Załącznik Nr 2 Opis przedmiotu zamówienia

OPIS PRZEDMIOTU ZAMÓWIENIA

I. Nazwa:

Informatyzacja Regionalnego Szpitala w Kołobrzegu w ramach projektu pn. „Przyspieszenie procesów transformacji cyfrowej ochrony zdrowia poprzez dalszy rozwój usług cyfrowych w ochronie zdrowia”

II. Nazwy i kody Wspólnego Słownika Zamówień (Klasyfikacji CPV):

48180000-3 - Pakiety oprogramowania medycznego,
48780000-9 - Pakiety oprogramowanie do zarządzania systemem, przechowywaniem i zawartością
48000000-8 - Pakiety oprogramowania i systemy informatyczne (w tym 48600000-4 - Pakiety oprogramowania dla baz danych i operacyjne),
48700000-5 - Pakiety oprogramowania użytkowego,
30233000-1 – Urządzenia do przechowywania i odczytu danych
48820000-2 – Serwery.
48600000-4 – Pakiety oprogramowanie dla baz danych i operacyjne,
72000000-5 - Usługi informatyczne: konsultacyjne, opracowywania oprogramowania, internetowe i wsparcia (w tym 72263000-6 - Usługi wdrażania oprogramowania).

SPIS TREŚCI

Rozdział I. Założenia początkowe oraz wymagania ogólne

I.1 Charakterystyka podmiotu leczniczego

Regionalny Szpital w Kołobrzegu zwany dalej „Zamawiającym", jest podmiotem leczniczym niebędącym przedsiębiorcą, w rozumieniu przepisów ustawy o działalności leczniczej.

Głównym celem działania Szpitala jest wykonywanie działalności leczniczej polegającej na udzielaniu świadczeń zdrowotnych oraz promocji zdrowia. Szpital posiada 13 oddziałów szpitalnych, 2 oddziały dzienne, 23 poradnie specjalistyczne wraz z Blokiem Operacyjnym i Zakładem Rehabilitacji. Dodatkowo dysponuje Zakładem Diagnostyki Obrazowej, Laboratorium Analitycznym i Mikrobiologicznym.

I.2 Akty prawne

Dostarczone rozwiązania teleinformatyczne, ze szczególnym uwzględnieniem dostarczanego i wdrażanego Oprogramowania, muszą być zgodne z powszechnie obowiązującymi przepisami prawa polskiego i europejskiego. Oprogramowanie musi pozwalać na gromadzenie, przetwarzanie i analizowanie danych i informacji w obszarach objętych wdrożeniem. Na bazie tych danych System musi umożliwiać wytwarzanie prawidłowej, kompletnej, ujętej w obowiązujących przepisach prawa dokumentacji (dokumenty, raporty, wykazy, oświadczenia, zaświadczenia itp.).

Rozdział II. Szczegółowy opis przedmiotu zamówienia

II.1 Zakup i wdrożenie kompletnego systemu gromadzenia danych medycznych PACS z dodatkowymi modułami oraz jego integracja z innymi systemami informatycznymi szpitala

Stan obecny

Obecnie Zamawiający użytkuje system gromadzenia danych medycznych PACS firmy AGFA HealthCare o nazwie Impax 6. System posiada głęboką integrację z radiologicznym systemem informatycznym RIS firmy TMS-Soft Sp. z o.o. pod nazwą Vizo. Do systemu przesyłane są dane z urządzeń typu:

- Rezonans komputerowy (MR)
- Tomograf komputerowy (CT)
- Aparaty Rentgenowskie
- Angiograf mobilny
- Aparaty mobilny RTG z ramieniem C
- Aparaty USG
- Endoskopy

Opis ogólny

Przedmiotem zamówienia jest zakup i wdrożenie kompletnego systemu gromadzenia danych medycznych PACS z dodatkowymi modułami oraz jego integracja z innymi systemami informatycznymi szpitala. System musi zawierać platformę techniczną niezbędną do jego instalacji i wdrożenia. Wykonawca dokona migracji danych z obecnie wykorzystywanego systemu PACS do nowego systemu.

Zabezpieczenie techniczne systemu

II.1.3.1. Macierz dyskowa – 1szt.

Lp.	Parametr	Charakterystyka (wymagania minimalne)
1.3.1.1.	**Obudowa**	Do instalacji w standardowej szafie RACK 19”, macierz musi zajmować maksymalnie 2U i pozwalać na instalacje 24 dysków 2.5”.
1.3.1.2.	**Kontrolery**	Dwa kontrolery RAID pracujące w układzie active-active posiadające łącznie minimum osiem portów 32Gb FC w standardzie SFP28
1.3.1.3.	**Kable/wkładki**	8 wkładek 32Gb FC SFP28 MM 8 kabli LC/UPC-LC/UPC OM4 min. 5m
1.3.1.4.	**Cache**	16GB na kontroler, pamięć cache zapisu mirrorowana między kontrolerami, przechowywana przez min. 72h w razie awarii.
1.3.1.5.	**Dyski**	Zainstalowane: • 8 dysków Hot-Plug o pojemności 1.92TB SAS SSD 12Gbps 2,5” • 16 dysków Hot-Plug o pojemności 2.4TB SAS 12Gbps 2,5”

		Możliwość rozbudowy przez dokładanie kolejnych dysków/półek dyskowych do łącznie minimum 276 dysków. Możliwość mieszania typów dysków w obrębie macierzy oraz pojedynczej półki.
1.3.1.6.	**Oprogramowanie/ Funkcjonalności**	1.3.1.6.1. Zarządzanie macierzą poprzez minimum przeglądarkę internetową, GUI oparte o HTML5. 1.3.1.6.2. Macierz powinna zostać dostarczona z licencją umożliwiającą utworzenie minimum 512 LUN'ów oraz 1024 kopii migawkowych na całą macierz. 1.3.1.6.3. Konieczne jest posiadanie automatycznego, bez interwencji człowieka, rozkładania danych między dyskami poszczególnych typów (tzw. auto-tiering). Dane muszą być automatycznie przemieszczane między rożnymi typami dysków. 1.3.1.6.4. Możliwość wykorzystania dysków SSD jako cache macierzy, możliwość rozbudowy pamięci cache do min. 8TB poprzez dyski SSD. 1.3.1.6.5. Licencja zaoferowanej macierzy powinna umożliwiać podłączanie minimum 8 hostów bez konieczności zakupu dodatkowych licencji. 1.3.1.6.6. Macierz musi posiadać funkcjonalność zdalnej replikacji danych do macierzy tej samej rodziny w trybie asynchronicznym.
1.3.1.7.	**Wsparcie dla systemów operacyjnych**	Windows Server 2025, Windows Server 2022, Windows Server 2019, Windows Server 2016, Red Hat Enterprise Linux 9.x (RHEL), SLES 15, Vmware ESXi 8.0, Citrix XenServer 8.x
1.3.1.8.	**Bezpieczeństwo**	Ciągła praca obu kontrolerów nawet w przypadku zaniku jednej z faz zasilania. Zasilacze, wentylatory, kontrolery RAID redundantne.
1.3.1.9.	**Warunki gwarancji dla macierzy**	36 miesięcy gwarancji realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 365x7x24 poprzez ogólnopolską linię telefoniczną producenta. Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia, oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji macierzy. • Wszystkie naprawy gwarancyjne powinny być możliwe na miejscu.

		• W czasie obowiązywania gwarancji dostawca zobowiązany jest do udostępnienia Zamawiającemu nowych wersji BIOS, firmware i sterowników (na płytach CD lub stronach internetowych).
1.3.1.10.	**Dokumentacja użytkownika**	Zamawiający wymaga dokumentacji w języku polskim lub angielskim
1.3.1.11.	**Certyfikaty**	Macierz musi być wyprodukowany zgodnie z normą ISO 9001:2015.

II.1.3.2. Serwer typ 1 – 2 szt.

Lp.	Parametr	Charakterystyka (wymagania minimalne)
1.3.2.1.	**Obudowa**	Obudowa Rack o wysokości max 2U. Możliwość instalacji minimum 24 dysków 3.5”. Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli.
1.3.2.2.	**Płyta główna**	Płyta główna z możliwością zainstalowania do dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.
1.3.2.3.	**Chipset**	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych
1.3.2.4.	**Procesor**	Zainstalowany jeden procesor 12-rdzeniowy klasy x86, min. 2.4 GHz, dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 239 w teście SPECrate2017_int_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej.
1.3.2.5.	**RAM**	Minimum 32 GB DDR5 RDIMM 5600MT/s, na płycie głównej powinno znajdować się minimum 16 slotów przeznaczone do instalacji pamięci. Płyta główna powinna obsługiwać do 1.5 TB pamięci RAM.
1.3.2.6.	**Gniazda PCI**	Min. 5 slotów PCIe Gen4, w tym min. 4 sloty x16.
1.3.2.7.	**Interfejsy sieciowe/FC/SAS**	• Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie Base-T • 1 dodatkowa dwuportowa karta 10/25Gb SFP28 (w slocie OCP) wraz z wkładkami 10Gb SFP+ SR. • 2 kable LC/UPC-LC/UPC OM4 min. 5m • 1 kabel UTP kat 5E min 5m • 2 wkładki 10Gb SFP+ SR do oferowanych przełączników w celu podłączenia serwera.
1.3.2.8.	**Dyski twarde**	• Możliwość instalacji dysków SAS, SATA, SSD. • Zainstalowane 16 dysków NL-SAS o pojemności min. 8TB, 12Gb, 3,5“ Hot-Plug. • Zainstalowane dwa dyski M.2 NVMe SSDs o pojemności min. 480GB Hot-Plug z możliwością konfiguracji RAID 1

1.3.2.9.	**Kontroler RAID**	Sprzętowy kontroler dyskowy, posiadający min. 8GB nieulotnej pamięci cache, możliwe konfiguracje poziomów RAID: 0, 1, 5, 6, 10, 50, 60. Wsparcie dla dysków samoszyfrujących.
1.3.2.10.	**Wbudowane porty**	• 3x USB, w tym min. 1 port USB 3.0 • 1 port VGA,
1.3.2.11.	**Video**	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920 x 1200
1.3.2.12.	**Wentylatory**	Redundantne
1.3.2.13.	**Zasilacze**	Redundantne, Hot-Plug min. 1100W każdy wraz z kablami zasilającymi o długości min. 4m.
1.3.2.14.	**System operacyjny/ dodatkowe oprogramowanie**	Windows Server 2025 Standard na 16 rdzenie.
1.3.2.15.	**Bezpieczeństwo**	• Zatrzask górnej pokrywy • Możliwość wyłączenia w BIOS funkcji przycisku zasilania. • BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła • Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. • Moduł TPM 2.0 • Możliwość dynamicznego włączania I wyłączania portów USB na obudowie – bez potrzeby restartu serwera • Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem
1.3.2.16.	**Diagnostyka**	Diody informujące o stanie serwera: stan dobry, awaria.
1.3.2.17.	**Karta Zarządzania**	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: • zdalny dostęp do graficznego interfejsu Web karty zarządzającej; • zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); • szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika; • możliwość podmontowania zdalnych wirtualnych napędów; • wirtualną konsolę z dostępem do myszy, klawiatury; • wsparcie dla IPv6; • wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; • możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer;

		• możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; • integracja z Active Directory; • możliwość obsługi przez dwóch administratorów jednocześnie; • wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. • możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera • możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera • Wirtualny schowek ułatwiający korzystanie z konsoli zdalnej
1.3.2.18.	**Certyfikaty**	• Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 • Serwer musi posiadać deklarację CE. • Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows" dla systemów Microsoft Windows Server 2019, Microsoft Windows Server 2022, Microsoft Windows Server 2025
1.3.2.19.	**Warunki gwarancji**	• Gwarancji producenta: 36 miesięcy • Możliwość rozszerzenia gwarancji przez producenta do 7 lat. • Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie oraz przez Internet • Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik wykonawcy / producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) ma rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbywać w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. • Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie wykonawcy. • Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta, w tym także sprzedanego oprogramowania. • Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon/portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na

		identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu. • Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. • Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera. • Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. • Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty. • Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. • Wymagane dołączenie do oferty oświadczenia Producenta potwierdzające, że serwer pochodzi z autoryzowanego kanału dystrybucji producenta.
1.3.2.20.	**Dokumentacja użytkownika**	• Zamawiający wymaga dokumentacji w języku polskim lub angielskim. • Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.

