby analiza była przeprowadzana na urządzeniu lub wymagała instalacji dodatkowego urządzenia lub oprogramowania. Nie dopuszcza się również żeby analiza była przeprowadzana przez firmy trzecie.

KSZTAŁTOWANIE PASMA (Traffic Shapping)

19. Urządzenie ma mieć możliwość kształtowania pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma.
20. Ograniczenie pasma lub priorytetyzacja ma być określana względem reguły na firewallu w odniesieniu do pojedynczego połączenia, adresu IP lub autoryzowanego użytkownika oraz pola DSCP.
21. Rozwiązanie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma a jedynie na śledzenie konkretnego typu ruchu (monitoring).
22. Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch.

OCHRONA ANTYWIRUSOWA

23. Rozwiązanie ma zezwalać na zastosowanie jednego z co najmniej dwóch skanerów antywirusowych dostarczonych przez firmy trzecie (innych niż producent rozwiązania).
24. Co najmniej jeden z dwóch skanerów antywirusowych ma być dostarczany w ramach podstawowej licencji.
25. Urządzenie ma być dostarczone wraz z komercyjnym skanerem Antywirusowym, nie dopuszcza się stosowania skanera rozwijanego w ramach projektów OpenSource.
26. Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym.
27. Administrator ma mieć możliwość zdefiniowania treści komunikatu dla użytkownika o wykryciu infekcji, osobno dla infekcji wykrytych wewnątrz protokołu POP3, SMTP i FTP. W przypadku SMTP i FTP ponadto ma być możliwość zdefiniowania 3-cyfrowego kodu odrzucenia.

OCHRONA ANTYSZPAM

28. Producent ma udostępniać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM).
29. Ochrona antyspam ma działać w oparciu o:
 - a. białe/czarne listy,
 - b. DNS RBL,
 - c. heurystyczny skaner.
30. W przypadku ochrony w oparciu o DNS RBL administrator może modyfikować listę serwerów RBL lub skorzystać z domyślnie wprowadzonych przez producenta serwerów. Może także definiować dowolną ilość wykorzystywanych serwerów RBL.
31. Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin.

WIRTUALNE SIECI PRYWANE (VPN)

32. Urządzenie ma posiadać wbudowany serwer VPN umożliwiający budowanie połączeń VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja).
33. Odpowiednio kanały VPN można budować w oparciu o:
 - a. PPTP VPN,
 - b. IPSec VPN,
 - c. SSL VPN
34. SSL VPN musi działać w trybach Tunel i Portal.
35. W ramach funkcji SSL VPN producenci powinien dostarczać klienta VPN współpracującego z oferowanym rozwiązaniem.

- 36. Urządzenie ma posiadać funkcjonalność przełączenia tunelu na łącznie zapasowe na wypadek awarii łączy dostawcy podstawowego (VPN Failover).
- 37. Urządzenie ma posiadać wsparcie dla technologii XAuth, Hub 'n' Spoke oraz modconf.
- 38. Urządzenie ma umożliwiać tworzenie tuneli w oparciu o technologię Route Based.

FILTR DOSTĘPU DO STRON WWW

- 39. Urządzenie ma posiadać wbudowany filtr URL.
- 40. Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 65 kategorii tematycznych stron internetowych.
- 41. Administrator musi mieć możliwość dodawania własnych kategorii URL.
- 42. Urządzenie nie jest limitowane pod względem kategorii URL dodawanych przez administratora.
- 43. Moduł filtra URL, wspierany przez HTTP PROXY, musi być zgodny z protokołem ICAP co najmniej w trybie REQUEST.
- 44. Administrator posiada możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru jest jedna z trzech akcji:
 - a. blokowanie dostępu do adresu URL,
 - b. zezwolenie na dostęp do adresu URL,
 - c. blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora.
- 45. Administrator musi mieć możliwość zdefiniowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony.
- 46. Strona blokady powinna umożliwiać wykorzystanie zmiennych środowiskowych.
- 47. Filtrowanie URL musi uwzględniać także komunikację po protokole HTTPS.
- 48. Urządzenie musi pozwalać na identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME.
- 49. Urządzenie posiada możliwość stworzenia białej listy stron dostępnych poprzez HTTPS, które nie będą deszyfrowane.
- 50. Urządzenie ma posiadać możliwość włączenia pamięci cache dla ruchu http.

UWIERZYTELNIANIE

- 51. Urządzenie ma zezwalać na uruchomienie systemu uwierzytelniania użytkowników w oparciu o:
 - a. lokalną bazę użytkowników (wewnętrzny LDAP),
 - b. zewnętrzną bazę użytkowników (zewnętrzny LDAP),
 - c. usługę katalogową Microsoft Active Directory.
- 52. Rozwiązanie musi pozwalać na równoczesne użycie co najmniej 5 różnych baz LDAP.
- 53. Rozwiązanie ma zezwalać na uruchomienie specjalnego portalu, który umożliwia autoryzację w oparciu o protokoły:
 - a. SSL,
 - b. Radius,
 - c. Kerberos.
- 54. Urządzenie ma posiadać co najmniej dwa mechanizmy transparentnej autoryzacji użytkowników w usłudze katalogowej Microsoft Active Directory.
- 55. Co najmniej jedna z metod transparentnej autoryzacji nie wymaga instalacji dedykowanego agenta.

56. Autoryzacja użytkowników z Microsoft Active Directory nie wymaga modyfikacji schematu domeny.

ADMINISTRACJA ŁĄCZAMI DO INTERNETU (ISP)

57. Urządzenie ma posiadać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing).
58. Mechanizm równoważenia obciążenia łączy internetowego ma działać w oparciu o następujące dwa mechanizmy:
- a. równoważenie względem adresu źródłowego,
 - b. równoważenie względem połączenia.
59. Mechanizm równoważenia łączy musi uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu.
60. Urządzenie ma posiadać mechanizm przełączenia na łączy zapasowe w przypadku awarii łączy podstawowego.
61. Urządzenie ma posiadać mechanizm statycznego trasowania pakietów.
62. Urządzenie musi posiadać możliwość trasowania połączeń dla IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łączy zapasowe w przypadku awarii łączy podstawowego.
63. Urządzenie musi posiadać możliwość trasowania połączeń względem reguły na firewallu w odniesieniu do pojedynczego połączenia, adresu IP lub autoryzowanego użytkownika oraz pola DSCP.
64. Rozwiązanie powinno zapewniać obsługę routingu dynamicznego w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP.
65. Rozwiązanie powinno wspierać technologię Link Aggregation.

POZOSTAŁE USŁUGI I FUNKCJE ROZWIĄZANIA

66. Urządzenie posiada wbudowany serwer DHCP z możliwością przypisywania adresu IP do adresu MAC karty sieciowej stacji roboczej w sieci.
67. Urządzenie musi pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP – DHCP Relay.
68. Konfiguracja serwera DHCP musi być niezależna dla protokołu IPv4 i IPv6.
69. Urządzenie musi posiadać możliwość tworzenia różnych konfiguracji dla różnych podsieci. Z możliwością określenia różnych bram, a także serwerów DNS
70. Urządzenie musi być wyposażone w klienta usługi SNMP w wersji 1,2 i 3.
71. Urządzenie musi posiadać usługę DNS Proxy.

ADMINISTRACJA URZĄDZENIEM

72. Producent musi dostarczać w podstawowej licencji narzędzie administracyjne pozwalające na podgląd pracy urządzenia, monitoring w trybie rzeczywistym stanu urządzenia.
73. Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego.
74. Interfejs konfiguracyjny musi być dostępny poprzez przeglądarkę internetową a komunikacja musi być zabezpieczona za pomocą protokołu https.
75. Komunikacja może odbywać się na porcie innym niż https (443 TCP).
76. Urządzenie ma być zarządzane przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami.
77. Rozwiązanie musi mieć możliwość zarządzania poprzez dedykowaną platformę centralnego zarządzania. Komunikacja pomiędzy urządzeniem a platformą centralnej administracji musi być szyfrowana.

- 78. Interfejs konfiguracyjny platformy centralnego zarządzania musi być dostępny poprzez przeglądarkę internetową a komunikacja musi być zabezpieczona za pomocą protokołu https.
- 79. Urządzenie ma mieć możliwość eksportowania logów na zewnętrzny serwer (syslog). Wysyłanie logów powinno być możliwe za pomocą transmisji szyfrowanej (TLS).
- 80. Rozwiązanie ma mieć możliwość eksportowania logów za pomocą protokołu IPFIX.
- 81. Urządzenie musi pozwalać na automatyczne wykonywanie kopii zapasowej ustawień (backup konfiguracji) do chmury producenta lub na dedykowany serwer zarządzany przez administratora.
- 82. Urządzenie musi pozwalać na odtworzenie backupu konfiguracji bezpośrednio z serwerów chmury producenta lub z dedykowanego serwera zarządzanego przez administratora.

RAPORTOWANIE

- 83. Urządzenie musi posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu.
- 84. System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania.
- 85. System raportowania musi posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego i Antyspamowego.
- 86. System raportujący musi umożliwiać wygenerowanie co najmniej 25 różnych raportów.
- 87. System raportujący ma dawać możliwość edycji konfiguracji z poziomu raportu.
- 88. W ramach podstawowej licencji zamawiający powinien otrzymać możliwość korzystania z dedykowanego systemu zbierania logów i tworzenia raportów w postaci wirtualnej maszyny.
- 89. Dodatkowy system umożliwia tworzenie interaktywnych raportów w zakresie działania co najmniej następujących modułów: IPS, URL Filtering, skaner antywirusowy, skaner antyspamowy

PARAMETRY SPRZĘTOWE

- 90. Urządzenie ma być wyposażone w dysk SSD o pojemności co najmniej 120 GB.
- 91. Liczba portów Ethernet 10/100/1000Mbps – min. 8.
- 92. Liczba portów światłowodowych 1Gbps – min. 2.
- 93. Liczba portów światłowodowych 10Gbps – min 2.
- 94. Urządzenie musi posiadać funkcjonalność budowania połączeń z Internetem za pomocą modemu 3G.
- 95. Przepustowość Firewalla – min. 20 Gbps
- 96. Przepustowość Firewalla wraz z włączonym systemem IPS – min. 12 Gbps.
- 97. Przepustowość filtrowania Antywirusowego – min. 2,2 Gbps
- 98. Minimalna przepustowość tunelu VPN przy szyfrowaniu AES wynosi min. 4 Gbps.
- 99. Maksymalna liczba tuneli VPN IPSec nie może być mniejsza niż. 1000
- 100. Maksymalna liczba tuneli typu Full SSL VPN nie może być mniejsza niż 150
- 101. Obsługa min. VLAN 512
- 102. Liczba równoczesnych sesji - min. 1 500 000 i nie mniej niż 60 000 nowych sesji/sekundę.
- 103. Rozwiązanie musi umożliwiać podłączenie dostarczanego urządzenia w klaster HA dwóch urządzeń działających co najmniej w trybie Active/Passive.
- 104. Urządzenie jest nielimitowane na użytkowników.
- 105. Urządzenie ma być objęte gwarancją typu NBD tzn. w przypadku awarii urządzenia wymiana na urządzenie zastępcze lub wymiana urządzenia na sprawne musi nastąpić na kolejny dzień roboczy od stwierdzenia awarii.

Wymaga się, aby dostawa obejmowała również:

- a. Minimum 36-miesięczną gwarancję producentów na dostarczone elementy systemu liczoną od dnia zakończenia wdrożenia całego systemu.
- b. Licencje dla wszystkich funkcji bezpieczeństwa producentów na okres minimum 36 miesięcy liczoną od dnia zakończenia wdrożenia całego systemu.