II.1.3.3. Serwer typ 2 – 3 szt.

Lp.	Parametr	Charakterystyka (wymagania minimalne)
1.3.3.1.	**Obudowa**	• Obudowa Rack o wysokości max 1U z możliwością instalacji min. 10 dysków 2,5” wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli. • Serwer wyposażony w panel LCD umieszczony na froncie obudowy • Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera

		przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI.
1.3.3.2.	**Płyta główna**	• Płyta główna z możliwością zainstalowania do dwóch procesorów. • Obsługa procesorów 64 rdzeniowych. • Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. • Płyta główna powinna obsługiwać do 8TB pamięci RAM. w konfiguracji dwuprocesorowej.
1.3.3.3.	**Chipset**	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych.
1.3.3.4.	**Procesor**	Zainstalowany jeden procesor 16-rdzeniowy, min. 2GHz, klasy x86 dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 266 w teście SPECrate2017_int_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej.
1.3.3.5.	**RAM**	• Minimum 128GB DDR5 RDIMM 5600MT/s, • Na płycie głównej powinno znajdować się minimum 32 slotów przeznaczonych do instalacji pamięci.
1.3.3.6.	**Gniazda PCI**	• minimum trzy sloty PCIe z czego 2 sloty Gen5
1.3.3.7.	**Interfejsy sieciowe/FC/SAS**	• Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT (porty nie mogą być osiągnięte poprzez karty w slotach PCIe) • 2 interfejsy sieciowe 10/25Gb Ethernet w standardzie SFP28 (porty nie mogą być osiągnięte poprzez karty w slotach PCIe), porty obsadzone modułami 10Gbs SFP+ SR • Dodatkowa, dwuportowa kart FC 32Gb wraz z wkładkami MM • 4 kable LC/UPC-LC/UPC OM4 min. 5m • 1 kabel UTP kat 5E min 5m • 2 wkładki 10Gb SFP+ SR do oferowanych przełączników w celu podłączenia serwera.
1.3.3.8.	**Dyski twarde**	• Zainstalowane dwa dyski 600GB SAS 12Gbps 10k 512n 2.5in Hot-Plug • Możliwość zainstalowania dwóch dysków M.2 NVMe SSDs o pojemności min. 960GB Hot-Plug z możliwością konfiguracji RAID 1.
1.3.3.9.	**Kontroler RAID**	Sprzętowy kontroler dyskowy, posiadający min. 8GB nieulotnej pamięci cache, możliwe konfiguracje poziomów RAID: 0, 1, 5, 6, 10, 50, 60.
1.3.3.10.	**Wbudowane porty**	4 x USB z czego nie mniej niż 1x USB 3.0, 1x VGA

1.3.3.11.	**Video**	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200
1.3.3.12.	**Zasilacze**	Redundantne, Hot-Plug min. 1100W każdy wraz z kablami zasilającymi o długości min. 4m.
1.3.3.13.	**Bezpieczeństwo**	• Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. • Możliwość wyłączenia w BIOS funkcji przycisku zasilania. • BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła • Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. • Moduł TPM 2.0 • Możliwość dynamicznego włączania I wyłączania portów USB na obudowie – bez potrzeby restartu serwera • Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem
1.3.3.14.	**Karta Zarządzania**	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: • zdalny dostęp do graficznego interfejsu Web karty zarządzającej; • zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); • szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika; • możliwość podmontowania zdalnych wirtualnych napędów; • wirtualną konsolę z dostępem do myszy, klawiatury; • wsparcie dla IPv6; • wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; • możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; • możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; • integracja z Active Directory; • możliwość obsługi przez dwóch administratorów jednocześnie; • wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. • możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera

		• możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera • Wirtualny schowek ułatwiający korzystanie z konsoli zdalnej
1.3.3.15.	**Certyfikaty**	• Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 • Serwer musi posiadać deklaracja CE. • Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows" dla systemów Microsoft Windows Server 2019, Microsoft Windows Server 2022, Microsoft Windows Server 2025.
1.3.3.16.	**Dokumentacja użytkownika**	• Zamawiający wymaga dokumentacji w języku polskim lub angielskim. • Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.
1.3.3.17.	**Warunki gwarancji**	• Gwarancji producenta: 36 miesięcy • Możliwość rozszerzenia gwarancji przez producenta do 7 lat. • Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet. • Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik wykonawcy / producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) ma rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbywać w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. • Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie wykonawcy. • Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta, w tym także oprogramowania. • Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon/ portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu.

		• Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. • Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera. • Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. • Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty. • Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. • Wymagane dołączenie do oferty oświadczenia Producenta potwierdzające, że serwer pochodzi z autoryzowanego kanału dystrybucji producenta.

II.1.3.4. Serwer typ 3 – 2 szt.

Lp.	Parametr	Charakterystyka (wymagania minimalne)
1.3.4.1.	**Obudowa**	• Obudowa Rack o wysokości max 2U z możliwością instalacji min. 8 dysków 2,5" Hot-Plug SATA/SAS/NVMe wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli. • Serwer wyposażony w panel LCD umieszczony na froncie obudowy • Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI.
1.3.4.2.	**Płyta główna**	Płyta główna z możliwością zainstalowania jednego procesora. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.
1.3.4.3.	**Chipset**	Dedykowany przez producenta procesora do pracy w serwerach jednoprocesorowych

1.3.4.4.	**Procesor**	• Zainstalowany jeden procesor 48-rdzeniowy, min. 2.75GHz, klasy x86 dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 518 w teście SPECrate2017_int_base w konfiguracji jedno procesorowej, dostępnym na stronie www.spec.org. • Możliwość obsługi procesorów 128-rdzeniowych
1.3.4.5.	**RAM**	Minimum 256GB DDR5 RDIMM 5600MT/s, na płycie głównej powinno znajdować się minimum 12 slotów przeznaczonych do instalacji pamięci. Płyta główna powinna obsługiwać do min. 3TB pamięci RAM.
1.3.4.6.	**Gniazda PCI**	Minimum 4 sloty PCIe, z czego przynajmniej 2 x16
1.3.4.7.	**Interfejsy sieciowe/FC/SAS**	• Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 2 interfejsy sieciowe 10/25Gb Ethernet w standardzie SFP28 (porty nie mogą być osiągnięte poprzez karty w slotach PCIe). Interfejsy SFP28 muszą być wyposażone we wkładki 10Gb SFP+ SR. • Dodatkowa, dwuportowa karta FC 32Gb wraz z wkładkami MM • 4 kable LC/UPC-LC/UPC OM4 min. 5m • 1 kabel UTP kat 5E min 5m • 2 wkładki 10Gb SFP+ SR do oferowanych przełączników w celu podłączenia serwera.
1.3.4.8.	**Dyski twarde**	• Zainstalowane dwa dyski 600GB SAS 12Gbps 10k 512n 2.5in Hot-Plug • Możliwość zainstalowania dwóch dysków M.2 NVMe SSDs o pojemności min. 960GB Hot-Plug z możliwością konfiguracji RAID 1.
1.3.4.9.	**Kontroler RAID**	Sprzętowy kontroler dyskowy, możliwe konfiguracje poziomów RAID: 0, 1, 10
1.3.4.10.	**Wbudowane porty**	• 4x USB w tym przynajmniej 1x USB 3.0 • 1x port VGA
1.3.4.11.	**Video**	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1080
1.3.4.12.	**Wentylatory**	Redundantne
1.3.4.13.	**Zasilacze**	Redundantne, Hot-Plug min.1100W każdy wraz z kablami zasilającymi o długości min. 4m.
1.3.4.14.	**Bezpieczeństwo**	• Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. • Możliwość wyłączenia w BIOS funkcji przycisku zasilania. • BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła • Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. • Moduł TPM 2.0

		• Możliwość dynamicznego włączania i wyłączania portów USB na obudowie – bez potrzeby restartu serwera • Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem
1.3.4.15.	**Karta Zarządzania**	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: • zdalny dostęp do graficznego interfejsu Web karty zarządzającej; • zdalne monitorowanie i informowanie o statusie serwera (np. prędkości obrotowej wentylatorów, konfiguracji serwera); • szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika; • możliwość podmontowania zdalnych wirtualnych napędów; • wirtualną konsolę z dostępem do myszy, klawiatury; • wsparcie dla Ipv6; • wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; • możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; • możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; • integracja z Active Directory; • możliwość obsługi przez dwóch administratorów jednocześnie; • wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. • możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera • możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera
1.3.4.16.	**Certyfikaty**	• Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 • Serwer musi posiadać deklaracja CE. • Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2019, Microsoft Windows Server 2022, Microsoft Windows Server 2025.
1.3.4.17.	**Dokumentacja użytkownika**	• Zamawiający wymaga dokumentacji w języku polskim lub angielskim. • Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu

		numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.
1.3.4.18.	**Warunki gwarancji**	• Gwarancji producenta: 36 miesięcy • Możliwość rozszerzenia gwarancji przez producenta do 7 lat. • Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet. • Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik wykonawcy / producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) ma rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbywać w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. • Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie wykonawcy. • Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta, w tym także oprogramowania. • Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon/ portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu. • Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. • Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera. • Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. • Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.

		• Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. • Wymagane dołączenie do oferty oświadczenia Producenta potwierdzające, że serwer pochodzi z autoryzowanego kanału dystrybucji producenta.

II.1.3.5. Serwer typ 4 – 2 szt.

Lp.	Parametr	Charakterystyka (wymagania minimalne)
1.3.5.1.	**Obudowa**	• Obudowa Rack o wysokości max 2U z możliwością instalacji min. 8 dysków 2,5" Hot-Plug SATA/SAS/NVMe wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli. • Serwer wyposażony w panel LCD umieszczony na froncie obudowy • Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI.
1.3.5.2.	**Płyta główna**	Płyta główna z możliwością zainstalowania dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.
1.3.5.3.	**Chipset**	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych
1.3.5.4.	**Procesor**	• Zainstalowane dwa procesory 32-rdzeniowe, min. 3.25GHz, klasy x86 dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 743 w teście SPECrate2017_int_base w konfiguracji dwuprocesorowej, dostępnym na stronie www.spec.org. • Możliwość obsługi procesorów 128 rdzeniowych
1.3.5.5.	**RAM**	Minimum 256GB DDR5 RDIMM 5600MT/s, na płycie głównej powinno znajdować się minimum 24 sloty przeznaczone do instalacji pamięci. Płyta główna powinna obsługiwać do min. 6TB pamięci RAM.
1.3.5.6.	**Gniazda PCI**	Minimum 8 slotów PCIe, z czego przynajmniej 2 x16
1.3.5.7.	**Interfejsy sieciowe/FC/SAS**	• Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT (porty nie mogą być osiągnięte poprzez karty w slotach PCIe).

		• 2 interfejsy sieciowe 10/25Gb Ethernet w standardzie SFP28 (porty nie mogą być osiągnięte poprzez karty w slotach PCIe). Interfejsy SFP28 muszą być wyposażone we wkładki 10Gb SFP+ SR. • Dodatkowa, dwuportowa karta FC 32Gb wraz z wkładkami MM • 4 kable LC/UPC-LC/UPC OM4 min. 5m • 1 kabel UTP kat 5E min 5m • 2 wkładki 10Gb SFP+ SR do oferowanych przełączników w celu podłączenia serwera.
1.3.5.8.	**Dyski twarde**	• Zainstalowane dwa dyski 600GB SAS 12Gbps 10k 512n 2.5in Hot-Plug • Możliwość zainstalowania dwóch dysków M.2 NVMe SSDs o pojemności min. 960GB Hot-Plug z możliwością konfiguracji RAID 1.
1.3.5.9.	**Kontroler RAID**	Sprzętowy kontroler dyskowy, możliwe konfiguracje poziomów RAID: 0, 1, 10
1.3.5.10.	**Wbudowane porty**	• 4x USB w tym przynajmniej 1x USB 3.0 • 1x port VGA
1.3.5.11.	**Video**	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1080
1.3.5.12.	**Wentylatory**	Redundantne
1.3.5.13.	**Zasilacze**	Redundantne, Hot-Plug min.1100W każdy wraz z kablami zasilającymi o długości min. 4m.
1.3.5.14.	**Bezpieczeństwo**	• Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. • Możliwość wyłączenia w BIOS funkcji przycisku zasilania. • BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła • Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. • Moduł TPM 2.0 • Możliwość dynamicznego włączania i wyłączania portów USB na obudowie – bez potrzeby restartu serwera • Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem
1.3.5.15.	**Karta Zarządzania**	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: • zdalny dostęp do graficznego interfejsu Web karty zarządzającej;

		• zdalne monitorowanie i informowanie o statusie serwera (np. prędkości obrotowej wentylatorów, konfiguracji serwera); • szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika; • możliwość podmontowania zdalnych wirtualnych napędów; • wirtualną konsolę z dostępem do myszy, klawiatury; • wsparcie dla Ipv6; • wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; • możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; • możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; • integracja z Active Directory; • możliwość obsługi przez dwóch administratorów jednocześnie; • wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. • możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera • możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera
1.3.5.16.	**Certyfikaty**	• Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 • Serwer musi posiadać deklaracja CE. • Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2019, Microsoft Windows Server 2022, Microsoft Windows Server 2025.
1.3.5.17.	**Dokumentacja użytkownika**	• Zamawiający wymaga dokumentacji w języku polskim lub angielskim. • Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.
1.3.5.18.	**Warunki gwarancji**	• Gwarancji producenta: 36 miesięcy • Możliwość rozszerzenia gwarancji przez producenta do 7 lat. • Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet. • Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik wykonawcy /

		producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) ma rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbywać w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. • Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie wykonawcy. • Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta, w tym także oprogramowania. • Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon/ portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu. • Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. • Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera. • Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. • Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty. • Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. • Wymagane dołączenie do oferty oświadczenia Producenta potwierdzające, że serwer pochodzi z autoryzowanego kanału dystrybucji producenta.

II.1.3.6. Wdrożenie platformy macierzowo-serwerowej (pozycje II.1.3.1-II.1.3.5)

Lp.	Wymagania i zakres ogólny dotyczący wszystkich elementów
1.3.6.1.	Instalacja urządzeń w szafach RACK w miejscu wskazanym przez Zamawiającego
1.3.6.2.	Okablowanie urządzeń dla ruchu LAN, SAN i zarządzanie w sposób udokumentowany i zalecany przez producenta dostarczanego urządzenia. Topologia połączeń w pełni redundantna. Awarią pojedynczego interfejsu i/lub komponentu nie może powodować przerwy w dostępie do usług świadczonych przez dane urządzenie lub oprogramowanie. Połączenie do elementów infrastruktury wskazanych przez Zamawiającego.
1.3.6.3.	Okablowanie połączeń zasilania.
1.3.6.4.	Opis wszystkich połączeń fizycznych przy pomocy naklejek/etykiet naklejanych na kable.
1.3.6.5.	Organizacja okablowania w organizerach kabli w sposób schludny i funkcjonalny
1.3.6.6.	Adresacja konsol Zarządzania według adresacji podanej przez Zamawiającego.
1.3.6.7.	Udostępnienie zasobów dyskowych (blokowych) macierzy według specyfikacji Zamawiającego (ilości i wielkości wolumenów).

II.1.3.7. Szafa Rack 42U – 1 szt.

Lp.	Parametr	Charakterystyka (wymagania minimalne)
1.3.7.1.	**Wysokość**	42U
1.3.7.2.	**Szerokość**	800 mm
1.3.7.3.	**Głębokość**	1090 mm
1.3.7.4.	**Maksymalna głębokość montażowa (urządzenia)**	Min. 939 mm
1.3.7.5.	**Szerokość szyn montażowych**	482,6 mm (19 cali)
1.3.7.6.	**Ilość belek nośnych**	• Dwie pary belek nośnych z możliwością regulacji położenia. • Wskaźnik głębokości ułatwiający regulację - numeracja punktów mocowania belek ze wskazaniem aktualnego położenia.
1.3.7.7.	**Wykonanie drzwi przednich**	Metalowe, jednoskrzydłowe, perforowane z klamką i zamkiem, możliwość zmiany kierunku otwierania drzwi
1.3.7.8.	**Wykonanie drzwi tylnych**	Metalowe, dwuskrzydłowe, perforowane z zamkiem trzypunktowym z klamką
1.3.7.9.	**Kąt otwarcia drzwi przednich i tylnych**	Min. 120°
1.3.7.10.	**Ściągane panele boczne**	Tak, osłony boczne połówkowe (4 szt.) z zamkami

1.3.7.11.	**Możliwość łączenia szaf**	Tak, zintegrowane wsporniki umożliwiające połączenie szaf w układy szeregowe
1.3.7.12.	**Otwory kablowe**	Tak, w panelu dachowym min. 4 okrągłe otwory o średnicy min. 50 mm oraz z tyłu panelu dachowego podłużne wycięcie o szerokości min. 360 mm.
1.3.7.13.	**Stopki poziomujące**	Tak
1.3.7.14.	**Kółka**	Tak, fabrycznie zainstalowane z możliwością demontażu
1.3.7.15.	**Zestaw przewodów uziemiających**	Tak, przewody uziemiające z możliwością beznarzędziowego rozłączenia
1.3.7.16.	**Numeracja jednostek U na belkach nośnych**	Tak
1.3.7.17.	**Nośność**	• Statyczna (na stopkach): 1580 kg • Dynamiczna (toczenie na kółkach): 1020 kg
1.3.7.18.	**Materiał wykonania**	Stal walcowana na zimno
1.3.7.19.	**Wykończenie powierzchni**	Malowane farbą proszkową, kolor czarny
1.3.7.20.	**Wymagania dodatkowe**	• Szafa w pełni zmontowana. • Możliwość beznarzędziowego demontażu drzwi, paneli bocznych i dachu. • Prowadnice montażowe 0U, znajdujące się z tyłu szafy po obydwu stronach, umożliwiające beznarzędziową instalację oferowanych listew zasilających PDU oraz opcjonalnych pionowych organizerów kabli. Możliwość montażu 2 listew PDU z każdej prowadnicy. • Zestaw 50 kompletów śruby montażowych M6.
1.3.7.21.	**Waga**	Maks. 170 kg
1.3.7.22.	**Certyfikaty i zgodność**	TIA/EIA 310-D, IEC 60950-1, CE, RoHS
1.3.7.23.	**Gwarancja**	Gwarancji producenta min. 3 lata

II.1.3.8. Zasilacz awaryjny UPS – 1 szt.

Zasilacz awaryjny UPS o mocy 11000VA 3:1 z dodatkowymi modułami bateryjnymi

Lp.	Parametr	Charakterystyka (wymagania minimalne)
1.3.8.1.	**Moc znamionowa (VA / W)**	11000VA / 10000W
1.3.8.2.	**Topologia**	online z podwójną konwersją
1.3.8.3.	**System korekcji współczynnika mocy (PFC)**	Tak
1.3.8.4.	**Odbudowa**	Możliwość instalacji wieżowej i montażu w szafie Rack 19”

1.3.8.5.	**Wysokość w szafie Rack**	UPS wraz z wymaganymi modułami bateryjnymi maks. 12U
1.3.8.6.	**Głębokość**	Maks. 700 mm
1.3.8.7.	**Zakres napięcia wejściowego**	305V-478V
1.3.8.8.	**Napięcie wejściowe**	380/400/415V
1.3.8.9.	**Częstotliwość wejściowa**	50/60 Hz (autodetekcja)
1.3.8.10.	**Zakres częstotliwości wejściowej**	Dla 50Hz: 40-60Hz Dla 60Hz: 50-70Hz
1.3.8.11.	**Prąd zwarciowy**	150 A
1.3.8.12.	**THDI**	<5%
1.3.8.13.	**Napięcie nominalne wyjściowe**	230/240V +/-1%
1.3.8.14.	**Całkowite zniekształcenia napięcia wyjściowego THDU**	<2%
1.3.8.15.	**Gniazda wyjściowe**	• 4 szt. IEC C19 (16A) • Listwa zaciskowa
1.3.8.16.	**Zdolność przeciążeniowa**	102–110%: 120s, 110–125%: 60s, 125–150%: 10s, >150%: 900ms
1.3.8.17.	**Sprawność (praca normalna)**	94,5% w trybie online (98% w trybie wysokiej sprawności)
1.3.8.18.	**Częstotliwość wyjściowa**	50/60 Hz automatycznie wykrywane lub konfigurowalne jako przetwornik częstotliwości
1.3.8.19.	**Współczynnik szczytu obciążenia**	3:1
1.3.8.20.	**Wewnętrzna funkcja obejścia**	Tak
1.3.8.21.	**Zewnętrznym moduł obejścia serwisowego (Maintenance Bypass)**	Tak
1.3.8.22.	**Możliwość wydłużenia czasu podtrzymania poprzez dodatkowe zewnętrzne moduły bateryjne**	Tak, do min. 11 modułów bateryjnych
1.3.8.23.	**Maksymalna wysokość jednego dodatkowego modułu bateryjnego**	3U
1.3.8.24.	**Oczekiwany czas podtrzymania dla obciążenia o mocy 10000W**	18 minut

1.3.8.25.	**Czas podtrzymania dla odciążenia o mocy 5000W**	42 minut
1.3.8.26.	**Zarządzanie akumulatorami**	• System ładowania nieciągłego baterii i z kompensacją temperatury. Do oferty dołączyć należy opis algorytmu ładowania nieciągłego baterii. W opisie znaleźć się muszą informacje nt. trwania okresów ładowania forsującego, konserwującego i okresu spoczynkowego (tzw. restingu). Okres spoczynkowy w jednym cyklu nie może być krótszy niż 14 dni. Opis powinien być materiałem firmowym producenta lub musi być przez niego potwierdzony. • Automatyczne sprawdzanie akumulatora, ochrona przed głębokim rozładowaniem, automatyczne rozpoznawanie dodatkowych akumulatorów zewnętrznych, wymiana akumulatorów „na gorąco" bez konieczności zamykania podłączonych urządzeń.
1.3.8.27.	**Interfejs użytkownika**	Wyświetlacz LCD obrotowy (informacje o statusie i pomiarach parametrów UPS, możliwość pomiaru zużycia energii w kWh)
1.3.8.28.	**Standardowe gniazda komunikacyjne**	• Komunikacyjna karta sieciowa web/SNMP • 1 port USB • 1 port szeregowy RS232 • 4 styki beznapięciowe • 1 blok zacisków do zdalnego załączania/ wyłączania • 1 blok zacisków do zdalnego wyłącznika awaryjnego
1.3.8.29.	**Komunikacyjna karta sieciowa web/SNMP**	• Protokoły i certyfikaty cyberbezpieczeństwa: UL 2900-1, IEC 62443-4-2, HTTPS, MQTTS, RADIUS, LDAP, SSH, pakiet szyfrów TLS 1.2 z minimum SHA256 • certyfikaty CA i PKI • prędkość Gigabit Ethernet • różne poziomy nadawania dostępu do konta administratora lub użytkownika • karta z możliwością wyposażenia w opcjonalny czujnik monitorowania warunków środowiskowych - umożliwiający zdalne monitorowanie temperatury, wilgotności i dwóch urządzeń stykowych, możliwość podłączenia do 3 czujników (połączonych łańcuchowo)
1.3.8.30.	**Oprogramowanie zarządzające**	Opcjonalne oprogramowanie producenta zasilacza UPS do monitorowania i zarządzania, ze wsparciem dla VMware oraz Microsoft Hyper-V, umożliwiające:

		• tworzenie scenariuszy zasilania ukierunkowanych na pojedyncze maszyny wirtualne, grupy maszyn wirtualnych lub automatyczne grupy maszyn wirtualnych • tworzenie scenariuszy zasilania ukierunkowanych na klastry w środowiskach hiperkonwergentnych • tworzenie scenariuszy zasilania z sekwencyjnym wyłączaniem poszczególnych maszyn wirtualnych
1.3.8.31.	**Poziom hałasu (1 metr od urządzenia)**	<50 dB
1.3.8.32.	**Parametry środowiskowe i bezpieczeństwo**	IEC/EN 62040-1, IEC/EN 62040-2, IEC/EN 62040-3, IEC 60950-1
1.3.8.33.	**Zezwolenia**	CE
1.3.8.34.	**Gwarancja i wsparcie producenta**	• Montaż w szafie Rack, podłączenie do instalacji elektrycznej i uruchomienie realizowane przez serwis producenta. • 3 lat gwarancji realizowanej przez serwis producenta w miejscu pracy urządzenia (on-site). • Jeden bezpłatny przegląd serwisowy realizowany przez serwis producenta w okresie gwarancji.