Instalacja elementów w modernizowanej serwerowni zapasowej

Wykonawca zobowiązany jest do instalacji wszystkich dostarczonych elementów infrastruktury IT w pomieszczeniu zapasowej serwerowni (bez prowadzenia prac budowlanych). Wykonawca zobowiązany jest dostarczyć wszystkie elementy niezbędne do instalacji i uruchomienia sprzętu (np. szyny, kable, przewody, panele, maskownice, śruby, baterie, itp.). Cały sprzęt musi zostać zainstalowany i uruchomiony zgodnie z zaleceniami producenta i zabezpieczony przed nieautoryzowanym dostępem. Wykonawca odpowiedzialny jest za odpowiednie zabezpieczenie (również fizyczne, np. kontrola dostępu, monitoring, itp.) dostarczonego sprzętu. Dostarczony sprzęt musi być monitorowany pod kątem bezpieczeństwa fizycznego (np. ciągły monitoring wizyjny oraz monitorowanie parametrów fizycznych – temperatura, wilgotność, zalanie, włamanie, itp.). Wykonawca odpowiedzialny jest za zapewnienie odpowiednich warunków niezbędnych do prawidłowego podłączenia całego dostarczonego sprzętu (np. modernizację rozdzielnic elektrycznej, podłączenie światłowodów, itp.). Zamawiający zaleca wykonanie wizji lokalnej w celu uwzględnienia wszystkich niezbędnych w ofercie elementów/kosztów.

Minimalny zakres niezbędnych prac do przeprowadzenia przez Wykonawcę zidentyfikowanych na chwilę ogłoszenia postępowania:

- dostarczyć drzwi wejściowe wraz z ościeżnicami [łącznie 3 szt.] (antywłamaniowe, szerokość min. 900mm, zapewniające wysokie bezpieczeństwo serwerowni. Drzwi muszą spełniać wymogi klasy min. RC4 oraz EI60).
- zabezpieczyć szyby w oknach folią „lustrzaną”. Okleić ściany fototapetą lateksową matową z wybranym przez Zamawiającego motywem.
- demontaż grzejników i trwałe zabezpieczenie układu przed możliwym zalaniem pomieszczenia (np. zaspawanie).
- dostawa redundantnego systemu klimatyzacji przeznaczonej do pracy w trybie ciągłym chłodzenia (24h/dobę, 365 dni). System klimatyzacji musi umożliwiać min. ustawienie pracy w trybie „rezerwy” (tj. jeden klimatyzator oczekuje w trybie ‘standby’ na awarię tego, który aktualnie działa) oraz w trybie „naprzemiennym” (tj. klimatyzatory mogą pracować na przemian w ustalonych okresach, np. co drugi dzień).
- modernizację sieci energetycznej:
 - rozbudowę rozdzielnic [wewnątrz pomieszczenia serwerowni] z zabezpieczeniami gwarantującymi ochronę przepięciową oraz od porażień prądem],
 - podłączenie do zasilania szaf serwerowych [dla UPSów o mocy min. 3kW max. 8kW w każdej szafie],
- dostawę i instalację systemu monitorowania parametrów fizycznych w serwerowni:
 - podłączenie i konfiguracja centrali w szafie RACK,
 - czujników temperatury (w pomieszczeniu oraz w każdej z szaf odrębnie)
 - czujników zalania (min. 2 czujniki)
 - czujników dymu (min. 2 czujniki)

- czujników wilgotności (min. 2 czujniki)
- dostawę systemu kontroli dostępu:
 - instalację centrali monitoringu wizyjnego CCTV
 - kamer CCTV: 4 szt. FullHD + 1 szt 4k
 - elektrozamka oraz czytnika kart RFID (zgodnych z dostarczanyimi kartami w standardzie Mifare)
 - czujników włamania [w oknach i drzwiach]
 - syreny alarmowej na zewnątrz budynku
- instalację dostarczonych szaf RACK 42U (2 szt.)
- instalację dostarczanego sprzętu serwerowego i sieciowego w dostarczonych szafach.

Klimatyzatory

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

- Parametry minimalne klimatyzacji:
- Moc chłodząca klimatyzatorów min. 6kW,
- Klasa efektywności energetycznej min. A++,
- Maksymalny pobór mocy elektrycznej: 3,2kW,
- Zakres temperatur pracy jednostki zewnętrznej (chłodzenie): -15 ~ +40°C,
- System klimatyzacji musi umożliwiać zdalne sterowanie za pomocą sieci LAN/WiFi.

Wszystkie kable i przewody należy ułożyć w istniejących kanałach wentylacyjnych.

Jeśli do prawidłowej pracy klimatyzacji niezbędne będą do wykonania jakiegokolwiek prace instalacyjne Wykonawca musi je uwzględnić w cenie oferty.

Wideomonitoring

Wykonawca dostarczy dedykowany system wideo-monitoringu. Rejestrator należy zainstalować w serwerowni w szafie RACK. Kamery należy zainstalować zgodnie z rysunkiem – Załącznik 8 do SIWZ.

Parametry minimalne kamer CCTV:

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

Kamery montowane na zewnątrz pomieszczenia serwerowni muszą być wandaloodporne.

Dodatkowo 1 kamerę należy zainstalować przed wejściem do pomieszczeń sekcji IT (2piętro). W pomieszczeniu sekcji IT należy zainstalować monitor (min 27") podglądu „live” obrazu z wszystkich kamer.

Parametry minimalne rejestratora wideo:

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

Kontrola dostępu

Wykonawca zainstaluje system kontroli dostępu (kompatybilny z posiadanymi przez Zamawiającego kartami Mifare). System kontroli dostępu będzie autonomicznym systemem umożliwiającym kontrolę dostępu do pomieszczeń sekcji IT (serwerownia oraz pok. 311 - 2piętro). System musi pozwalać na bezprzewodowe otwarcie drzwi wejściowych do pomieszczeń sekcji IT. Zamawiający skonfiguruje system w ten sposób i dostarczy min. 3 piloty.

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

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

System monitorowania parametrów fizycznych

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

Wykonawca dostarczy i zainstaluje system składający się z min.:

- Centrali monitorującej z systemem zdalnego dostępu po sieci LAN/WLAN oraz modułem GSM,
- Czujników zalania / obecności wody – min. 2 szt. – usytuowane w okolicy możliwych źródeł zalania,
- Czujników temperatury – min. 5 szt. (3 szt. w szafach RACK, 1 szt. pod sufitem, 1 szt. na ścianie na wysokości około 1,5m od posadzki),
- Czujnika otwarcia drzwi – 1 szt.,
- Detektorów ruchu – 2 szt.,
- Czujników/detektorów dymu,
- Czujników wibracyjnych lub zbitcia szyby lub włamania – min 3 szt. zamontowane w oknach,
- Syreny alarmowej zamontowanej na elewacji budynku.

Czujnik dymu, wilgotności i temperatury zainstalowany pod sufitem

Wrażliwość: 0,05 - 0,2 db/m;

Czas reakcji: około 10 sec +/- 20%;

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

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

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

Czujnik temperatury wewnętrzny

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

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

Czujnik zalania

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

Detektor ruchu

Kąt widzenia: min. 100°;

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

Tablica elektryczna TI

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

W tablicy elektrycznej TI zamontować dostarczane aparaty elektryczne:

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

Instalacja zasilania szaf serwerowych

W serwerowni zainstalowane zostaną łącznie dwie szafy serwerowe, wymagające zasilania napięciem 240V, o mocy min. 4kW każda.

Dla potrzeb zasilania szaf serwerowych przewidziano dwa gniazda 230V/16A, dla każdej szafy oddzielnie [łącznie 6szt.]. Gniazda należy instalować do koryta kablowego nad miejscem lokalizacji szafy. Instalację zasilania szaf serwerowych należy wykonać za pomocą: gniazda wtyczkowego 1-fazowego 230V, 16A - podłączone przewodem YDYżo min. 3x2,5mm².

Przewody należy prowadzić w korycie kablowym. Wszystkie montowane gniazda wtyczkowe powinny być przystosowane do podłączenia przewodu ochronnego PE. Kolorystykę oraz producenta gniazd należy ustalić z Zamawiającym przed montażem osprzętu.

Ochrona dodatkowa od porażen prądem elektrycznym

Ochrona przed dotykiem bezpośrednim realizowana jest poprzez izolowanie części czynnych – izolacja przewodów oraz obudowy aparatów i urządzeń elektrycznych. Uzupełnieniem tej ochrony jest zastosowanie wyłączników różnicowoprądowych o prądzie różnicowym 30mA. Ochrona przed dotykiem pośrednim zrealizowana jest poprzez samoczynne wyłączenie zasilania w układzie TN-S oraz połączenia wyrównawcze. Do szyny PE należy przyłączyć wszystkie metalowe elementy instalacji wodno-kanalizacyjnej i wentylacyjnej (klimatyzacji), metalowe rury instalacji elektrycznej oraz wszelkie metalowe elementy konstrukcyjne. Połączenia wyrównawcze wykonać przewodem LgYżo 10 mm².

Ochrona przepięciowa

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

- wyładowań atmosferycznych,
- czynności łączeniowych w energetyce,

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

Instalacja zasilania klimatyzatorów

Dla potrzeb wentylacji serwerowni, zainstalowane zostaną dwie jednostki zewnętrzne oraz dwie jednostki wewnętrzne. Jednostki zewnętrzne zasilane będą kablem min. YKYżo 3x2,5mm² z tablicy TI, natomiast jednostki wewnętrzne zasilane są z jednostek zewnętrznych kablem YKYżo 4x1,5mm². łączny pobór prądu przez zestaw jednostki zewnętrznej/wewnętrznej powinien wynosić maksymalnie 3,5kW [7kW dla zestawu redundantnych klimatyzatorów]. Kable zasilające prowadzić w na zewnątrz w rurze ochronnej wewnątrz istniejących kanałów wentylacyjnych. Obudowy

klimatyzatorów oraz wszystkie elementy instalacji klimatyzacji (np. kanały wentylacyjne) należy objąć instalacją połączeń wyrównawczych. Jednostki zewnętrzne należy zamontować na dachu budynku.

System archiwizacji danych obrazowych

System archiwizacji musi wykorzystywać relacyjny motor bazy danych przynajmniej w zakresie przechowywania metadanych archiwizowanych plików DICOM. Dopuszcza się transakcyjny serwer relacyjnych baz danych ORACLE / Microsoft SQL / PostgreSQL / MySQL / DB2. Musi istnieć możliwość wykupienia wsparcia technicznego u producenta bazy lub podmiotu oferującego taką usługę danych dla oferowanej wersji silnika bazy danych.
Zamawiający wymaga, aby system można było instalować na min. dwóch serwerach aplikacyjnych oraz przy dodatkowych licencjach na bazę danych – bazę danych również na dwóch serwerach. Konfiguracja serwerów bazodanowych i systemu bazodanowego musi umożliwiać ciągłość pracy w przypadku awarii dowolnego z dwóch serwerów. Nie jest wymagana żadna ingerencja użytkownika, aby po awarii dowolnego z serwerów bazodanowych przełączyć system na działający serwer. Dodatkowo architektura dwuserwerowa musi pozwalać na rozłożenie obciążenia pracy systemu bazodanowego na oba z nich.
Zamawiający dostarczy niezbędne licencje systemu operacyjnego pozwalające na uruchomienie systemu archiwizacji w środowisku Zamawiającego.
Automatyczne uruchomienie serwera archiwizacji do pełnej funkcjonalności po restarcie bez udziału administratora np. po awarii zasilania.
System musi być wyposażony w zabezpieczenia przed nieautoryzowanym dostępem na poziomie klienta (aplikacja) i serwera (serwer baz danych).
System musi archiwizować wyniki obrazowe w jakości diagnostycznej (DICOM).
System musi archiwizować badania obrazowe w archiwum on-line, którego pojemność może być przez Zamawiającego rozszerzana. Możliwe jest tworzenie kolejnych katalogów / partycji / lokalizacji sieciowych, na których będą zapisywane badania po wypełnieniu dotychczasowych.
System musi automatycznie tworzyć kopie zapasową danych obrazowych na wskazanej macierzy zapasowej (możliwość jednoczesnej obsługi dwóch macierzy zapasowych online) i w razie awarii archiwum głównego, automatycznie przełączać się na dostęp do danych z archiwum zapasowego.
System musi umożliwiać wykonywanie kopii zapasowej bazy danych co najmniej raz dziennie bez zatrzymywania pracy systemu.
Wykonawca jest zobowiązany udzielić Zamawiającemu licencji bezterminowo i bez ograniczeń dla wszystkich programów wymaganych do poprawnego działania systemu w zakresie opisu przedmiotu zamówienia. Określenie licencji jako „bezterminowych i bez ograniczeń” oznacza, że muszą one charakteryzować się następującymi cechami: nie są ograniczone czasowo i nie wygasną po zakończeniu trwania umowy; nie ograniczają liczby zarejestrowanych w systemie użytkowników; nie mają ograniczeń stanowiskowych – Zamawiający będzie mógł zainstalować dostarczone oprogramowanie na dowolnej liczbie posiadanych stanowisk komputerowych;
Wykonawca jest zobowiązany udzielić Zamawiającemu licencji dla potrzeb administracyjnych, umożliwiających konfigurowanie uprawnień dostępu do systemu archiwizacji dla co najmniej 1 użytkownika korzystającego z dowolnego uprawnionego komputera.
Wykonawca jest zobowiązany udzielić Zamawiającemu licencji bezterminowo i bez ograniczeń na moduł dystrybucji sieciowej systemu archiwizacji dla systemu HIS (otwieranie obrazów z archiwum przez system HIS).
System archiwum musi być przygotowany do pracy niezależnie od HIS (np. przy wyłączonym systemie HIS).

Minimalna liczba licencji usług serwera archiwum (w przypadku limitowania) musi wystarczyć do zaspokojenia potrzeb Zamawiającego czyli:

- 2 x serwer obsługujący min. 60.000 badań/rok
- 5 x klient diagnostyczny RTG (według szczegółowego opisu poniżej)
- 200 x klient kliniczny przeglądowy
- podłączenie przy wdrożeniu wszystkich posiadanych przez zamawiającego urządzeń DICOM (DICOM Store SCU)
- 1 x połączenie HL7
- 1 x obsługa DICOM Modality Worklist dla wszystkich urządzeń Zamawiającego

Moduły takie jak: archiwum / obsługa DICOM Modality Worklist / klient kliniczny przeglądowy / klient diagnostyczny muszą pochodzić od jednego producenta.

Integracje z innymi systemami i urządzeniami.

System dystrybucji i udostępniania danych obrazowych musi posiadać własne oprogramowanie diagnostyczne oraz kliniczne działające w technice pełny klient-serwer. Aplikacje klienckie muszą korzystać wyłącznie z bazy danych serwera archiwum. Musi istnieć możliwość skonfigurowania systemu tak, aby obrazy nie były przechowywane na stacji klienta, lub były przechowywane w pamięci podręcznej przez określony czas po zakończeniu pracy aplikacji klienckiej. W tym możliwość wskazania przez jednego użytkownika, jakie badania mają zostać pobrane do pamięci podręcznej komputera innego użytkownika (np. używane przy wskazaniu, które badania ma opisać lekarz pracujący w innej lokalizacji na urządzeniu mobilnym – określone badania pobierają się w tle).

Możliwość automatycznego udostępniania danych pacjenta i badania dla aparatów diagnostycznych (DICOM Modality WorkList). Aplikacja musi umożliwiać konfigurowanie list roboczych (MWL, Modality Worklist) dla poszczególnych urządzeń, w tym m.in. do ograniczania dostępnych wyników na podstawie oddziału zlecającego, pracowni diagnostycznej, AETitle aparatu, daty zlecenia.

Możliwość wprowadzenia konwersji polskich znaków diakrytycznych do znaków występujących w języku angielskim (np. zastąpienie liter 'ą' literą 'a') dla komunikacji z wybranymi urządzeniami lub grupą urządzeń. Możliwość zmiany strony kodowej w komunikacji z wybranym urządzeniem spośród co najmniej: Latin1 (IR 100), Latin2 (IR 101), Unicode (IR 192).

System umożliwia skonfigurowanie dostępu do danych dla użytkowników z dowolnego komputera w sieci. Możliwość wymuszenia szyfrowanego połączenia między serwerem a stacją kliencką bez instalacji dodatkowego oprogramowania. W celu uruchomienia szyfrowanego połączenia między stacją kliencką, a serwerem Zamawiający dostarczy i utrzyma aktualny certyfikat SSL.

System musi umożliwiać archiwizację i wyświetlanie danych przesyłanych w oparciu o standard DICOM 3.0, min. klasy SOP (SCU):

Standard CR Image Storage 1.2.840.10008.5.1.4.1.1.1

Standard Digital X-ray Image Storage (presentation, processing) 1.2.840.10008.5.1.4.1.1.1.1,
1.2.840.10008.5.1.4.1.1.1.1.1

Standard Mammography Image Storage (presentation, processing) 1.2.840.10008.5.1.4.1.1.1.2,
1.2.840.10008.5.1.4.1.1.1.2.1

Standard Intra-oral X-ray Image Storage (presentation, processing) 1.2.840.10008.5.1.4.1.1.1.3,
1.2.840.10008.5.1.4.1.1.1.3.1

Standard CT Image Storage 1.2.840.10008.5.1.4.1.1.2

Enhanced CT Image Storage 1.2.840.10008.5.1.4.1.1.2.1

Standard US Multiframe Image Storage (retired) 1.2.840.10008.5.1.4.1.1.3

Standard US Multiframe Image Storage 1.2.840.10008.5.1.4.1.1.3.1

Standard MR Image Storage 1.2.840.10008.5.1.4.1.1.4

Enhanced MR Image Storage 1.2.840.10008.5.1.4.1.1.4.1

Standard US Image Storage (retired) 1.2.840.10008.5.1.4.1.1.6

Standard US Image Storage 1.2.840.10008.5.1.4.1.1.6.1
Standard Secondary Capture Image Storage 1.2.840.10008.5.1.4.1.1.7
Multi-frame Single Bit Secondary Capture Image Storage 1.2.840.10008.5.1.4.1.1.7.1
Multi-frame Grayscale Byte Secondary Capture Image Storage 1.2.840.10008.5.1.4.1.1.7.2
Multi-frame Grayscale Word Secondary Capture Image Storage 1.2.840.10008.5.1.4.1.1.7.3
Multi-frame True Color Secondary Capture Image Storage 1.2.840.10008.5.1.4.1.1.7.4
Standard Overlay Storage 1.2.840.10008.5.1.4.1.1.8
Standard Modality LUT Storage 1.2.840.10008.5.1.4.1.1.10
Standard VOI LUT Storage 1.2.840.10008.5.1.4.1.1.11
Grayscale Softcopy Presentation State Storage 1.2.840.10008.5.1.4.1.1.11.1
Standard X-ray Angio Image Storage 1.2.840.10008.5.1.4.1.1.12.1
Standard X-ray Radio Fluoroscopy Image Storage 1.2.840.10008.5.1.4.1.1.12.2
Standard NM Image Storage 1.2.840.10008.5.1.4.1.1.20
Raw Data Storage 1.2.840.10008.5.1.4.1.1.66
Spatial Registration Storage 1.2.840.10008.5.1.4.1.1.66.1
Spatial Fiducials Storage 1.2.840.10008.5.1.4.1.1.66.2
Standard VL Image Storage (retired) 1.2.840.10008.5.1.4.1.1.77.1
Standard VL Multi-frame Image Storage 1.2.840.10008.5.1.4.1.1.77.2
Standard VL Endoscopic Image Storage 1.2.840.10008.5.1.4.1.1.77.1.1
Standard Video Endoscopic Image Storage 1.2.840.10008.5.1.4.1.1.77.1.1.1
Standard VL Microscopic Image Storage 1.2.840.10008.5.1.4.1.1.77.1.2
Standard Video Microscopic Image Storage 1.2.840.10008.5.1.4.1.1.77.1.2.1
Standard VL Slide Microscopic Storage 1.2.840.10008.5.1.4.1.1.77.1.3
Standard VL Photographic Image Storage 1.2.840.10008.5.1.4.1.1.77.1.4
Standard Video Photographic Image Storage 1.2.840.10008.5.1.4.1.1.77.1.4.1
Standard Ophthalmic Photographic 8 Bit Image Storage 1.2.840.10008.5.1.4.1.1.77.1.5.1
Standard Ophthalmic Photographic 16 Bit Image Storage 1.2.840.10008.5.1.4.1.1.77.1.5.2
Structured Reporting Storage (Basic Text, Enhanced SR, Comprehensive) 1.2.840.10008.5.1.4.1.1.88.11, 1.2.840.10008.5.1.4.1.1.88.22, 1.2.840.10008.5.1.4.1.1.88.33
Mammography CAD SR 1.2.840.10008.5.1.4.1.1.88.50
Key Object Selection Document Storage 1.2.840.10008.5.1.4.1.1.88.59
Chest CAD SR 1.2.840.10008.5.1.4.1.1.88.65
Standard PET Image Storage 1.2.840.10008.5.1.4.1.1.128
Standard PET Curve Storage 1.2.840.10008.5.1.4.1.1.129
Standard RT Image Storage 1.2.840.10008.5.1.4.1.1.481.1
Standard RT Dose Storage 1.2.840.10008.5.1.4.1.1.481.2
Standard RT Structure Set Storage 1.2.840.10008.5.1.4.1.1.481.3
Standard RT Plan Storage 1.2.840.10008.5.1.4.1.1.481.5
Breast Tomosynthesis Image Storage 1.2.840.10008.5.1.4.1.1.13.1.3
Encapsulated PDF Storage 1.2.840.10008.5.1.4.1.1.104.1
Standard Waveform 12 Lead ECG Storage 1.2.840.10008.5.1.4.1.1.9.1.1
System umożliwia archiwizację i wyświetlanie danych przesyłanych w oparciu o standard DICOM 3.0 lub równoważny, min. klasy SOP (SCP):
Standard Echo 1.2.840.10008.1.1
Storage Commitment 1.2.840.10008.1.20.1
Standard Digital X-ray Image Storage (presentation, processing) 1.2.840.10008.5.1.4.1.1.1.1, 1.2.840.10008.5.1.4.1.1.1.1.1
Standard Mammography Image Storage (presentation, processing) 1.2.840.10008.5.1.4.1.1.1.2, 1.2.840.10008.5.1.4.1.1.1.2.1

Standard Intra-oral X-ray Image Storage (presentation, processing) 1.2.840.10008.5.1.4.1.1.1.3, 1.2.840.10008.5.1.4.1.1.1.3.1

Standard CR Image Storage 1.2.840.10008.5.1.4.1.1.1

Standard CT Image Storage 1.2.840.10008.5.1.4.1.1.2

Enhanced CT Image Storage 1.2.840.10008.5.1.4.1.1.2.1

Standard US Multiframe Image Storage (retired) 1.2.840.10008.5.1.4.1.1.3

Standard US Multiframe Image Storage 1.2.840.10008.5.1.4.1.1.3.1

Standard MR Image Storage 1.2.840.10008.5.1.4.1.1.4

Enhanced MR Image Storage 1.2.840.10008.5.1.4.1.1.4.1

Standard US Image Storage (retired) 1.2.840.10008.5.1.4.1.1.6

Standard US Image Storage 1.2.840.10008.5.1.4.1.1.6.1

Standard Secondary Capture Image Storage 1.2.840.10008.5.1.4.1.1.7

Multi-frame Single Bit Secondary Capture Image Storage 1.2.840.10008.5.1.4.1.1.7.1