II.1.3.9. Listwa zasilająca PDU – 2 szt.

Lp.	Parametr	Charakterystyka (wymagania minimalne)
1.3.9.1.	**Rodzaj wtyczki**	IEC 60309 32A 1Ph (jednofazowa)
1.3.9.2.	**Zakres napięcia wejściowego**	200-240 V
1.3.9.3.	**Częstotliwość znamionowa**	50/60 Hz
1.3.9.4.	**Moc**	7,4 kW
1.3.9.5.	**Wartość znamionowa prądu**	32 A
1.3.9.6.	**Długość przewodu zasilającego**	3 metry, przewód w wykonaniu bezhalogenowym
1.3.9.7.	**Gniazda wyjściowe**	12 x C13 + 12 x uniwersalne gniazdo kompatybilne zarówno z wtykiem C14, jak i C20
1.3.9.8.	**Automatyczny wyłącznik nadprądowy**	Tak, 2 jednobiegunowe z monitorowaniem stanu
1.3.9.9.	**Możliwość montażu w szafie rack**	Tak, 0U (montaż pionowy)
1.3.9.10.	**Fabryczny system montażowy**	Tak, możliwość instalacji z boku lub z tyłu listwy

1.3.9.11.	**System utrudniający przypadkowe wyciągniecie wtyczek z gniazd**	Tak, rozwiązanie fabryczne producenta, kompatybilne z przewodami P-lock
1.3.9.12.	**Dopuszczalna temperatura pracy**	0-60°C
1.3.9.13.	**Moduł kontroli z wyświetlaczem LCD, z interfejsem sieciowym**	Tak, wymienialny na gorąco, ze wskazaniami pomiarów i powiadomieniami o alarmach
1.3.9.14.	**Moduł kontroli zarządzany przy pomocy przycisków, portu USB lub interfejsu sieciowego**	Tak
1.3.9.15.	**Pomiar parametrów elektrycznych na wejściu listwy**	Tak
1.3.9.16.	**Wielkości pomiarowe**	Napięcie, moc, prąd, energia, moc czynna, moc pozorna, moc szczytowa
1.3.9.17.	**Możliwość zdalnego przełączania (wł./wył.) indywidualnych gniazd oraz sekwencyjnego załączania gniazd**	Tak, przełączanie realizowane w oparciu o przekaźniki bistabilne
1.3.9.18.	**Dokładność pomiaru mocy**	+/- 1% IEC klasa 1 dla V, W, A i kWh
1.3.9.19.	**Monitoring temperatury i wilgotności**	Tak, z dodatkowymi czujnikami podłączanymi do dedykowanego złącza RJ45 (do 3 czujników połączonych łańcuchowo)
1.3.9.20.	**Porty komunikacji sieciowej**	2 x Gigabit Ethernet
1.3.9.21.	**Możliwość połączenia łańcuchowego listew**	Tak, do 32 szt., obsługa RSTP Loop
1.3.9.22.	**Możliwość współdzielenia zasilania**	Tak, listwa podłączona do sieci elektrycznej może zasilać moduł sterujący drugiej, niepodłączonej do sieci elektrycznej.
1.3.9.23.	**Obsługiwane protokoły komunikacji**	HTTPS, SSH, SNMPv3, MQTT, LDAPS, LDAP over TLS, Radius, TLS 1.2, SSL, RestAPI, Modbus TCP
1.3.9.24.	**Cyberbezpieczeństwo**	Zgodność ze standardami UL 2900-1 i IEC 62443-4-2.
1.3.9.25.	**Zgodność ze standardami**	CB, CE, EN 62368-1:2014, EN IEC 61000-6-2:2019, EN IEC 61000-6-4:2019, EN 61000-3-2:2014, EN 61000-3-12:2011, EN 61000-3-3:2013, EN IEC 61000-3-11:2019, EN IEC 63000:2018
1.3.9.26.	**Dodatkowe certyfikaty**	ISO 9001 producenta urządzenia
1.3.9.27.	**Gwarancja**	Gwarancji producenta min. 3 lata

II.1.3.10. Usługa wdrożenia (pozycje II.1.3.7 - II.1.3.9)

Lp.	Zakres wdrożenia
1.3.10.1.	Dostarczenie szafy Rack do pomieszczenia wskazanego przez Zamawiającego.
1.3.10.2.	Ustawienie szafy i wypoziomowanie.
1.3.10.3.	Zamontowanie w szafie rack zasilacza UPS wraz z modułami bateryjnymi, podłączenie do instalacji elektrycznej i uruchomienie wykonane przez serwis producenta.
1.3.10.4.	Konfiguracja karty sieciowej web/SNMP – m.in. nadanie adresu IP, powiadomienia e-mail o stanie zasilacza, polityka zasilania odbiorów przy zaniku napięcia oraz polityka autorestartu.
1.3.10.5.	Aktualizacja firmware karty sieciowej web/SNMP oraz zasilacza UPS do najnowszej dostępnej wersji.
1.3.10.6.	Zamontowanie listew PDU w dedykowanych kanałach z tyłu dostarczonej szafy Rack.
1.3.10.7.	Podłączanie listew PDU do zasilacza awaryjnego UPS - sposób podłączenia musi być ustalony i zaakceptowany przez Zamawiającego.
1.3.10.8.	Konfiguracja interfejsu sieciowego web/SNMP listew PDU.
1.3.10.9.	Aktualizacja firmware listew PDU do najnowszej dostępnej wersji.

Charakterystyka systemu gromadzenia danych medycznych PACS

Lp.	Charakterystyka (wymagania minimalne)
1.4.1.	Oprogramowanie zarejestrowane w Polsce jako wyrób medyczny w klasie co najmniej IIa lub posiadające certyfikat CE właściwy dla urządzeń/oprogramowania medycznego w klasie co najmniej IIa stwierdzający zgodność z dyrektywą 93/42/EEC
1.4.2.	Oprogramowanie medyczne spełniające profile integracji IHE, min. • Scheduled Workflow, • Patient Information Reconciliation, • Key Image Notes, • Consistent Time, • Portable Data for Imaging, • Consistent Presentation of Images, • Patient Identifier Cross-referencing
1.4.3.	Oprogramowanie dostarczane z bezterminową licencją na użytkowanie i umożliwiające pracę nielimitowanej liczbie użytkowników na 120 000 badań
1.4.4.	System umożliwia pełną obsługę administracyjną, możliwość dopisywania dodatkowych urządzeń generujących obrazy do systemu PACS oraz Worklist przez przeszkolonego użytkownika bez dodatkowych kosztów Zamawiającego
1.4.5.	Licencje systemu bazodanowego dostarczane przez dostawcę.
1.4.6.	Wykonawca dostarczy niezbędne licencje systemu operacyjnego pozwalające na uruchomienie systemu PACS w środowisku Klienta.
1.4.7.	System wyposażony w zabezpieczenia przed nieautoryzowanym dostępem na poziomie klienta (aplikacja) i serwera (serwer baz danych).
1.4.8.	System pracuje w systemie operacyjnym Windows 10, Windows 11
1.4.9.	System umożliwia jednoczesną pracę dla użytkowników:

	• w roli radiologa • w roli technika elektroradiologa • w roli sekretarki medycznej • w roli lekarza klinicysty • w roli administratora
1.4.10.	Oprogramowanie oparte na koncepcji licencji przyznanych użytkownikowi systemu a nie stacji roboczej, a zarządzanie nimi realizowane jest przez system PACS (licencja pływająca)
1.4.11.	Pełna zgodność ze standardem DICOM 3.0 w zakresie komunikacji z urządzeniami medycznymi
1.4.12.	System umożliwia automatyczną komunikację z innymi systemami w standardzie DICOM.
1.4.13.	System umożliwia integrację z innymi systemami poprzez protokół HL7 w wersji 2.3.x
1.4.14.	System obsługuje standard UTF-8
1.4.15.	Obsługa protokołów DICOM C-Move, C-Find, C-Store SCU i SCP, DICOM
1.4.16.	Możliwość współpracy z usługą Active Directory (usługą katalogową systemu Windows polegającą na jednomiejscowej lokalizacji uprawnień użytkowników, obiektów w sieci i ich udostępniania).
1.4.17.	System posiada możliwość generowania DICOM Modality Worklist z obsługą polskich znaków diaktrycznych oraz z możliwością wyłączenia jej obsługi na konkretny aparat.
1.4.18.	System posiada możliwość generowania DICOM Modality Worklist na podstawie zlecenia badania odebranego z systemu HIS oraz wprowadzonego w module radiologicznym.
1.4.19.	Oprogramowanie korzysta z bazy danych badań systemu PACS (architektura klient – serwer)
1.4.20.	Oprogramowanie nie przechowuje lokalnie danych obrazowych ani bazy danych wykonanych badań/pacjentów
1.4.21.	Oprgramowanie posiada możliwość przenoszenia wybranego zbioru badań (także pojedynczego badania) pomiędzy zdefiniowanymi archiwami (cache).
1.4.22.	Możliwość wykorzystania istniejącego kontrolera domeny obsługującego protokół LDAP w zakresie minimum autoryzacji użytkowników
1.4.23.	Automatyczna kompresja odbieranych badań do formatu DICOM JPEG Lossless (obrazy diagnostyczne skompresowane bezstratnie)
1.4.24.	Oprogramowanie umożliwiające uruchomienie aplikacji wraz z jej ustawieniami na innym komputerze bez interwencji serwisowej
1.4.25.	Oprogramowanie przechowuje na serwerze PACS ustawienia interfejsu użytkownika – uruchomienie przez użytkownika oprogramowania na dowolnej stacji powoduje przywrócenie jego specyficznego interfejsu użytkownika
1.4.26.	Dostęp do systemu tylko po uprzednim zalogowaniu się.
1.4.27.	System blokujący dostęp użytkownika do oprogramowania po skonfigurowanej liczbie nieudanych prób zalogowania się.
1.4.28.	System posiada funkcjonalność ustawienia czasu automatycznego wylogowania stacji roboczej z oprogramowania w przypadku braku aktywności oraz czasu ważności hasła konta użytkownika
1.4.29.	System posiada funkcjonalność określenia katalogu ról użytkowników oprogramowania.
1.4.30.	System posiada funkcjonalność przydzielenia użytkownika do określonej roli użytkownika w systemie
1.4.31.	System posiada funkcjonalność przydzielenia odpowiednich uprawnień do określonej roli użytkownika systemu
1.4.32.	System posiada możliwość tworzenia widoków listy badań w zależności od przypisanej roli i uprawnień
1.4.33.	System posiada możliwość automatycznego i ręcznego przypisania priorytetów badania (min. 4-ro stopniowa skala) w zależności od obecnego statusu badania