Multi-frame Grayscale Byte Secondary Capture Image Storage 1.2.840.10008.5.1.4.1.1.7.2

Multi-frame Grayscale Word Secondary Capture Image Storage 1.2.840.10008.5.1.4.1.1.7.3

Multi-frame True Color Secondary Capture Image Storage 1.2.840.10008.5.1.4.1.1.7.4

Standard Overlay Storage 1.2.840.10008.5.1.4.1.1.8

Standard Curve Storage 1.2.840.10008.5.1.4.1.1.9

Standard Modality LUT Storage 1.2.840.10008.5.1.4.1.1.10

Standard VOI LUT Storage 1.2.840.10008.5.1.4.1.1.11

Grayscale Softcopy Presentation State Storage 1.2.840.10008.5.1.4.1.1.11.1

Standard X-ray Angio Image Storage 1.2.840.10008.5.1.4.1.1.12.1

Standard X-ray Radio Fluoroscopy Image Storage 1.2.840.10008.5.1.4.1.1.12.2

Standard NM Image Storage 1.2.840.10008.5.1.4.1.1.20

Raw Data Storage 1.2.840.10008.5.1.4.1.1.66

Spatial Registration Storage 1.2.840.10008.5.1.4.1.1.66.1

Spatial Fiducials Storage 1.2.840.10008.5.1.4.1.1.66.2

Standard VL Image Storage (retired) 1.2.840.10008.5.1.4.1.1.77.1

Standard VL Multi-frame Image Storage 1.2.840.10008.5.1.4.1.1.77.2

Standard VL Endoscopic Image Storage 1.2.840.10008.5.1.4.1.1.77.1.1

Standard Video Endoscopic Image Storage 1.2.840.10008.5.1.4.1.1.77.1.1.1

Standard VL Microscopic Image Storage 1.2.840.10008.5.1.4.1.1.77.1.2

Standard Video Microscopic Image Storage 1.2.840.10008.5.1.4.1.1.77.1.2.1

Standard VL Slide Microscopic Storage 1.2.840.10008.5.1.4.1.1.77.1.3

Standard VL Photographic Image Storage 1.2.840.10008.5.1.4.1.1.77.1.4

Standard Video Photographic Image Storage 1.2.840.10008.5.1.4.1.1.77.1.4.1

Standard Ophthalmic Photographic 8 Bit Image Storage 1.2.840.10008.5.1.4.1.1.77.1.5.1

Standard Ophthalmic Photographic 16 Bit Image Storage 1.2.840.10008.5.1.4.1.1.77.1.5.2

Structured Reporting Storage (Basic Text, Enhanced SR, Comprehensive) 1.2.840.10008.5.1.4.1.1.88.11, 1.2.840.10008.5.1.4.1.1.88.22, 1.2.840.10008.5.1.4.1.1.88.33

Mammography CAD SR 1.2.840.10008.5.1.4.1.1.88.50

Key Object Selection Document 1.2.840.10008.5.1.4.1.1.88.59

Chest CAD SR 1.2.840.10008.5.1.4.1.1.88.65

Standard PET Image Storage 1.2.840.10008.5.1.4.1.1.128

Standard PET Curve Storage 1.2.840.10008.5.1.4.1.1.129

Standard RT Image Storage 1.2.840.10008.5.1.4.1.1.481.1

Standard RT Dose Storage 1.2.840.10008.5.1.4.1.1.481.2

Standard RT Structure Set Storage 1.2.840.10008.5.1.4.1.1.481.3

Standard RT Plan Storage 1.2.840.10008.5.1.4.1.1.481.5

<p>Breast Tomosynthesis Image Storage 1.2.840.10008.5.1.4.1.1.13.1.3</p> <p>Encapsulated PDF Storage 1.2.840.10008.5.1.4.1.1.104.1</p> <p>Patient Root Query/Retrieve - FIND 1.2.840.10008.5.1.4.1.2.1.1</p> <p>Patient Root Query/Retrieve - MOVE 1.2.840.10008.5.1.4.1.2.1.2</p> <p>Patient Root Query/Retrieve - GET 1.2.840.10008.5.1.4.1.2.1.3</p> <p>Study Root Query/Retrieve - FIND 1.2.840.10008.5.1.4.1.2.2.1</p> <p>Study Root Query/Retrieve - MOVE 1.2.840.10008.5.1.4.1.2.2.2</p> <p>Study Root Query/Retrieve - GET 1.2.840.10008.5.1.4.1.2.2.3</p> <p>Patient Study Only Query/Retrieve - FIND 1.2.840.10008.5.1.4.1.2.3.1</p> <p>Patient Study Only Query/Retrieve - MOVE 1.2.840.10008.5.1.4.1.2.3.2</p> <p>Patient Study Only Query/Retrieve - GET 1.2.840.10008.5.1.4.1.2.3.3</p>
<p>Obsługa poniższych Transfer Syntax:</p> <p>Implicit VR Little Endian Transfer Syntax 1.2.840.10008.1.2</p> <p>Explicit VR Little Endian Transfer Syntax 1.2.840.10008.1.2.1</p> <p>Explicit VR Big Endian Transfer Syntax 1.2.840.10008.1.2.2</p> <p>JPEG Baseline Transfer Syntax 1.2.840.10008.1.2.4.50</p> <p>JPEG Extended Transfer Syntax 1.2.840.10008.1.2.4.51</p> <p>JPEG Lossless, Non-Hierarchical, First-Order Prediction Transfer Syntax 1.2.840.10008.1.2.4.70</p> <p>JPEG2000 Image Compression (Lossless Only) 1.2.840.10008.1.2.4.90</p> <p>JPEG2000 Image Compression 1.2.840.10008.1.2.4.91</p> <p>RLE Transfer Syntax 1.2.840.10008.1.2.5</p>
<p>System musi posiadać deklarację potwierdzającą zgodność z wymogami zawartymi wyżej zarówno dla serwera archiwum jak i oprogramowania klienckiego, tzw. DICOM Conformance Statement.</p>
<p>System musi umożliwiać konfigurację wielu ścieżek, w których będą przechowywane pliki obrazowe. Możliwość określenia typu badań i źródła, z którego obrazy będą zapisywane w wybranej ścieżce.</p>
<p>Możliwość nadania priorytetu wybranej ścieżce określającego kolejność zapisywania danych w dostępnych ścieżkach (min. 8 priorytetów). Możliwość określenia maksymalnego zapewnienia dysku wybranej ścieżki, po przekroczeniu którego dane nie będą w niej zapisywane.</p>
<p>System umożliwia tworzenie kopii zapasowej obrazu w zdefiniowanej ścieżce. W przypadku awarii archiwum głównego następuje automatyczne przełączenie systemu na dostęp do danych z archiwum zapasowego bez przerywania pracy, możliwe jest wówczas automatyczne otwarcie oraz wysłanie badania z poziomu archiwum zapasowego bez ingerencji użytkownika czy administratora systemu.</p>
<p>Obsługa co najmniej dwóch niezależnych repozytoriów na kopie zapasowe danych obrazowych, każde z możliwością definiowania wielu ścieżek dostępowych (partycje, udziały sieciowe).</p>
<p>Automatyczna walidacja odebranych badań na poziomie protokołu DICOM w stosunku do informacji ze zlecenia z systemu HIS. System musi sygnalizować, które badanie zostało zwalidowane jako wykonane do zlecenia i ma poprawne dane badania oraz rozróżniać badania niezwalidowane. Możliwość wyświetlenia tylko badań powiązanych ze zleceniami z systemu HIS.</p>
<p>Procesy aplikacji na stacji klienckiej muszą pracować na koncie standardowego użytkownika systemu Windows bez praw administratora.</p>
<p>Jeśli system będzie posiadał licencje „per user” lub „per grupa” musi być wyposażony w menedżera licencji umożliwiającego centralne zarządzanie licencjami.</p>
<p>Archiwizacja wszystkich danych przekazywanych przez urządzenia diagnostyczne. Dane muszą być zapisywane w archiwum on-line a także w kopii zapasowej w formacie DICOM, bez utraty jakichkolwiek informacji. Raz zapisane pliki badania w formacie DICOM nie mają aktualizowanych danych, aktualizacja danych badania oraz pacjenta obejmuje jedynie informacje w bazie danych.</p>
<p>Automatyczna zmiana informacji w odbieranych plikach DICOM przed ich zapisaniem w archiwum. Minimum na podstawie AETitle nadawcy, rodzaju urządzenia.</p>

Obsługa nagrywania lokalnego na stacji roboczej płyt CD/DVD z badaniami. Możliwość nagrania płyty CD / DVD z badaniami po anonimizacji, wyboru pojedynczego lub wielu badań do nagrania na jednej płycie, zawarcia opisu badania (także w formie SR), adnotacji naniesionych przez radiologa. Płyta musi być nagrywana z przeglądarką DICOM, która wyświetla dane demograficzne pacjenta i badania w konfigurowalny sposób. Na płytę nagrywane muszą być również pliki JPG z obrazami badania.
Możliwość określenia rodzaju kompresji dla przechowywanych obrazów pochodzących z danej modalności, w tym co najmniej bez kompresji, skompresowane bezstratnie algorytmem JPEG2000.
Graficzny panel administracyjny pozwalający na zmianę danych pacjenta, serii i badania, dzielenie badania oraz łączenie badań, przenoszenie serii między badaniami.
Panel administracyjny umożliwiający: <ul style="list-style-type: none"> - zarządzanie użytkownikami - zarządzanie grupami użytkowników i prawami tych grup - zarządzanie węzłami DICOM - zarządzanie regułami autoroutingu.
Rejestrowanie zdarzeń systemowych z datą i godziną oraz stacją źródłową, min: logowanie/wylogowanie użytkownika, otworenie badania, zmiana danych pacjenta.
Graficzny panel statystyczny z możliwością eksportu danych do formatu akceptowanego przez MS Excel, min: liczba badań ze względu na typ, lekarza zlecającego; liczby opisanych badań ze względu na radiologa.
Możliwość tworzenia naukowej bazy badań, pozwalającej na przypisywanie badań lub obrazów do dowolnie skonfigurowanych kategorii prywatnych oraz publicznych.
Możliwość dostępu z oddalonej lokalizacji po szyfrowanym łączu do badań i opisów wraz z możliwością uruchomienia przeglądarki diagnostycznej z wyborem między trybem standardowym i dostosowanym do wolnego łącza Internetowego.
System archiwum musi posiadać certyfikat klasy minimum IIa lub równoważny, właściwy dla urządzeń lub oprogramowania medycznego używanego w procesie bezpośredniego diagnozowania lub/i monitorowania życiowych procesów fizjologicznych.
Autorouting badań po zadanych regułach, min: typ badania, klasa SOP, ID pacjenta, nazwa badania, stacja źródłowa, lekarz zlecający, ramy czasowe ze względu na dzień tygodnia i godzinę. Możliwość określenia czy badanie ma być anonimizowane, przesłane zdekompresowane, skompresowane bezstratnie lub stratnie. Możliwość wymuszenia, aby przy autoroutingu przesyłać jednocześnie określoną ilość badań poprzednich danego pacjenta.
Administrator musi posiadać dostęp do plików logów dla usług powiązanych z systemem archiwum - w tym m.in.: <ul style="list-style-type: none"> • import badań z urządzeń • autorouting; • administrator systemu archiwum; • listy robocze MWL; • interfejs wymiany danych HL7; • tworzenie kopii obrazów DICOM; • system dystrybucji obrazów.
Aplikacja musi umożliwiać przeglądanie zawartości danych nagłówkowych plików DICOM.
Aplikacja musi umożliwiać wyszukiwanie badań w archiwum na podstawie kryteriów, min.: <ul style="list-style-type: none"> • nazwisko i imię pacjenta; • data urodzenia pacjenta; • identyfikator pacjenta; • numer badania; • zakres dat wykonania badania;

<ul style="list-style-type: none"> • zakres dat importu badania do systemu; • frazy występującej w opisie do badania; • status badania (co najmniej opisane, nieopisane); • priorytet; • nazwa badania; • lekarz zlecający; • lekarz opisujący; • data wykonania opisu; • modalność; • urządzenie, z którego zostało wysłane badanie (AETitle).
<p>Aplikacja musi umożliwiać wyszukiwanie badań na urządzeniach DICOM podłączonych do systemu archiwum - wraz możliwością pobrania ich do archiwum lub przesłania do innych urządzeń DICOM podłączonych do systemu.</p>
<p>Aplikacja musi umożliwiać wysyłanie badań przez DICOM C-STORE do innych węzłów DICOM, w tym możliwość grupowych wysyłek przez wskazanie badania / badań i więcej niż jednego węzła, na które badanie ma być wysłane w jednym zadaniu.</p>
<p>Aplikacja musi umożliwiać zmianę danych pacjenta i badania znajdującego się w archiwum DICOM w zakresie:</p> <ul style="list-style-type: none"> • imię, nazwisko pacjenta; • data urodzenia pacjenta; • płeć pacjenta; • numer badania; • nazwa badania. <p>Zmiany są zapisywane w bazie danych, nie w plikach DICOM. Przy wysyłce bądź eksporcie danych z systemu nagłówki DICOM w tworzonych / wysyłanych plikach są aktualizowane informacjami z bazy danych.</p>
<p>Aplikacja musi umożliwiać przenoszenie pomiędzy badaniami (np. w przypadku błędu technika):</p> <ul style="list-style-type: none"> • jednej lub wielu serii obrazów; • jednego lub wielu obrazów.
<p>Aplikacja musi umożliwiać śledzenie zmian danych pacjenta i badania w bazie danych.</p>
<p>Administrator musi mieć możliwość skonfigurowanie serwera archiwum w zakresie zmian następujących parametrów:</p> <ul style="list-style-type: none"> • nazwa AE, • numer portu nasłuchu, • poziom logowania zdarzeń, • ilość połączeń do serwera, • Storage Commitment, • parametry komunikacji HL7.
<p>Administrator musi mieć możliwość podglądu stanu i kontroli usług (start / stop / restart) związanych z serwerem archiwum min.:</p> <ul style="list-style-type: none"> • import badań; • autorouting; • obsługa zapytań query/retrieve • moduł list roboczych (MWL); • interfejs wymiany danych HL7; • system dystrybucji obrazów.
<p>Aplikacja musi pozwalać na podgląd wykorzystania licencji dostępowych do serwera archiwum oraz umożliwiać administratorowi rozłączanie sesji użytkowników.</p>

Aplikacja musi pozwalać na zarządzanie grupami użytkowników i przypisywanie uprawnień do grupy:

- Ustawienia autoroutingu;
- Usuwanie badań;
- Eksport badań;
- Zanonimizowany eksport badań;
- Zarządzanie użytkownikami i grupami użytkowników;
- Przesyłanie badań pomiędzy węzłami;
- Zarządzanie węzłami;
- Nagrywanie badań na płyty;
- Dodawanie komentarzy do badań;
- Wydruk zdjęć na drukarce medycznej;
- Wykonywanie opisów;
- Podgląd treści opisu;
- Zapisywanie adnotacji i pomiarów na badaniach.

Możliwość ograniczenia dostępu do danych przechowywanych w systemie archiwum na podstawie typu badania (modalność), jednostki kierującej, lekarza zlecającego. Użytkownikowi musi być możliwość ograniczyć dostęp tylko do badań mu przypisanych. Możliwość przypisywania badań automatycznie na podstawie reguł jak i ręcznie przez osobę, która do danego badania ma dostęp.

Integracja z systemem HIS poprzez interfejs HL7 w zakresie wymiany informacji o pacjentach, zleceniach i opisach. Dostarczony system archiwum musi współpracować z posiadanym systemem HIS w sposób pozwalający na pracę wg następującego schematu:

- badania są rejestrowane w systemie HIS bez udziału innych systemów klasy ERP (RIS, LIS, CIS itp.),
- informacja o zarejestrowanym badaniu jest wysyłana do systemu archiwum w celu obsługi DICOM Modality Worklist (zakres wymiany danych – ID pacjenta, PESEL, Nazwisko i Imię, numer zlecenia, lekarz i oddział / placówka zlecająca, kod i nazwa procedury, zaplanowana data wykonania badania, termin rejestracji, komentarz do badania, urządzenie diagnostyczne, na którym badanie ma się odbyć);
- system archiwum informuje HIS o wykonaniu badania w Zakładzie Diagnostyki Obrazowej,
- opis badań wykonany w jednym systemie uznanym za opisowy jest przekazywany do drugiego,
- system HIS jest systemem nadrzędnym, wszelkie zmiany danych badania i pacjenta wykonuje się po stronie systemu HIS,
- identyfikatory pacjentów oraz badań (zleceń) które w systemie archiwum stanowią PatientID (0010,0020) oraz Accession Number (0008,0050) są nadawane przez system HIS.

System musi komunikować się z systemem HIS za pomocą protokołu HL7 w wersji min. 2.x

System musi obsługiwać komunikację HL7 z HIS bezpośrednio, bez jawnego bądź ukrytego udziału systemu typu RIS, moduły integracyjne muszą być zaimplementowane w systemie archiwum lub, jeśli działają jako zewnętrzne aplikacje, muszą korzystać z bazy danych systemu archiwum.

System archiwum musi generować DICOM Modality Worklist dla urządzeń diagnostycznych na podstawie odebranych od systemu HIS wiadomości HL7.

Generowana worklista musi mieć możliwość filtrowania wyników osobno dla każdego węzła AET (odpytującego aparatu diagnostycznego). Minimalne kryteria filtrowania wyników zapytań:

- modalność
- zakres dat
- AET aparatu, np. przy wielu aparatach pytających o badania CR system archiwum wystawi każdemu badaniu przypisane tylko dla danego aparatu podczas rejestracji w HIS (zgodnie z danymi przesłanymi w HL7 ze zleceniem)

System archiwum musi automatycznie poprawiać/synchronizować dane w generowanej przez system DICOM Modality Worklist, na podstawie danych odebranych od systemu HIS w wiadomościach HL7

Automatyczna zmiana statusu zleconego badania w generowanej przez system DICOM Modality Worklist, dla urządzeń diagnostycznych w następujących przypadkach:

- automatycznej zmianie statusu badania na zakończone po odebraniu wiadomości DICOM MPPS od urządzenia diagnostycznego,
- automatycznej zmianie statusu badania na zakończone po odebraniu obrazu DICOM przypisanego danemu zleceniu przez system archiwum od urządzenia diagnostycznego,
- ręcznego połączenia odebranego badania z pozycją na liście badań DICOM Modality Worklist przez uprawnionego użytkownika (np. w przypadku gdy badanie zostało najpierw wykonane, a następnie zarejestrowane w systemie HIS).

System archiwum musi automatycznie usuwać pozycję DICOM Modality Worklist po wycofaniu (anulowaniu) zlecenia w systemie HIS na podstawie otrzymanego z systemu HIS komunikatu HL7

System archiwum po odebraniu wiadomości DICOM MPPS o zakończeniu badania od urządzenia diagnostycznego lub po odebraniu pierwszego obrazu badania od urządzenia diagnostycznego lub po ręcznym, w interfejsie/panelu użytkownika, wygenerowaniu informacji o zakończeniu, wysyła do systemu HIS za pomocą wiadomości HL7 ORM^O01 lub ORU^R01 następujące informacje:

- o zakończeniu badania (wywołuje zmianę statusu zlecenia po stronie HIS np. z "do realizacji" na "nieautoryzowane"),
- odsyłacz do przeglądarki klinicznej (link musi się pojawić w załącznikach do wyników po stronie HIS)
- identyfikator technika wykonującego pobrany z tagów DICOM archiwizowanych obrazów, np. 0008,1070 Operator'sName (zmapowany na odpowiedni identyfikator użytkownika w systemie HIS musi pojawić się na liście personelu uczestniczącego w wykonaniu badania).

System archiwum musi odbierać od systemu HIS komunikaty HL7 ORU^R01 z wynikami (opisami) badań. Odebrane opisy muszą być udostępniane w przeglądarce obrazów wraz z badaniem oraz dodatkowo możliwe jest skonwertowanie ich do formatu DICOM SR (DICOM Structured Report i dołączenie do badania w systemie archiwum jako kolejna seria, udostępniane stacjom diagnostycznym, do nagrania na płytę oraz prawidłowo wyświetlane w przeglądarce klinicznej. Minimum informacji niezbędnych do umieszczenia w utworzonej serii SR to:

- dane pacjenta: imię i nazwisko, płeć, data urodzenia, identyfikator PatientID,
- tekst opisu - status (autoryzowane),
- dane lekarza autoryzującego badanie w systemie HIS,
- data opisu (autoryzacji).

Obsługa uaktualnień w obiegu danych dotyczących pacjenta (HL7 ADT^A08), jego badań (HL7 ORM^O01) oraz ich opisów (ORU^R01). Ewentualne zmiany są automatycznie uwidocznione w badaniach znajdujących się w systemie archiwum i systemie dystrybucji obrazów. Nowe (aktualne) dane są udostępniane węzłom DICOM podczas operacji FIND, MOVE lub Query/Retrieve. Oryginalne dane pozostają niezmiennione na poziomie plików (dane w nagłówku pliku DICOM są niezmienniane).

Obsługa scalania kart pacjenta – po odebraniu z systemu HIS wiadomości HL7 ADT^A18 lub ADT^A40 (wydarzenie patient merge) lub ADT^A31 system archiwum automatycznie przypisuje badania scalanego pacjenta do karty docelowego pacjenta i łączy historię badań pacjenta. Zmiany są automatycznie uwidocznione w badaniach znajdujących się w systemie archiwum i systemie

dystrybucji obrazów. Nowe (aktualne) dane są udostępniane węzłom DICOM podczas operacji FIND, MOVE lub Query/Retrieve. Oryginalne dane pozostają niezmienione na poziomie plików (dane w nagłówku pliku DICOM są niezmieniane).

Administrator systemu z panelu administracji ma możliwość połączenia istniejącego w systemie badania z odpowiednią pozycją Modality Worklist utworzoną na podstawie danych zlecenia z systemu HIS. Zmiany są automatycznie uwidocznione w badaniach znajdujących się w systemie archiwum i systemie dystrybucji obrazów. Nowe (aktualne) dane są udostępniane węzłom DICOM podczas operacji FIND, MOVE lub Query/Retrieve. Oryginalne dane pozostają niezmienione na poziomie plików (dane w nagłówku pliku DICOM są niezmieniane). Po połączeniu system archiwum musi wysłać do systemu HIS za pomocą wiadomości HL7 ORM^O01 lub ORU^R01 następujące informacje:

- o zakończeniu badania (wywołuje zmianę statusu zlecenia po stronie HIS np. z "do realizacji" na "nieautoryzowane"),
- link do przeglądarki klinicznej (link musi się pojawić w załącznikach do wyników po stronie HIS)
- identyfikator technika wykonującego pobrany z tagów DICOM archiwizowanych obrazów, np. 0008,1070 Operator'sName (zmapowany na odpowiedni identyfikator użytkownika w systemie HIS musi pojawić się na liście personelu uczestniczącego w wykonaniu badania).