1.4.34.	System posiada możliwość automatycznej eskalacji badania w zależności od długości trwania jego statusu, poprzez podniesienie jego priorytetu. (np. po trzech godzinach oczekiwania na opis badania z oddziału SOR, priorytet badania zostaje automatycznie zmieniony na wyższy).
1.4.35.	System posiada możliwość automatycznej eskalacji badania w zależności od długości trwania jego statusu, poprzez dodanie go do dynamicznej listy badań innego użytkownika lub grupy użytkowników (np. jeśli badanie nie zostało opisane w ciągu 30 dni, zostaje automatycznie przypisane do kolejnego radiologa lub grupy radiologów).
1.4.36.	System zapewnia wyświetlanie listy poprzednio wykonanych badań pacjenta, które zostały wysłane do systemu PACS
1.4.37.	System umożliwia automatyczne wyświetlanie listy poprzednio wykonanych badań pacjenta znajdujących się w zewnętrznym archiwum zintegrowanym z systemem PACS poprzez zdefiniowanie dedykowanych kryteriów wyświetlania, w tym po kryteriach łącznych: • Id Pacjenta, Nazwisko, Imię, Data urodzenia Konfiguracja jest możliwa na poziomie danego użytkownika
1.4.38.	System musi umożliwiać oznaczanie badań i przypisywanie ich do Tagów musi umożliwiać późniejsze ich wyszukiwanie (np. badania kliniczne, badania do prac naukowych.).
1.4.39.	System musi posiadać możliwość określenia stopnia ważności opisu w wielostopniowej skali. Możliwość wyszukania oznaczonych opisów w archiwum PACS.
1.4.40.	System posiada funkcje projektowania szablonów treści opisu oraz wykorzystania ich do automatycznego uzupełniania treści opisu.
1.4.41.	System posiada funkcje automatycznego dodawania do treści opisu (w miejscu kursora) wyniku pomiaru wykonanego na obrazie.
1.4.42.	System posiada funkcje projektowania szablonów treści opisu oraz wykorzystania ich do automatycznego uzupełniania treści opisu.
1.4.43.	System posiada funkcję projektowania szablonu opisu strukturalnego z wykorzystaniem: • narzędzi formatowania tekstu wbudowanym edytorem tekstu • tabel • podziału na sekcje z uwzględnieniem oznaczenia sekcji jako koniecznej do wypełnienia • predefiniowanych wzorców • pól, które należy uzupełnić - zmiennych (np. dzisiejsza data, bieżąca godzina, wartość z bazy danych systemu np. lekarz/e opisujący)
1.4.44.	System posiada funkcję przypisania szablonu do użytkownika, rodzaju urządzenia diagnostycznego, rodzaju badania (procedury).
1.4.45.	System posiada możliwość zmiany (Ad Hoc) domyślnego szablonu badania na inny.
1.4.46.	Oprogramowanie umożliwia bezpośrednie diagnozowanie i monitorowanie procesów życiowych, np. badania tomograficzne z kontrastem.
1.4.47.	System posiada możliwość opisywania badań radiologicznych poprzez wbudowany moduł opisowy.
1.4.48.	Wszystkie opisy badań przechowywane są bezpośrednio w module radiologicznym
1.4.49.	System posiada otworzenia aktywnej listy badań (wiele badań jednocześnie) oraz posiada możliwość rozpoczęcia opisu wybranego badania. System posiada możliwość szybkiego przełączania się między tymi badaniami z zachowaniem wszystkich wprowadzonych zmian w opisie oraz w warstwie prezentacji orazów: wprowadzone pomiary, adnotacje
1.4.50.	System posiada możliwość anulowania rozpoczętego opisu badania oraz powrót do stanu sprzed opisu.
1.4.51.	Funkcja automatycznego odświeżania listy badań oczekujących na opis dostępnej i widocznej dla lekarza radiologa w czasie rzeczywistym.

1.4.52.	System posiada możliwość automatycznego otwarcia kolejnego badania z dynamicznej listy po zakończeniu opisu poprzedniego badania.
1.4.53.	System posiada możliwość wyeksportowania opisu badania w formie wydruku
1.4.54.	System posiada możliwość wydruku badań na kamerach cyfrowych poprzez DICOM Print
1.4.55.	Funkcja nagrywania na lokalnej nagrywarce stacji roboczej płyt CD/DVD wraz z przeglądarką DICOM uruchamiająca się automatycznie na komputerze klasy PC Możliwość nagrania pojedynczego na badania lub wielu badań na płycie CD/DVD. Możliwość załączenia opisu badania (pdf) oraz wyboru zakresu danych, w tym: całego badania, obrazów kluczowych oraz wybranych obrazów wskazanych przez użytkownika w czasie zlecania nagrywania.
1.4.56.	Funkcja importowania plików graficznych NON-DICOM do zlecenia lub istniejącego badania z rozrzerzeniem min.: jpg, png, pdf, bmp, tiff, gif. Importowany plik zostanie zapisany jako nowa seria badania
1.4.57.	Możliwość importu badania z płyty CD/DVD z plikiem DICOMDIR
1.4.58.	Możliwość import badania z nośnika USB/CD/DVD bez pliku DICOMDIR
1.4.59.	Możliwość importu badania z lokalnego dysku oraz zewnętrznego zdefiniowanego PACS poprzez wskazanie ścieżki do folderu z badaniem.
1.4.60.	System posiada możliwość przeniesienia niewłaściwie przypisanych obrazów w badaniu do innego badania przez uprawnionego użytkownika
1.4.61.	System posiada możliwość rozdzielenia badania na wiele badań zgodnie ze zleceniami (wiele procedur) przez uprawnionego użytkownika
1.4.62.	System posiada możliwość scalenia dwóch lub więcej badań w jedno badanie. Dane pacjenta oraz badania zostają wybrane na podstawie wyboru głównego badania przez użytkownika, do którego zostaną przeniesione obrazy z innego badania. Scalania można dokonać uprawniony użytkownik.
1.4.63.	System posiada możliwość dołączenia do badania dokumentów elektronicznych (np. dokument pdf, pliku graficzny, dokument w podłączonym skanerze). Powiązane z badaniem dokumenty są widoczne w obszarze tekstowym. Możliwość wyświetlenia i wydruku dokumentów.
1.4.64.	System pozwala wyszukać badania na podstawie dowolnej kombinacji warunków i parametrów, min takich jak.: • Imię i Nazwisko pacjenta • Data urodzenia • PESEL • Id Pacjenta • Płeć • Wiek • Numer procedury • Nazwa procedury • Modalność, w tym: możliwość wskazania wielu modalości jednocześnie • Data badania, w tym: (data badania od - do; zdefiniowane okresy czasu - tj. dzisiaj, wczoraj, ostatnia godzina, ostatni tydzień, ostatni miesiąc) • Nazwa pracowni • Jednostka zlecająca • Oddział zlecający • Lekarz zlecający • Technik wykonujący badanie • Lekarz wykonujący • Lekarz opisujący • Lekarz zatwierdzający opis

	• Status badania • Zdefiniowane słowa kluczowe • Badanie zaimportowane do archiwum systemu z zewnątrz (np. wgrane CD/DVD) • Fraza komentarza do badania umieszczonego w systemie przez dowolnego użytkownika • Fraza z rozpoznania do badania
1.4.65.	Możliwość definiowania słownika (więcej niż jednego) słów kluczowych poprzez administratora systemu.
1.4.66.	• Możliwość oznaczania badań zdefiniowanymi słowami kluczowymi wraz z archiwizacją tych oznaczeń w systemie PACS. • Możliwość wyszukania badań po zdefiniowanym słowie kluczowym.
1.4.67.	System posiada funkcję wyszukiwania zaawansowanego. Umożliwia wyszukiwanie badań poprzez definiowanie zapytań z operatorami logicznymi "i" i "lub" (umożliwiający wyświetlenie badań spełniające warunki: • zaczyna się od; • jest; • nie jest; • kończy się na; • zawiera; • nie zawiera
1.4.68.	Wyszukiwanie zaawansowane oraz budowanie zapytań jest realizowane poprzez interfejs użytkownika modułu radiologicznego na podstawie zdefiniowanych pól wyboru, a nie poprzez formułowanie bezpośrednich zapytań SQL do bazy danych
1.4.69.	System posiada możliwość dodawania oraz usuwania wyświetlanych kolumn na poziomie danego pulpitu użytkownika oraz na poziomie interfejsu indywidualnego użytkownika.
1.4.70.	System posiada możliwość dostosowywania rozmiaru wyświetlanych kolumn wraz z możliwością zdefiniowania kolejności wyświetlania pól (rosnąco/malejąco) na poziomie interfejsu użytkownika.
1.4.71.	System posiada możliwość wyświetlenia wielu badań z listy jednocześnie spełniających zadane kryteria wraz z możliwością przełączania się między nimi bez ich zamykania.
1.4.72.	System pozwala użytkownikowi na tworzenie własnej bazy ciekawych przypadków, którymi on zarządza i są one niedostępnych dla innych użytkowników (znaczniki prywatne)
1.4.73.	System posiada wbudowany komunikator umożliwiający wymianę wiadomości on-line pomiędzy użytkownikami systemu. Możliwość ustawienia statusu (aktywny; nie przeszkadzać, z dala od komputera) wraz z możliwością zrobienia wpisu w odniesieniu do wybranego statusu
1.4.74.	System posiada możliwość obsługi jednego/dwóch/czterech monitorów diagnostycznych. System posiada możliwość obsługi monitora tekstowego RIS.
1.4.75.	System posiada możliwość otworzenia wyświetlonego badania w wybranym przez użytkownika zintegrowanym systemie postprocessingowym. Otwarcie badania wywołane za pomocą jednego kliknięcia z poziomu modułu radiologicznego.
1.4.76.	System posiada możliwość włączenia i wyłączenia wyświetlania nawigatora
1.4.77.	System posiada możliwość relokacji nawigatora na poziomie użytkownika oraz umiejscowienie go: po lewej; po prawej stronie; na górze; na dole - w zależności od preferencji użytkownika.
1.4.78.	Prezentacja serii w nawigatorze pozwala na określenie: • ile obrazów zawiera seria, • które serie pochodzą z którego badania, • które serie są obecnie są wyświetlane, • które serie pochodzą z obecnie opisywanego badania,