Realizacja komunikacji HL7 ma zostać wykonana w oparciu o topologię gwiazdy i niezależną szynę wymiany danych, do której w przyszłości Zamawiający będzie mógł podłączyć inne systemy np. laboratorium, teleradiologii, itp.

Integracja desktopowa z dowolnego zewnętrznego systemu poprzez wywołanie z niego aplikacji. Możliwość uruchomienia przeglądarki archiwum ze wskazaniem użytkownika z systemu wywołującego. Wywoływanie minimum:

Badania po numerze akcesji

Badania po parze numerów – akcesji i identyfikatora pacjenta

Badania po numerze STUDY INSTANCE UID

Wszystkich badań danego pacjenta

Możliwość konfiguracji systemu, aby powtórnie wysyłane badania były ponownie importowane (nadpisywane), buforowane (zapis w inne niż archiwum główne miejsce), usuwane bez zapisu.

Obsługa DICOM Query/Retrieve dla zewnętrznych węzłów DICOM (stacje diagnostyczne, urządzenia diagnostyczne, duplikatory). Możliwość ustawienia usługi Query/Retrieve na odrębnym porcie i innej nazwie niż usługa DICOM C-STORE. Możliwość konfiguracji unikatowych ustawień dla zapytań Query/Retrieve dla wybranych urządzeń (min. Konwersja polskich znaków diakrytycznych na postać znaków dostępnych w języku angielskim). Możliwość konfiguracji dostępu do badań przez DICOM Query/Retrieve dla węzłów DICOM tylko pochodzących z danej grupy urządzeń (np. tylko CT).

Obsługa woluminów tymczasowych do przetrzymywania części plików.

Możliwość eksportu badania na dysk zewnętrzny w jakości diagnostycznej i referencyjnej wraz z przeglądarką obrazów.

Klient kliniczny – przeglądowy / dystrybucja sieciowa

Klient kliniczny przeglądowy tego samego producenta co system archiwum.

Automatyczna instalacja z sieci oprogramowania klienckiego na stacjach roboczych. Aplikacja nie wymaga żadnej ingerencji użytkownika podczas instalacji na dowolnym komputerze w sieci.

Automatyczna aktualizacja oprogramowania bez ingerencji użytkownika. Możliwość dystrybucji nowych wersji oprogramowania na stacjach klienckich przed ich wgraniem na środowisko serwerowe.

Dostęp do systemu chroniony hasłem. Możliwość automatycznego wylogowania użytkownika po zadanym okresie nieaktywności. Możliwość blokowania konta użytkownika po zdefiniowanej próbie nieudanych logowań. Możliwość określenia stopnia skomplikowania haseł użytkowników.
Aplikacja automatycznie wykrywa ilość podłączonych monitorów i wybiera odpowiedni tryb wyświetlania na podstawie informacji zapisanych w profilu użytkownika, min: protokoły wyświetlania na poszczególnych monitorach. Możliwość odłączenia dowolnego monitora z pracy z aplikacją na potrzeby np. wykorzystywania go przez system RIS.
W przypadku podłączenia czterech monitorów system umożliwia podział na następujące obszary wyświetlania: 1-1-1-1; 1-3; 1-2-1; 3-1; 1-1-2; 2-2; 2-1-1; 4
Wyszukiwanie badań co najmniej wg numeru ID badania, numeru ID pacjenta, nazwiska (imienia) pacjenta, daty wykonania, rodzaju badania, typu urządzenia, nazwy badania, daty wykonania opisu, statusu. Możliwość tworzenia i zapisywania własnych filtrów na podstawie zadanych kryteriów.
Zakładki „Ulubione” w których przechowywane są odnośniki do wybranych przez użytkownika badań. Możliwość podziału zakładek na foldery i podfoldery. Każdy użytkownik widzi tylko swoje zakładki.
Po wybraniu badania na liście roboczej oprogramowanie sygnalizuje obecność innych badań wygranego pacjenta, wyświetla opis badania oraz miniatury obrazów badania.
Możliwość szybkiego podglądu badań i opisów tego samego pacjenta z poziomu okna przeglądarki obrazów DICOM bez konieczności powrotu na listę badań.
Automatyczną aktualizacją list roboczych z wykazem badań w wybranych przez użytkownika interwałach czasowych.
Możliwość wydruku opisu (wszystkie dotychczasowe wersje, np. jeżeli nowa wersja jest uzupełnieniem, lub tylko ostatnia) jak i obrazów badania na drukarce lokalnej
Możliwość definiowania indywidualnych pasków narzędziowych z dostępnych narzędzi do obróbki obrazu. Graficzny edytor pasków. Przypisywanie różnych pasków narzędziowych do różnych rodzajów badań.
Graficzny edytor definiowania indywidualnych protokołów wyświetlania w zależności od min. liczby podłączonych monitorów, typu badania, AETitle źródła badania, nazwy badania. Konfiguracja min: wybrania monitorów na którym mają być wyświetlane obrazy; podział obszaru min. 1x1,2x2,2x3,3x4,4x5; wybranego paska narzędziowego, wyświetlania poprzednich badań pacjenta, rozmieszczenia serii na ekranie (ustawienie umiejscowienia w zależności od numeru lub kolejności serii) i ustawień okna dla wybranej serii.
System umożliwia zapisanie indywidualnych ustawień wyświetlania dla każdego użytkownika centralnie, tak żeby były one dostępne na każdej stacji roboczej. Indywidualne ustawienia zawierają co najmniej: protokoły wyświetlania z podziałem na ilość podłączonych monitorów do stacji klienckiej, skróty klawiszowe, ustawienia konfiguracji listy roboczej, predefiniowane filtry wyszukiwania badań, ustawienia przeszukiwania listy badań. Użytkownik logujący się z dowolnej maszyny otrzymuje ustawienia ze swojego profilu.
Wyświetlanie min. badań typu CR, DX, MG, USG, MR, CT, ECG, SC, OT, NM i PET
Możliwość jednoczesnego wyświetlenia badań różnych pacjentów
Możliwość jednoczesnego wyświetlania badania otwartego bezpośrednio z płyty (bez importu) oraz pochodzącego z archiwum.
Sortowanie obrazów w serii według znaczników DICOM min. wg numeru ID obrazu, pozycji warstwy, czasu akwizycji
Możliwość ręcznego ustalenia dowolnej kolejności obrazów w serii.
Możliwość utworzenia badania z wyświetleniem tylko obrazów „istotnych” – kluczowych.
Organizowanie przeglądania sekwencji obrazów, min:

<ul style="list-style-type: none"> - zmiana kolejności, - tryb animacji (ustawianie prędkości, kierunku, początku i końca zapętlenie animacji), - scalanie obrazów wybranych serii.
System musi umożliwiać zapis (eksport) na lokalnym dysku obrazu z adnotacjami jako plik JPEG BMP, TIFF, DICOM, AVI. Przy zapisie plików wieloklatkowych do AVI – możliwość wyboru kodeka (w tym MPEG4).
System musi umożliwiać podział badania wieloklatkowego na pojedyncze obrazy.
<p>Obróbka obrazów w zakresie podstawowym, min.</p> <ul style="list-style-type: none"> - ustawienia okna; - negatyw / pozytyw; - blendowanie; - obroty 90° i 180°, odbicia lustrzane; - wyświetlanie w trybie skali 1:1 - funkcja ruchomej lupy z płynnym powiększaniem; - ukrywanie danych pacjenta; - płynne powiększanie całości obrazu; - określenie zakresu działania modyfikacji obrazu – jeden obraz, cała seria; - filtr wyostrażający i wygładzający.
<p>Pomiary na obrazach w zakresie podstawowym, min.:</p> <ul style="list-style-type: none"> - Odległości po linii prostej; - Odległość po krzywej; - Histogram; - Kalibracja geometryczna; - Kąty między dwoma nieprzecinającymi się prostymi (kąt Cobba); - Kąty między kolejnymi nieprzecinającymi się prostymi; - Automatyczne kreślenie linii łączącej środki dwóch innych odcinków; - Kąt między dwoma liniami łączącymi środki par innych odcinków; - Kąt pomiędzy dwoma półprostymi o wspólnych początkach; - Balans kręgosłupa; - Wskaźnik sercowo-płucny; - Wskaźnik rozbieżności długości kości udowych; - Pomiar objętości obszaru na podstawie obrazów 2D z wyborem algorytmu eliptycznego, sferycznego i Lamberta; - Wyznaczanie linii centralnej; - Wartość piksela znajdującego się pod kursorem myszy (w przypadku badań TK, wartość HU); - Pomiary statystyczne na wybranym ROI (region zainteresowania) w kształcie elipsy, wielokąta lub dowolnego kształtu z wyznaczeniem wartości minimalnej, maksymalnej średniej i odchylenia standardowego oraz prezentacją histogramu zaznaczonego obszaru.
<p>Nanoszenie i usuwanie adnotacji na obrazach</p> <ul style="list-style-type: none"> - Tekst dowolny; - Tekst predefiniowany przez użytkownika; - Linie proste; - Strzałki z podpisem; - Notatka dodawana do wybranego miejsca obrazu, z wyświetleniem tylko tytułu tej notatki, z możliwością otworzenia pełnego tekstu; - Prostokąty; - Wielokąty regularne; - Okręgi; - Edycja (przesuwanie i zmiany zawartości / kształtów);

<ul style="list-style-type: none"> - Szybkie ukrywanie i przywracanie; - Szybkie usuwanie wybranych oraz wszystkich adnotacji; - Etykietowanie kręgów.
Predefiniowanie indywidualnych ustawień okna z podziałem na typ badania, min. 10 ustawień, z szybkim dostępem za pomocą skrótów klawiszowych.
Automatyczna synchronizacja i przeglądanie synchroniczne serii TK i MR w obrębie badania. Ręczna synchronizacja i przeglądanie synchroniczne serii TK i MR w różnych badaniach. Możliwość określenia, które serie podlegają synchronizacji – dotyczy synchronizacji automatycznej jak i ręcznej.
Możliwość skopiowania wybranego kawałka obrazu do schowka systemowego.
Znacznik informujący użytkownika o wyświetleniu wszystkich obrazów w serii.
Ostrzeżenie w postaci dodatkowego komunikatu w przypadku, gdy nie wszystkie obrazy z danego badania zostały wyświetlone.
Progresywne wczytywanie obrazów z indywidualnym skokowym określeniem domyślnej ilości wczytanych danych ze względu na typ badania.
Indywidualnie definiowane skróty klawiszowe, min. wyświetl opis badania, zamknij badanie, otwórz badanie, zmiana okna, minimalizacja, lista robocza, włącz/wyłącz dane demograficzne, włącz/wyłącz adnotacje i pomiary.
Prezentacja statusu badania na liście roboczej. Min. status informujący o oczekiwaniu na opis, zakończeniu opisu, zatwierdzeniu opisu.
System umożliwia ustawienie aplikacji stacji klienckiej w stan czuwania, tak, że badania spełniające zdefiniowane kryteria są ściągane do pamięci podręcznej stacji diagnostycznej bez ingerencji użytkownika.
Możliwość wyświetlenia listy badań z DICOMDIR znajdujących się na nośniku optycznym umieszczonym w lokalnym napędzie CD. Możliwość importu tych badań do systemu archiwum z edycją podstawowych danych pacjenta.
Możliwość pobierania badań z innych systemów za pomocą DICOM Query/Retrieve
Możliwość otworzenia pojedynczych plików DICOM z lokalnego folderu/napędu CD.
Możliwość automatycznego otwierania wraz z badaniem komentarza do zlecenia pochodzącego z systemu HIS bądź wpisanego przez innego użytkownika ręcznie w systemie archiwum.
Automatyczne ładowanie przez przeglądarkę obrazów zaimportowanych po otwarciu badania.
Możliwość konfiguracji wyświetlanych jako etykiety na otwartych zdjęciach szczegółów badania / obrazu w tym możliwość wyświetlenia minimum: Imię i nazwisko pacjenta, identyfikator pacjenta, inne id pacjenta, numer badania, data urodzenia pacjenta, parametry ekspozycji i dawki, technik wykonujący badanie Możliwość zmiany wielkości i rodzaju czcionki dla każdej ze szczegółowych informacji.
Aplikowanie tablic LUT przy wyświetlaniu dla zdjęć, gdzie są one dostępne.
Możliwość konfiguracji wyboru funkcji dostępnych pod klawiszami myszy.
Możliwość integracji z systemem Active Directory i obsługę logowania do aplikacji przy pomocy loginu i hasła z Active Directory jak i hasła lokalnego.
Klient diagnostyczny
Klient diagnostyczny RTG tożsamy z klientem klinicznym rozszerzony o poniższe funkcjonalności.
Zapisywanie w systemie archiwum i udostępnianie zmian wprowadzonych na obrazach, min: adnotacje i pomiary, ustawienia okna, kalibracja, obrót, odbicie lustrzane.
Możliwość wykonywania tzw. zrzutów ekranowych min. z wybranego obrazu, całego ekranu i dodanie ich do badania w archiwum jako nowa seria.
Możliwość oznaczenia wybranego obrazu w badaniu jako „istotny”.

Możliwość umieszczania na wydruku opisu obrazów z badania lub wykonanych zrzutów.
Wtórne rekonstrukcje MPR warstw CT i MR (2D) w płaszczyznach – wieńcowej, strzałkowej, skośnej. Możliwość zapisania rekonstrukcji jako nowa seria w badaniu ze wskazaniem ilości i odstępów między zapisywanymi rekonstruowanymi obrazami.
Wtórne rekonstrukcje MPR warstw TK i MR po dowolnej krzywej (3DMPR). Możliwość zapisania rekonstrukcji jako nowa seria w badaniu.
Określenie grubości warstwy rekonstrukcji. Płynna zmiana grubości warstwy i możliwość ręcznego ustawienia wartości.
Rekonstrukcje MIP, MinIP, z określeniem dowolnego regionu zainteresowania. Możliwość „odcinania” nieistotnych części rekonstrukcji.
Tworzenie automatycznych sekwencji obrazów rekonstrukcji MIP w różnych pozycjach i zapisanie ich do systemu archiwum.
Możliwość oznaczenia kręgów na widoku w płaszczyźnie czołowej lub strzałkowej, tak, że po przejściu do widoku płaszczyzny poziomej system powinien pokazywać informację na wysokości jakiego kręgu znajduje się wyświetlany obraz.
Możliwość tworzenia katalogów "kominkowych", w których można zapamiętać chwilowe ustawienia parametrów wyświetlania danego badania (obraz w serii, parametry okna, obrót, rekonstrukcja) tak, aby można było w przyszłości wywołać to badanie z takimi ustawieniami wyświetlania jak zapisane bez konieczności indywidualnego przywracania poszczególnych parametrów wyświetlania – możliwość współdzielenia zapisanych stanów z innymi użytkownikami i tworzenia listy z zapisanych prac.
Możliwość zapisania zmian sposobu i układu wyświetlania badania, aby można było do niego wrócić z poziomu otwartego badania w przyszłości. Obsługa zapisu wielu stanów. Możliwość konfiguracji, aby gdy w pamięci jest zapisany układ wyświetlania badania to był on automatycznie aplikowany przy otwieraniu badania.
Możliwość zapisywania powiększeń obrazu jako plików GSPS (Grayscale Softcopy Presentation State) oraz możliwość włączenia ich automatycznego aplikowania przy uruchamianiu badania.
Sygnalizacja pojawiania się nowych badań w systemie archiwum.
Możliwość dodania i odtworzenia głosowego opisu badania.
Możliwość stworzenia opisu tekstowego i zatwierdzenia badania. Co najmniej dwa stopnie zatwierdzania opisów – opis wstępny (możliwy do edycji), opis końcowy (bez możliwości edycji).
Możliwość tworzenia nowych wersji opisów do już zatwierdzonych badań z zastrzeżeniem, że radiolodzy i administratorzy mają wgląd w poprzednie wersje opisów.
Możliwość tworzenia i edycji szablonów opisowych dostępnych przy tworzeniu opisów. Możliwość grupowania szablonów.
Inne wymagania dla systemu i wdrożenia
Interfejs w języku polskim, pomoc w języku polskim
Możliwość wyboru interfejsu pomiędzy językiem polskim a angielskim.
Możliwość rozszerzenia o zintegrowany z systemem komunikatora umożliwiający podgląd informacji o zalogowanych użytkownikach, wymianę informacji tekstowych między użytkownikami i przekazywanie odniesień do badań wprost z przeglądarki systemu archiwum.
Grupowanie użytkowników. Możliwość definiowania uprawnień na poziomie grup użytkowników (ról)
Dzienniki zdarzeń Serwera archiwum. Rejestrowanie zdarzeń związanych z pracą systemu.
Dzienniki zdarzeń systemu dystrybucji sieciowej. Rejestrowanie zdarzeń związanych z pracą systemu webowej dystrybucji badań.

Notowanie zdarzenia protokołów. Przychodzące i wychodzące wiadomości DICOM i HL7 (DICOM Modality Worklist, MPPS, C-FIND).
Notowanie zdarzenia walidacji badań. Zmiany numerów i nazwisk pacjentów, numerów badań, dowiązywanie badań, negatywne weryfikacje
Możliwość wysyłki treści opisu do badań poprzez wiadomość e-mail, który jest szyfrowany certyfikatem lub hasłem.
Obsługa plików DICOM encapsulated PDF.
Przechowywanie haseł w bazie danych w postaci wyniku funkcji skrótu. Hasło powinno zostać zmienione przez dodatkową zmienną wartość, a następnie z wyniku powinien być przeliczony skrót. W systemie przechowywana jest zmienna wartość dodana do hasła i skrót hasła z tą wartością. Zalecane funkcje skrótu: SHA-2 Niedozwolone funkcje skrótu: MD1 - MD5, SHA-1
Możliwość rozbudowy systemu o następujące moduły tego samego producenta do zaawansowanej diagnostyki badań tomograficznych obejmujący: <ul style="list-style-type: none"> • Rekonstrukcje 3D • Wirtualną kolonoskopię • Perfuzja
Możliwość rozbudowy systemu o moduł do gromadzenia informacji o efektywnej dawce promieniowania wchłoniętego przez pacjenta w czasie badań radiologicznych
Możliwość oznaczania obrazów jako poufne, czyli widoczne jedynie dla uprawnionej grupy użytkowników.
Migracja posiadanych danych obrazowych ze starego systemu archiwum w zakresie wczytanie do nowego systemu oryginalnych danych obrazowych (Zamawiający udostępni oryginalne pliki DICOM z badaniami) lub podłączenie starego systemu jako drugi węzeł „tylko do odczytu” – z możliwością wyszukiwania danych i przeglądania obrazów.
<p>Wsparcie dla dostarczonego systemu</p> <p>Zgłaszanie awarii: w elektronicznym systemie zgłoszeń udostępnionym przez Wykonawcę (lub drogą mailową w przypadku braku takiego systemu), a także telefonicznie w dni robocze w godzinach 8:00-16:00.</p> <p>Zapewnienie pomocy telefonicznej (helpdesku) w systemie w godzinach 8:00-16:00 we wszystkie dni robocze.</p> <p>Usunięcie awarii (oprogramowania lub sprzętu) w następnym dniu roboczym od daty zgłoszenia</p> <p>Awaria zgłoszona w godzinach pomiędzy 16.00 a 24.00 dnia roboczego traktowana jest jak przyjęta o godz. 8.00 następnego dnia roboczego;</p> <p>Awaria zgłoszona w godzinach pomiędzy 0.00 a 8.00 dnia roboczego - traktowana jest jak przyjęty o godz. 8.00 danego dnia roboczego;</p> <p>Awaria zgłoszona w dniu ustawowo lub dodatkowo wolnym od pracy - traktowana jest jak przyjęty o godz. 8.00 najbliższego dnia roboczego;</p> <p>Wykonawca obejmie opieką serwisową wszystkie dostarczone elementy. Przez objęcie opieką serwisową zamawiający rozumie utrzymanie wyposażenia w niezakłóconym działaniu, konserwację zgodnie z wymogami producenta oraz dokonywanie wszelkich potrzebnych napraw.</p> <p>Wykonawca zapewni zdalne wsparcie systemu umożliwiające dokonywanie diagnozy awarii i napraw oprogramowania, oraz przedstawi imienny wykaz osób uprawnionych do pracy zdalnej.</p> <p>Zamawiający wymaga objęcia ochroną antywirusową zaoferowanych systemów posiadanych przez Zamawiającego programem antywirusowym.</p> <p>Rozbudowa sprzętowa systemu o dodatkowe zasoby dyskowe (rozbudowa macierzy archiwum) nie będzie wymagała od Zamawiającego wykupywania dodatkowych licencji a konfiguracja nowego</p>

sprzętu odbędzie się w ramach obowiązującej umowy.

W przypadku wymiany przez Zamawiającego urządzeń diagnostycznych podłączonych do zaoferowanych systemów Wykonawca wykona nieodpłatnie podłączenia nowych węzłów DICOM w ramach posiadanych licencji.

Nadzór autorski nad systemem

Zgłaszanie i usuwanie błędów w oprogramowaniu odbywać się będzie na zasadach zgłaszania awarii systemu opisanych powyżej.

Udostępnianie nowych wersji oprogramowania zgodnie z zaleceniami producenta. Nowe wersje oprogramowania są instalowane u Zamawiającego przez Wykonawcę, w sposób i liczbie pozwalającej na niezakłócone funkcjonowanie oprogramowania. Za aktualizację wersji oprogramowania u Zamawiającego odpowiedzialność ponosi Wykonawca, który ma zaplanować i przeprowadzić proces aktualizacji oprogramowania, w sposób zapewniający prawidłowe funkcjonowanie oprogramowania po zakończeniu procesu aktualizacji, na wszystkich stanowiskach objętych oprogramowaniem.

Instalacja aktualizacji i nowych wersji oprogramowania aplikacyjnego dostosowujących systemy do zmian ustawowych i wymogów jakie Zamawiający musi spełniać w obszarze zakresu i formatu danych przekazywanych innym podmiotom w terminach wejścia ich w życie.

Rozwój oprogramowania (nowe elementy systemu objętego niniejszym postępowaniem zgodnie ze zmieniającymi się powszechnie obowiązującymi przepisami prawa, przepisami prawa wewnętrznie obowiązującymi wydanymi na podstawie delegacji ustawowej). Wykonawca ma obowiązek dostarczać zamawiającemu nieodpłatnie oprogramowanie podlegające każdorazowo aktualizacji wynikającej ze zmieniających się przepisów prawa, dotyczy to również wszelkich zmian i aktualizacji zakresu przepisów wydawanych przez NFZ.

Wykonawca jest zobowiązany do stosowania wszystkich przepisów i regulaminów obowiązujących u Zamawiającego, które mogą mieć zastosowanie w realizacji niniejszego zamówienia, w tym obowiązujących wykładni prawnych lub wskazówek jednostek nadrzędnych (np. Narodowy Fundusz Zdrowia, Ministerstwo Zdrowia, Samorządowy Wydział Zdrowia, Organ Założycielski, inne).