	• czy wszystkie obrazy danej serii zostały wyświetlone podczas bieżącego wyświetlania badania
1.4.79.	System posiada opcję wyboru na poziomie użytkownika wyświetlania w nawigatorze miniatur serii lub listy serii (po nazwie)
1.4.80.	System posiada możliwość wybrania z nawigatora dowolnej serii badania i wyświetlenia jej obrazów na monitorze/monitorach w wybranym układzie ekranu
1.4.81.	Funkcja aktywnej lokalizacji – wybrany przez użytkownika punkt na obrazie należący do jednej płaszczyzny rzutu (np. sagittal) automatycznie pojawia się na odpowiadającym obrazie w innej płaszczyźnie (np. coronal i transverse)
1.4.82.	Funkcja jednoczesnego przewijania obrazów wielu wyświetlanych serii badania/badań pacjenta. Możliwość uruchomienia automatycznej nawigacji serii za pomocą narzędzia oraz skrótu klawiszowego.
1.4.83.	Funkcja wyświetlania oraz ukrycia linii referencyjnych na innych płaszczyznach (surowych lub MIP/MPR) podczas przewijania obrazów z wybranej serii badania
1.4.84.	System posiada funkcję oznaczenia obrazu jako kluczowego wraz z określeniem powodu, co najmniej: • jako załącznik do opisu, • do wydrukowania, • dla lekarza kierującego
1.4.85.	System gromadzi oznaczone obrazy kluczowe dla pacjenta ze wszystkich widocznych w historii badań. Możliwość wyświetlenia wszystkich obrazów kluczowych z otwartych badań zbiorczo bez konieczności przeglądania wszystkich serii.
1.4.86.	System umożliwia oznaczenie badania jako wyjściowego na liście badań pacjenta. Oznaczenie jest widoczne w historii badań pacjenta.
1.4.87.	Protokoły wyświetlania badań
1.4.88.	System posiada możliwość konfiguracji sekwencji protokołów wyświetlania badania z uwzględnieniem: procedury badania, rodzaju urządzenia diagnostycznego i regionu anatomicznego (części ciała), stacji o określonej liczbie monitorów
1.4.89.	Funkcja projektowania i zapisania sposobów prezentacji obrazów (rozkład na ekranie/ach) związanych z protokołem wyświetlania
1.4.90.	Wyświetlenie obrazów badania następuje automatycznie zgodnie z istniejącym protokołem wyświetlania, którego warunki spełnia badanie i zgodnie ze sposobem prezentacji obrazów
1.4.91.	System posiada możliwość przełączania się pomiędzy sposobami prezentacji obrazów w ramach wybranego protokołu wyświetlania badania za pomocą myszy oraz za pomocą skrótów klawiaturowych.
1.4.92.	System posiada możliwość zapisania bieżącego sposobu wyświetlania jako nowy protokół wyświetlania badania lub jako modyfikację wybranego istniejącego protokołu wyświetlania badania
1.4.93.	System umożliwia zdefiniowanie i zapisanie określonych kryteriów przy tworzeniu nowego protokołu wyświetlania z uwzględnieniem min.: • numeru serii oraz frazy, którą nazwa seria zawiera • automatycznego połączenia wyświetlanych obrazów po wybraniu protokołu • poziomu okna (W/L) dla poszczególnych serii w określonym widoku
1.4.94.	System posiada możliwość indywidualnego projektowania i zapisywania protokołów wyświetlania przez użytkownika dla CT i MR w zależności od potrzeb użytkownika - minimum 15 indywidualnych
1.4.95.	System posiada możliwość przełączania się pomiędzy zdefiniowanymi lub utworzonymi przez użytkownika protokołami wyświetlania badania.

1.4.96.	System umożliwia zdefiniowanie warunków otwierania badań na poziomie zalogowanego użytkownika do wyboru: • wyświetlanie badania bieżącego (oraz manualne dodawanie badań do porównania) • wyświetlanie badania bieżącego oraz automatyczne dodanie poprzednich badań (wg reguł administratora) do nawigatora serii • wyświetlanie automatycznie badań porównawczo (jeśli jest dostępne poprzednie badanie pacjenta w historii)
1.4.97.	System umożliwia szybkie porównanie badań historycznych pacjenta (dla tej samej modalności) wyświetlanych w nawigatorze serii. Możliwość poruszania sie pomiędzy badaniami bez konieczności przeglądania i przeciągania konkretnej serii w wyświetlanym widoku.
1.4.98.	Operacje na obrazach badań
1.4.99.	Progresywne wyświetlanie obrazów - szybkie wyświetlanego obrazu i stopniowe przesyłania kolejnych danych (np. pozostałych obrazów serii)
1.4.100.	Funkcja włączenia i wyłączenia automatycznej nawigacji pomiędzy wyświetlanymi seriami na poziomie systemu oraz zalogowanego użytkownika. Możliwość ustawienia skrótu klawiszowego dla uruchomienia synchronizacji serii.
1.4.101.	Funkcja wyświetlenia/ukrycia danych demograficznych pacjenta na obrazach
1.4.102.	Funkcja eksportu wybranego obrazu lub oznaczonych obrazów badania bez danych osobowych na lokalne urządzenie w formatach takich jak: png, jpg
1.4.103.	Funkcja kolimacji obrazu badania: prostokątna i eliptyczna
1.4.104.	Funkcja wyświetlania dla wskazanego piksela wartości gęstości optycznej dla badań CR oraz jednostek Hounsfielda dla badań TK
1.4.105.	Funkcja przedstawienia przebiegu wartości piksela wzdłuż wyznaczonej prostej
1.4.106.	Funkcja wygenerowania histogramu dla wybranego obszaru oznaczonego na obrazie
1.4.107.	Funkcja oznaczenia regionu zainteresowania (ROI) za pomocą okręgu, elipsy, wielokąta
1.4.108.	Funkcja płynnej regulacji kontrastu na obrazie oraz możliwość wybrania z predefiniowanych ustawień dla: mózgu, kości, śródpiersia, płuc, wątroby, brzucha, miednicy. Funkcja zdefiniowania na poziomie użytkownika skrótów klawiszowych dla uruchomienia wybranych ustawień okna na obrazie.
1.4.109.	Funkcja definiowania własnych predefiniowanych ustawień poziomu okna (W/L) z uwzględnieniem filtra wyostrzającego dla wybranych parametrów okna.
1.4.110.	Funkcja powiększania obrazu, min.: • płynne powiększanie oraz pomniejszanie za pomocą myszy; • powiększenie 1:1;
1.4.111.	Funkcja powiększania wybranego fragmentu obrazu, tzw. Lupa - powiększenie x2, x4, x6
1.4.112.	Funkcja pomiaru kąta, w tym także: pomiary kąta Cobba oraz kąta HKA
1.4.113.	Funkcja wyznaczenia linii centralnej
1.4.114.	Funkcja pomiaru różnicy długości pomiędzy dwoma wyznaczonymi prostymi
1.4.115.	Funkcja pomiaru prostopadłego - odległość punktu od wyznaczonej linii
1.4.116.	Funkcja pomiaru równoległego poziomego
1.4.117.	Funkcja dodania dowolnego tekstu do obrazu badania o długości min. 16 znaków
1.4.118.	Funkcja dodania strzałki do obrazu badania
1.4.119.	Funkcja kalibracji liniowej i kołowej obrazu w celu prawidłowego wyświetlania wartości odległości pomiędzy dwoma punktami, kalibracja przeprowadzona przez użytkownika względem obiektu odniesienia na obrazie
1.4.120.	Funkcja pomiaru odległości pomiędzy dwoma punktami na obrazie

1.4.121.	Funkcja pomiaru stosunku długości dwóch linii zdefiniowanych przez użytkownika (np. wskaźnik sercowo-płucny)
1.4.122.	Funkcja pomiaru pojemności komory serca
1.4.123.	Funkcja pomiaru przegrody międzykomorowej (IVS), jamy lewej komory (LVID), ściany tylnej lewej komory (LVPW) TAK
1.4.124.	Funkcja pomiaru czasu spadku ciśnienia do połowy (PHT)
1.4.125.	Funkcja pomiaru całki prędkości przepływu w czasie (VTI)
1.4.126.	Funkcja pomiaru odległości w badaniach jednowymiarowych (M-mode)
1.4.127.	Funkcja pomiaru czasu w badaniach jednowymiarowych (M-mode) i dopplerowskich
1.4.128.	Funkcja pomiaru prędkości w badaniach dopplerowskich
1.4.129.	Funkcja usunięcia adnotacji wprowadzonych przez użytkownika
1.4.130.	Funkcja zapisania adnotacji na obrazie przez użytkownika. Zapisane adnotacje są dostępne dla innych użytkowników systemu.
1.4.131.	Funkcja przemieszczania i edycji wszystkich adnotacji wprowadzonych przez użytkownika
1.4.132.	Funkcja wyświetlenia/ukrycia adnotacji wprowadzonych przez użytkownika
1.4.133.	Funkcja obrotu obrazu o 180˚ oraz o 90˚ stopni w lewo/w prawo
1.4.134.	Funkcja odbicia obrazu w poziomie oraz w pionie
1.4.135.	Funkcja płynnego obrotu obrazu o dowolnie wybrany przez użytkownika kąt
1.4.136.	Funkcja inwersji pozytyw/negatyw na obrazie badania
1.4.137.	Funkcja cofnięcia ostatnio wykonanej zmiany obrazu
1.4.138.	Funkcja powrotu do poprzedniej, ostatnio zachowanej postaci obrazu
1.4.139.	Funkcja rekonstrukcji wielopłaszczyznowych MPR. Wybranie serii i upuszczenie jej w wyświetlanym oknie rekonstrukcji MPR powoduje automatyczną rekonstrukcję dla nowo wybranej serii
1.4.140.	Funkcja renderowania ze zmodyfikowaną grubością warstwy MIP
1.4.141.	Funkcja renderowania CPR na podstawie krzywej w widokach: straightened CPR, stretched CPR
1.4.142.	Funkcja renderowania wolumetrycznego 3D i 3D MIP oraz możliwość wyeksportowania animacji jako pliku mp4
1.4.143.	Funkcja regulacji grubości warstwy w projekcjach MPR z możliwością wyboru spośród zdefiniowanych wartości oraz poprzez manualne dostosowanie
1.4.144.	Funkcja oznaczania kręgów i krążków międzykręgowych kręgosłupa. Oznaczenia kolejnych kręgów/krążków na obrazie badania wyświetlane są w rzutach MPR
1.4.145.	Funkcja fuzji dwóch zarejestrowanych serii badań. Możliwość regulacji blendy pomiędzy wyświetlanymi seriami
1.4.146.	Funkcja edycji dokonanej automatycznie fuzji obrazów z możliwością uwzględnienia i wskazania dopasowania fuzji na poziomie wyznaczonego regionu zainteresowania. Możliwość manualnego dostosowania fuzji obrazów, np w przypadku artefaktów oddechowych, zmiany masy ciała, itp.
1.4.147.	Funkcja utworzenia i zapisania migawki (zrzutu) oglądanego w danej chwili obrazu do późniejszego odtworzenia widoku, na którym została utworzona migawka. W systemie jest widoczne kto i kiedy taki zrzut wykonał.
1.4.148.	Funkcja wyświetlenia topogramu dla badań TK i MR
1.4.149.	Funkcja przeglądania animacji wraz z możliwością ustawień: • prędkości animacji; • zakresu obrazów do animacji; • przeglądanie animacji w pętli; • zmiany kierunku animacji;
1.4.150.	Funkcja zdefiniowania skrótów klawiszowych na poziomie zalogowanego użytkownika dla operacji:

	• pomiar odległości • pomiar stosunku długości 2 wyznaczonych prostych (wskaźnik sercowo-płucny) • pomiar gęstości (ROI) za pomocą narzędzi: okręgu oraz elipsy 2 i 3 puntowej • pomiar kąta (w tym kąta Cobba) • włącz/ukryj linie MPR • utworzenia i zapisania migawki (zrzutu) oglądanego w danej chwili obrazu do późniejszego odtworzenia widoku, na którym została utworzona migawka.
1.4.151.	Kominki i konferencje radiologiczne
1.4.152.	Moduł kominków radiologicznych / konferencji wbudowany w moduł radiologiczny
1.4.153.	Moduł posiada mechanizm planowania, uruchamiania konferencji oraz współdzielenia obszaru obrazowego wyświetlanego badania w czasie rzeczywistym.
1.4.154.	Moduł posiada możliwość określenia dla konferencji/kominka następujących parametrów: • Nazwa kominka • Datę i czas rozpoczęcia • Czas trwania • Częstotliwość powtarzania się (dziennie, co tydzień, miesięcznie) • Datę i czas zakończenia cyklicznych konferencji/kominków • Maksymalną liczbę przypadków do omówienia, jakie mogą dodać uczestnicy konferencji/kominków na daną sesję • Prowadzącego konferencję/kominek - Administratora konferencji/kominka • Uczestników konferencji (użytkownik, grupa użytkowników)
1.4.155.	Funkcja dodawania badania do konferencji/kominka dla uprawnionych użytkowników. W trakcie dodawania badania do konferencji, użytkownik może dodać informację o przyczynie dodania badania do omówienia
1.4.156.	Funkcja generowania dedykowanego linku (ad hoc) do danej konferencji/kominka dla określonych użytkowników
1.4.157.	System umożliwia w ramach prowadzonej konferencji/kominka, udostępnianie obszaru obrazowego prezentera uczestnikom konferencji/kominka: • manipulacja obrazami wyświetlanego badania (zgodnie z wymaganymi narzędziami) • wskaźnik pokazujący lokalizację kursora myszy prezentera Uczestnicy konferencji/kominka mają możliwość dołączenia do rozpoczynającej się sesji kominkowej z poziomu modułu kominków oraz poprzez wygenerowany link otrzymany w aplikacji webowej
1.4.158.	Funkcjonalności do analizy AI
1.4.159.	System posiada wbudowane narzędzia umożliwiające integrację protokołów AI, w tym przetwarzanie oraz analizę skanów wykonanych na urządzeniach różnych dostawców.
1.4.160.	Wynik analizy algorytmu sztucznej inteligencji jest dostępny dla lekarza radiologa bezpośrednio w module radiologicznym.
1.4.161.	System umożliwia zdefiniowanie dedykowanego przepływu pracy (workflow) dla badań analizowanych przez mechanizm AI, np.. Na podstawie metadanych generowanych przez aplikacje AI możliwość płynnego przydzielenia badania do dedykowanej grupy/użytkownika.
1.4.162.	System umożliwia wykorzystanie wyników badań pochodzących z analizy AI i uwzględnienie ich automatycznie w dedykowanym szablonie opisowym dostępnym w module opisowym.
1.4.163.	System umożliwia wykorzystanie dedykowanych protokołów wyświetlania dla badań i wizualizacji danych pochodzących z analizy AI.
1.4.164.	System posiada funkcję sortowania i priorytetyzacji badań (tzw. triage) oraz wyświetlania ich w module radiologcznym (na liście roboczej badań do opisu) na podstawie metadanych

	uzyskanych podczas analizy AI, np. badania wymagające pilnej diagnozy mają wyższy priorytet.
1.4.165.	System na podstawie metadanych uzyskanych podczas analizy AI umożliwia wizualne oznaczanie badań wymagających pilnej diagnozy (pilnego opisu), np. wyróżnienie kolorem (na liście roboczej badań do opisu).
1.4.166.	System umożliwia automatyczną analizę i porównanie badań bieżących i historycznych pacjenta (analizowanych przez zintegrowane algorytmy AI), poprzez dedykowane protokoły wyświetlania.
Funkcjonalności dla oceny zmian chorobowych	
1.4.167.	System posiada wbudowane narzędzia umożliwiające śledzenie zmian onkologicznych w czasie zgodne z wytycznymi RECIST 1.1
1.4.168.	System umożliwia wykonanie dedykowanego pomiaru zmian onkologicznych (target oraz non-target) wraz z automatycznym umieszczeniem wartości pomiarowych w tabeli
1.4.169.	System umożliwia wybranie ze zdefiniowanej listy organu, dla którego dokonywany jest pomiar zmiany wraz z możliwością opisania zmiany
1.4.170.	System umożliwia rejestrowanie pomiarów w dedykowanej tabeli wykonywanych dla badania wyjściowego oraz każdego kolejnego badania porównawczego
1.4.171.	System posiada funkcje zapisania obrazu, na którym dokonywany jest pomiar, a pomiary w tabeli są zsynchronizowane z obrazami badania
1.4.172.	System wyświetla automatycznie obraz po wybraniu pomiaru w tabeli śledzenia zmian (jeśli poprzednio obraz ten został zapisany). System automatycznie przekierowuje do dedykowanego obrazu umożliwiając ocenę porównawczą bieżącego badania pacjenta na tym samym poziomie anatomicznym
1.4.173.	System po zakończeniu oceny przeglądu zmian dla kolejnego badania oblicza sumę docelową oraz różnicę względem stanu wyjściowego i względem NADIR
1.4.174.	System posiada możliwość określenia i umieszczenia w tabeli przez użytkownika ewaluacji zmian i odpowiedzi na leczenie (zgodnie z RECIST - CR, PR, PD, SD).
1.4.175.	System umożliwia skopiowanie wartości z tabeli śledzenia zmian do opisywanego badania

Charakterystyka Vendor Neutral Archive (VNA)

Lp.	Charakterystyka (wymagania minimalne)
Ogólne	
1.5.1.	Wsparcie dla profili integracyjnych IHE: XDS-I.b (Imaging Document Consumer, Imaging Document Source, Document Repository), IOCM (Change Requester, Image Manager/Archive, Image Display), ATNA (Audit Record Repository, Secure Application), PIX (Patient Identifier Cross-reference Consumer), PDQ (Patient Demographics Consumer), Scheduled Workflow (Image Manager / Archive, PPS Manager, Image Display, Evidence Creator), Patient Information Reconciliation (Image Manager / Archive, PPS Manager),
1.5.2.	Automatyczne tworzenie i zapisywanie sum kontrolnych np. MD5 wszystkich zarchiwizowanych plików oraz ich automatyczną weryfikację w momencie wydobywania z archiwum długoterminowego.
1.5.3.	Możliwość tworzenia kopii zapasowych bazy danych.
1.5.4.	Kopia zapasowa bazy danych tworzona min. 1 raz na 24 godziny zapewniając pełną stabilność oraz wydajność systemu
1.5.5.	Tworzenie kopii zapasowej bazy danych bez przerywania pracy systemu.
1.5.6.	Konfigurowalne zasady routingu badań do innych systemów (na podstawie dowolnego Tag-u DICOM-owego) lub konfigurowalne zasady routingu do innych systemów przez kreator tworzący reguły na podstawie znaczących informacji z komunikacji HL7 oraz tagów

	DICOM pozwalający na skierowanie badań do innych węzłów w sposób stały dla wszystkich badań danego rodzaju lub z danego źródła (np. badania CT, badania z danego aparatu), jak i zmienny w zależności od wyboru dokonanego przy zleceniu (np. oddział zlecający).
1.5.7.	Funkcja automatycznej kompresji odbieranych badań do formatu DICOM JPEG Lossless (obrazy diagnostyczne skompresowane bezstratnie)
1.5.8.	Mechanizm DICOM IOCM (Image Object Change Management) wysyłający obiekty DICOM do archiwum badań obrazowych informujące o zmianach w badaniu.
1.5.9.	System musi przyjmować, archiwizować oraz udostępniać dane DICOM w nie zmienionej postaci (z wyłączeniem danych zmodyfikowanych w bazie danych systemu archiwizacji obrazów na podstawie danych wprowadzonych przez użytkownika, np. dane osobowe pacjenta, dane demograficzne, dane zlecenia, opis badania).
1.5.10.	Mechanizm Tag Morphing - morfowanie tagów DICOM – dla wybranego źródła DICOM administrator systemu ma możliwość konfiguracji automatycznego dodania/usunięcia/ modyfikacji wybranych tagów DICOM.
1.5.11.	Funkcjonalność przypisania konta użytkownika do ról i nadania odpowiednich uprawień.
1.5.12.	Funkcja wyszukiwania obrazów (po wykonanej procedurze, modalności, nr PESEL pacjenta oraz dacie wykonania badań (okresie od do) oraz eksportu wybranej grupy lub pojedynczego badania zanonimizowanych obrazów DICOM do zewnętrznego źródła. Funkcja ta musi być dostępna z profilu administratora lub lekarza radiologa.
1.5.13.	Możliwość zdefiniowania reguł ILM (Image Lifecycle Management) w celu określenia czasu przechowywania różnych obrazów. Musi być możliwe łącznie reguł, tak aby dało się tworzyć własne spersonalizowane kryteria. Na przykład wiek pacjenta (reguła - „Pacjent miał co najmniej X lat w momencie wykonania badania") można połączyć z rodzajem badania (reguła - „Badania pediatryczne nie mogą zostać usunięte") co poskutkuje usunięciem tylko badań, nie spełniających tych kryteriów.
1.5.14.	Minimalne wymagane parametry wykorzystywane do konfiguracji reguł: 1.5.14.1. Określone nazwy stacji akwizycji 1.5.14.2. Określone działy szpitala 1.5.14.3. Pacjent starszy niż określony wiek 1.5.14.4. Określone rodzaje modalności 1.5.14.5. Określone procedury 1.5.14.6. Wiek badania
1.5.15.	Możliwość konfigurowania reguł ILM dla poszczególnych grup przestrzeni (storage groups).
1.5.16.	Funkcja prefetching-u badań na podstawie zleceń z zewnętrznych systemów np. RIS, HIS.
1.5.17.	Funkcja prefetching-u poprzednich badań pacjenta z archiwum długoterminowego na podstawie otrzymania pierwszego obrazu nowego badania i/lub automatycznego wysłania tych badań do zewnętrznych systemów DICOM.
1.5.18.	Funkcja budowania zasad prefetching-u badań, umożliwiającą wyszczególnienie które z poprzednich badań są istotne dla bieżącego badania w celu automatycznego ich przywracania z archiwum długoterminowego oraz zewnętrznych systemów DICOM, na podstawie danych HL7 i/lub DICOM (np. obszar anatomiczny, rodzaj urządzenia diagnostycznego, wiek badania, priorytet badania)
1.5.19.	Funkcjonalność konfiguracji archiwizacji hierarchicznej, w której dane rzadziej używane przenoszone są na archiwa oparte na dyskach wolniejszych, a dane używane częściej przenoszone są na dyski szybsze.
1.5.20.	Mechanizm automatycznego pobierania do przestrzeni online cache obrazów poprzednich badań pacjenta z zewnętrznych systemów DICOM na podstawie zleceń z zewnętrznych systemów np. RIS, HIS oraz na podstawie odebranych badań DICOM z zewnętrznych systemów.
Dodawanie danych non-DICOM przez interfejs webowy	

1.5.21.	Funkcjonalność dodawania danych non-DICOM (jako DICOM Encapsulated) bezpośrednio do istniejącego lub nowego badania z poziomu interfejsu webowego. Minimalnie wymagane rozszerzenia: PDF, DOC, DOCX, XLSX, PPTX, TXT, XML, ZIP, PNG, BMP, JPG, TIFF, AVI, MP4, MPEG (kodeki MPEG-2, MPEG-4), MOV, WMV, M4A, MP3, AIFF, AU, WAV.
1.5.22.	Maksymalna obsługiwana wielkość obrazów w formacie JPG i PNG musi wynosić co najmniej 16384x16384 pixeli (256 megapixeli).
1.5.23.	Minimalna wymagana wielkość obsługiwanych plików non-DICOM importowanych jako DICOM Encapsulated musi wynosić co najmniej 2GB.
1.5.24.	W przypadku dodawania do nowego badania, system VNA podczas wgrywania danych non-DICOM musi automatycznie utworzyć nowe badanie przypisane do wybranego przez użytkownika pacjenta.
1.5.25.	Możliwość konfiguracji reguł wgrywania danych non-DICOM z poziomu webowego interfejsu przeglądarki klinicznej. Minimalnie wymagane są poniższe reguły: 1.5.25.1. dodawanie zdjęć z poziomu webowego interfejsu uruchomionego na urządzeniu mobilnym (smartphonie), jest możliwe tylko i wyłącznie bezpośrednio z kamery urządzenia 1.5.25.2. ograniczenie jakie formaty plików z listy obsługiwanych mogą być wgrywane (np. zablokowanie wgrywania plików ZIP) 1.5.25.3. departamenty i procedury domyślne
Automatyczny import	
1.5.26.	Funkcjonalność automatycznego importu danych DICOM oraz non-DICOM (w ich natywnym formacie lub w postaci DICOM Encapsulated) z wyznaczonych folderów na przestrzeni dyskowej (udziałów NFS).
1.5.27.	Maksymalna wielkość obsługiwanych plików non-DICOM importowanych jako DICOM Encapsulated musi wynosić co najmniej 2GB.
1.5.28.	Wymagane jest aby zaimportowane dane zostały automatycznie połączone z odpowiednim rekordem pacjenta. Połączenie tych danych musi się obywać z pomocą poniższej wymaganej metody: 1.5.28.1. Przesłanie informacji dotyczących rekordu pacjenta w nazwie importowanego pliku. 1.5.28.2. Nazwa importowanego pliku musi zawierać: • PN — imię i nazwisko pacjenta, • BD — data urodzenia pacjenta, • ID — identyfikator pacjenta, • IR — wystawca identyfikatora pacjenta, • SX — płeć pacjenta, • AC — numer dostępu, • CAT — kategorie Przykład: PN{LISA^FREDRICK^^Mrs}BD{19951103)ID{BX001}IR{GMAX5454}SX(F}.png
1.5.29.	Możliwość konfiguracji, czy automatycznie zaimportowane dane mają być przechowywane w postaci: 1.5.29.1. Natywnej 1.5.29.2. Jako DICOM Encapsulated 1.5.29.3. Natywnej oraz jako DICOM Encapsulated na raz
1.5.30.	Zaimportowane pliki obrazów (PNG, BMP, JPG, TIFF) oraz PDF muszą być możliwe do wyświetlenia z poziomu interfejsu webowego przeglądarki klinicznej dostarczonej z systemem archiwizacji obrazów.
1.5.31.	Pozostałe zaimportowane dane muszą być dostępne dla systemu oraz systemów trzecich przy pomocy API zgodnego ze standardem FHIR w wersji R4 (https://hl7.org/fhir/R4/)