System monitorowania i zarządzania infrastrukturą serwerów

System zarządzania infrastrukturą wirtualizacji serwerów musi spełniać następujące kryteria:

1. Rozwiązanie musi zapewnić możliwość obsługi wielu instancji systemów operacyjnych na jednym serwerze fizycznym.
2. Pojedynczy klaster może się skalować min. z 8 fizycznych hostów (serwerów) z zainstalowaną warstwą wirtualizacji.
3. Oprogramowanie do wirtualizacji zainstalowane na serwerze fizycznym musi obsługiwać i wykorzystać procesory fizyczne wyposażone w min 256 logicznych wątków oraz do min. 8 TB pamięci fizycznej RAM.
4. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych min. od 1 do 64 procesorowych.
5. Oprogramowanie do wirtualizacji musi zapewniać możliwość stworzenia dysku maszyny wirtualnej o wielkości do min. 4 TB.
6. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością przydzielenia do 1 TB pamięci operacyjnej RAM.
7. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć min. do 10 wirtualnych kart sieciowych.
8. Rozwiązanie musi umożliwiać łatwą i szybką rozbudowę infrastruktury o nowe usługi bez spadku wydajności i dostępności pozostałych wybranych usług.

9. Rozwiązanie powinno w możliwie największym stopniu być niezależne od producenta platformy sprzętowej.
10. Polityka licencjonowania musi umożliwiać przenoszenie licencji na oprogramowanie do wirtualizacji pomiędzy serwerami różnych producentów z zachowaniem wsparcia technicznego i zmianą wersji oprogramowania na niższą (downgrade). Licencjonowanie nie może odbywać się w trybie OEM.
11. Rozwiązanie musi wspierać następujące systemy operacyjne: Windows Server, Windows 7, Windows 10, Debian Linux, FreeBSD.
12. Rozwiązanie musi umożliwiać przydzielenie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera w celu osiągnięcia maksymalnego współczynnika konsolidacji.
13. Rozwiązanie musi umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie zarezerwowane na dyskach lokalnych serwera lub na macierzy.
14. Rozwiązanie powinno posiadać centralną konsolę graficzną do zarządzania maszynami wirtualnymi i do konfigurowania innych funkcjonalności. Dostęp do konsoli może być realizowany z poziomu przeglądarki internetowej z wykorzystaniem HTML.
15. 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.
16. Oprogramowanie do wirtualizacji powinno zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych (tzw. snapshot) na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy.
17. Oprogramowanie do wirtualizacji musi zapewnić możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi.
18. Oprogramowanie do wirtualizacji oraz oprogramowanie zarządzające musi posiadać możliwość integracji z usługami katalogowymi Microsoft Active Directory.
19. Rozwiązanie musi zapewniać mechanizm bezpiecznego uaktualniania warstwy wirtualizacyjnej (hosta, maszyny wirtualnej) bez potrzeby wyłączania wirtualnych maszyn. Mechanizm ten jest elementem składowym rozwiązania i nie wymaga dodatkowej licencji na system operacyjny.
20. Rozwiązanie musi zapewniać mechanizm replikacji wskazanych maszyn wirtualnych w obrębie klastra serwerów fizycznych.
21. Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych pomiędzy serwerami fizycznymi. Mechanizm powinien umożliwiać 4 lub więcej takich procesów przenoszenia jednocześnie.
22. Rozwiązanie musi mieć możliwość przenoszenia zwirtualizowanych dysków maszyn wirtualnych pomiędzy fizycznymi zasobami dyskowymi. Mechanizm powinien umożliwiać realizację co najmniej 2 takich procesów przenoszenia jednocześnie.
23. 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.
24. 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 min. 4000 portów.

25. 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.
26. Wirtualne przełączniki muszą obsługiwać wirtualne sieci lokalne (VLAN).

Licencje

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

Wykonawca określi i dostarczy ilości i rodzaje licencji wymaganych do realizacji Projektu inne niż wymagane, tj.:

- Microsoft Windows Server 2019² lub równoważny – zgodnie z warunkami licencjonowania do uruchomienia co najmniej 14 maszyn wirtualnych na wszystkich dostarczonych serwerach fizycznych (3 serwery – 6 procesorów).
- Licencje dostępowe (CAL) Domeny [device] – min. 230 szt. – przeznaczone do zastosowania w dostarczonym systemie domeny.
- Licencje dostępowe do systemu wirtualnego/zdalnego pulpitu – min. 230 szt. – zgodne z dostarczonym oprogramowaniem zdalnego pulpitu współpracującego z zaoferowanymi terminalami.
- System wirtualizacji – zgodnie z warunkami licencjonowania do uruchomienia co najmniej 300 maszyn wirtualnych na wszystkich serwerach Zamawiającego (8 serwerów – 16 procesorów fizycznych).

² Z uwagi na posiadanie oprogramowania pracującego jedynie w środowisku Microsoft Windows, Zamawiający wymaga dostarczenia licencji na system Microsoft Windows Server 2019 z możliwością dostarczenia oprogramowania równoważnego – z zastrzeżeniem, że Zamawiający nie dopuszcza wykorzystania emulacji systemów.

Zakres 2 – Konfiguracja i uruchomienie sprzętu oraz oprogramowania systemowego

Wszystkie dostarczane urządzenia muszą zostać zainstalowane [tj. wypakowane, zmontowane, zamontowane w szafach rack lub na biurkach, uruchomione i skonfigurowane] w docelowym miejscu pracy [wskazanym przez Zamawiającego] w terminie wskazanym przez Zamawiającego [miejsce i termin instalacji należy uzgodnić na min. 2 dni robocze przed planowaną dostawą urządzeń].

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

Serwery, przełączniki, macierz, UTM oraz wszystkie inne dostarczone w ramach tego postępowania urządzenia przeznaczone do instalacji w szafie RACK, muszą być zainstalowane w szafie RACK.

Serwery

Na serwerach należy zainstalować system wirtualizacji i skonfigurować go do korzystania z zasobów dyskowych macierzy. Wykonawca zaplanuje schemat rozmieszczeń, ilości i przydział zasobów dla wszystkich serwerów wirtualnych wymaganych do realizacji Przedmiotu Zamówienia.

Macierz dyskowa

Do macierzy należy podłączyć i skonfigurować wszystkie dyski w taki sposób, aby fizyczne i wirtualne maszyny uruchomione na serwerach fizycznych mogły korzystać z dysków macierzy w możliwie najszybszy sposób. Dyski NLSAS mają obsługiwać archiwum PACS.

Zabezpieczenie e-Uслуг

Wykonawca dokona instalacji fizycznej wszystkich wymaganych urządzeń teletechnicznych oraz dostarczanego sprzętu. Wszystkie urządzenia muszą zostać podłączone i uruchomione.

Wykonawca wdroży [tj. zainstaluje, uruchomi, skonfiguruje i przetestuje] infrastrukturę zapasową serwerów wirtualnych oraz procedurę przełączania usług. Na serwerach fizycznych Wykonawca utworzy infrastrukturę serwerów wirtualnych. Serwery wirtualne należy skonfigurować do korzystania z zasobów sieciowych i dyskowych. Wszystkie maszyny wirtualne muszą zostać skonfigurowane zgodnie z ich przeznaczeniem [np. Active Directory, DHCP, DNS, SQL, IIS, etc.].

Firewall – UTM

W konfiguracji urządzeń muszą zostać włączone min. usługi:

- ochrony przed atakami typu DoS/DDoS, itp.,
- ochrony antywirusowej,
- web filter,
- IDS/IPS.

Instalowane urządzenie musi chronić zainstalowane wewnątrz sieci Zamawiającego serwery aplikacyjne e-Uслуг [głównie przed atakami typu DoS, sql-injection, itp.]. Urządzenie należy podłączyć światłowodami z punktem styku sieci OLMAN.

Architektura Domeny

W celu zapewnienia wysokiego poziomu bezpieczeństwa wszystkich usług i danych, należy wdrożyć usługę Domeny – również w trybie HA, tj. min. 3 serwery wirtualne na min. 2 serwerach fizycznych

– zgodnie z zaleceniami producenta oprogramowania. W ramach wdrożenia należy uruchomić integrację systemu HIS z usługą logowania do domeny. W ramach tego zadania Wykonawca utworzy wspólnie z ASI polityki dostępu do systemów i zaimplementuje je w GPO. Podłączenie komputerów do domeny jest obowiązkiem Zamawiającego, Wykonawca musi jednak świadczyć usługę asysty w przypadku problemów z podłączeniem do domeny.

Architektura RDP

W ramach projektu, w celu udostępnienia obsługi e-Usług personelowi szpitala niezależnie od lokalizacji, zostanie uruchomiona usługa zdalnego pulpitu [RDP]. Usługa ta musi zostać uruchomiona w trybie HA, tj. min. 4 serwerów wirtualnych na min. 2 serwerach fizycznych. Aby w pełni wykorzystać infrastrukturę, należy uruchomić serwery loadbalancingu pomiędzy tymi serwerami [również w trybie HA np. z DNS round-robin].

Usługi wspomagające

DNS

Należy uruchomić min. dwa serwery DNS działające w trybie HA i skonfigurować wszystkie niezbędne usługi – w tym round-robin dla load balancerów. Usługa DNS musi posiadać możliwość włączenia filtrowania kategorii stron internetowych, których adresy system DNS będzie zwracał.

NTP

Należy uruchomić min. dwa serwery NTP działające w trybie HA lub wzajemnej synchronizacji i skonfigurować wszystkie usługi i urządzenia do korzystania z tych serwerów.

Wykonawca przeprowadzi instruktarze z całej instalowanej infrastruktury w trakcie wdrożenia.

Zakres 3 – Przygotowanie i dostarczenie dokumentacji projektowej oraz powykonawczej

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

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

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

Gwarancja i wsparcie

Świadczenie usługi gwarancji i wsparcia ma na celu zapewnienie ciągłości sprawnego działania Systemu poprzez realizację działań naprawczych wynikających z analizy ujawnionych problemów, wykrytych Dysfunkcji systemów, niewłaściwego działania systemu, spadku wydajności, wykryciu zagrożenia włamania, itp. Zakres i warunki opisane w §10 Umowy.

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

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

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

Wykonawca zapewni usługę wsparcia użytkowników udostępniając:

- usługę typu helpdesk, udostępnioną pod adresem e-mail, numerem telefonu
- portal typu helpdesk – dostępny on-line w trybie 356/7/24, gdzie będą publikowane m.in. statusy zgłoszeń oraz ich treść i historia korespondencji
- przez niniejszy portal będą mogły być dokonywane zgłoszenia Dysfunkcji

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

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

Wykonawca zapewni wystarczającą ilość konsultantów do zapewnienia ciągłości usługi gwarancji.

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

W ramach usługi Wykonawca zobowiązany jest do nieodpłatnego usuwania dysfunkcji:

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

Wykonawca musi informować Zamawiającego o dostępnych aktualizacjach i poprawkach Systemów.

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

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

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

Zgłoszenia będą klasyfikowane zgodnie ze słownikiem pojęć, zawartym w Załączniku nr 1 do niniejszego OPZ, przez Zamawiającego w uzgodnieniu z Wykonawcą.

Wykonawca zobowiązany jest do usunięcia dysfunkcji w terminach wymienionych w pkt 7 procedury podejmowania prac serwisowych zawartej w Załączniku nr 1 do niniejszego OPZ.

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

Terminy wymienione w Załączniku nr 1 do niniejszego OPZ obowiązują również w przypadku dostarczonego sprzętu.