Funkcjonalności dostępne dla administratora serwera PACS

Lp.	Charakterystyka (wymagania minimalne)
1.6.1.	Edytor metadanych DICOM. Umożliwia wyszukiwanie, podgląd oraz manualną edycję metadanych DICOM. Narzędzie umożliwia ww. operacje na pojedynczym pliku bądź na plikach we wskazanym folderze. Edytowane metadane mogą być zapisane do wielu obiektów DICOM w ramach jednej operacji edycji - na poziomie tagów pacjenta, padania bądź serii. Narzędzie posiada wbudowaną wyszukiwarkę metadanych. Kryteriami wyszukiwania mogą byc: tag DICOM lub zawartość tagu. Narzędzie umożliwia również anonimizację badań według jednego z trzech profili: standard DICOM, deidentyfikacja jedynie danych pacjenta, deidentyfikacja danych pacjenta oraz niektórych dat. Narzędzie umożliwia utworzenie pliku indeksu wszystkich obiektów: DICOMDIR. Narzędzie umożliwia eksport wszystkich metadanych do pliku tekstowego.
1.6.2.	EI Audit Log Viewer
1.6.3.	Narzędzie umożliwia dostęp do dziennika audytu systemu (Audit Record Repository). Dla podglądu zdarzeń dziennika dostępne są następujące kryteria wyszukiwania: data początkowa, data końcowa, identyfikator użytkownika, identyfikator badania (Study UID), numer akcesji badania (accession number), identyfikator kartoteki pacjenta. Wyszukane zdarzenia dziennika mogą być filtrowane wg następujących kryteriów: identyfikator zdarzenia, typ zdarzenia (np. logowanie), wykonana akcja, rezultat wykonanej akcji, tekstowy ciąg znaków do wyszukania w źródle XML zdarzania. Wyszukane zdarzenia mogą być wybrane i eksportowane do pliku XLS lub XML. Eksport bardzo dużej liczby zdarzeń z dziennika umożliwia definicja zaplanowanego zadania, które zostanie wykonane przez serwer PACS a rezultaty zostaną zwrócone w postaci pliku. Zadanie określone jest: kryteriami wyszukiwania (jak w podglądzie zdarzeń), harmonogramem wykonania, formatem pliku wynikowego (CSV, XLS, XML, ZIP), adresem email na który wysłane zostanie powiadomienie o ukończeniu zadania, katalogiem do którego zapisane zostaną wyniki zadania.
1.6.4.	Narzędzie do porównania danych zapisanych w systemach PACS: produkcyjnym i testowym. Następujących dane zapisane w obu systemach mogą zostać porównane: metadane konfiguracji systemu, kartoteki pacjentów (wszystkie zgromadzone w systemie PACS albo tylko jedna), badania, załączniki do badania, opisy badań. Narzędzie umożliwia zdefiniowanie harmonogramu zadania, wykonywanego po stronie serwera. Wykonanie zadania może być sygnalizowane wysłaną wiadomością e-mail. Wyniki zadania mogą zostać zapisane w pliku CSV lub XLS.
1.6.5.	Narzędzie służące do wyświetlania dzienników zdarzeń serwera PACS. Umożliwia pobranie i połączenie w jednym miejscu dzienników zdarzeń wskazanych bądź wszystkich serwerów funkcjonalnych klastra serwera PACS. Dzienniki zdarzeń mogą być pobrane na bieżąco z serwerów bądź wskazane jako plik ZIP uprzednio zarchiwizowanych dzienników zdarzeń. Możliwe jest również otwarcie pojedynczego dziennika zdarzeń, wskazanego jako plik z rozszerzeniem LOG. Zdarzenia ładowane z dzienników do pamięci roboczej narzędzia mogą być filtrowane wg następujących kryteriów: zakres czasu zdarzeń, kategoria zdarzenia (wszystkie, informacja rozszerzona, informacja, ostrzeżenie, błąd). Wyświetlane zdarzenia mogą być przeszukiwane wg następujących kryteriów: węzeł klastra który zapisał zdarzenie, plik dziennika zdarzeń w którym zostało ono zapisane, wątek serwera który zapisał zdarzenie, moduł serwera którego dotyczy zdarzenie, kategoria zdarzenia, treść komunikatu zdarzenia. W przypadku treści komunikatu zdarzenia możliwe jest użycie kilku fraz połączonych spójnikami logicznymi ORAZ bądź LUB. Wyświetlane zdarzenia mogą być eksportowane do: schowka systemu operacyjnego, pliku CSV, pliku XML, pliku XLS. Narzędzie umożliwia analize liczby wystąpień poszczególnych komunikatów w wyświetlanych zdarzeniach. Narzędzie umożliwia eksport pojedynczego pliku dziennika zdarzeń, w którym znajduje się wskazane zdarzenie.

1.6.6.	"Narzędzie do wyszukiwania i przeglądania kartotek pacjentów. Kartoteki mogą być wyszukiwane wg następujących kryteriów: identyfikator pacjenta, imię, nazwisko, data urodzenia, numer akcesji badania (accession number), identyfikator wizyty (admission number), wewnętrzny identyfikator rekordu pacjenta w bazie danych serwera PACS. Kryteria mogą zawierać znaki wieloznaczne, np do wyszukiwania pacjentów o nazwisku zaczynającym się danym ciągiem liter. Narzędzie wyświetla następujące elementy kartoteki pacjenta : dane demograficzne, identyfikatory wraz z domenami wystawcy identyfikatora, połączone kartoteki, dane kontaktowe, załączniki do rekordu pacjenta, dane wizyt, lista badań. Po wskazaniu kartoteki pacjenta, możliwe są następujące operacje na niej: eksport danych do pliku XLS, dodanie/edycja/modyfikacja statusu aktywności/usunięcie identyfikatora pacjenta. Po wskazaniu badania w kartotece pacjenta, można wysłać wiadomości HL7 ORM lub ORU zawierające informacje o: ostatnim zapisanym w systemie PACS statusie badania, dostępności obrazów, opisie badania.
1.6.7.	Po wyszukaniu i wskazaniu kartoteki pacjenta możliwe jest również połączenie jej z inną kartoteką. Operacja odwrotna - rozłączenie błędnie połączonych kartotek - również jest możliwa. Narzędzie umożliwia przenoszenie badań z błędnie przypisanej kartoteki pacjenta do właściwej. Narzędzie udostępnia wyniki działania wewnętrznego procesu serwera PACS, który monitoruje operacje łączenia kartotek pacjenta i według zdefiniowanych reguł oznacza niektóre z nich jako nietypowe - przykładowo gdy łączone są kartoteki pacjentów różnej płci. Z poziomu listy nietypowych połączeń kartotek, szpitalny administrator systemu PACS może - w zależności od stanu faktycznego - dokonać właściwych korekt, uprzednio opisanymi funkcjonalnościami. Ponieważ źródłem danych kartoteki pacjenta może być albo szpitalny rekord pacjenta w systemie HIS, albo metadane zawarte w badaniu, w wyjątkowych przypadkach niezgodności w danych mogą spowodować że dane badanie nie będzie otwierane przez system PACS z powodu niejednoznaczności co do stanu faktycznego. Jedna z funkcjonalności narzędzia pozwala wskazać z którego źródła dane w kartotece są zgodne ze stanem faktycznym - co skutkować będzie ich wyświetleniem wraz z obrazami badania w systemie PACS. Wszystkie operacje wykonane w narzędziu, jak również wyszukiwanie i otrzymane rezultaty, zapisywane są w odrębnym dzienniku zdarzeń, dostępnym z poziomu poleceń narzędzia."
1.6.8.	"Narzędzie pozwalające na zarządzane badaniami przechowywanymi na serwerze PACS. Zbiór badań może być wskazany jako tekstowa lista identyfikatorów badania (Study UID) lub zapytanie SQL do bazy danych. Lista może być edytowana poprzez dodawanie lub usuwanie pojedynczych badań. Możliwy jest eksport listy wybranych badań. Operacje na badaniach możliwe są na poziomie: badania, serii, obiektu DICOM (instancji). Każda z operacji na zbiorze badań może zostać wykonana i kontrolowana przez narzędzie uruchomione na stacji roboczej bądź jako zadanie serwera PACS. W drugim przypadku możliwe jest zdefiniowanie harmonogramu wykonania zadania.
1.6.9.	Operacje możliwe do wykonania przez narzędzie na zbiorze badań to: skopiowanie do wybranego zewnętrznego węzła DICOM, archiwizacja w systemie PACS, archiwizacja w wybranym zewnętrznym systemie PACS, synchronizacja badań w archiwum krótkoterminowym (incoming cache) z archiwum długoterminowym, usunięcie badań z systemu PACS, powtórne uruchomienie reguł transferu zdefiniowanych w systemie PACS, wysyłka wiadomości HL7 ORM lub ORU zawierających informacje o: ostatnim zapisanym w systemie PACS statusie badania/dostępności obrazów/opisie badania. Każda z wykonanych operacji zapisywana jest w odrębnym dzienniku zdarzeń - dostępnym z poziomu narzędzia."
1.6.10.	Narzędzie wykonujące bezpośrednie zapytania SQL na bazie danych systemu PACS. Wszystkie prezentowane informacje są tylko do odczytu. Niektóre z uprzednio zdefiniowanych zapytań, dostępnych przy użyciu narzędzia: 1.6.10.1. szczegółowy wykaz zmian statusu zadania, osoby do której zostało ono przypisane oraz wyzwolonych reguł przebiegu pracy 1.6.10.2. szczegółowy wykaz operacji wykonanych na badaniu

	1.6.10.3. wykaz zapytań SQL w największym stopniu obciążających serwer bazy danych 1.6.10.4. wykaz i ustawienia zewnętrznych systemów zdefiniowanych w systemie PACS 1.6.10.5. wykaz zewnętrznych systemów, które nie wymieniały się danymi z systemem PACS przez ostatnie 60 dni 1.6.10.6. wykaz stacji roboczych ostatnio podłączonych do serwera PACS 1.6.10.7. wykaz nieukończonych zadań, pogrupowany wg typu zadania. 1.6.10.8. historia procedur danego badania 1.6.10.9. historia zadań, umożliwiająca odpowiedź na pytanie czy dane zadanie zostało wyświetlone na liście badań danego użytkownika 1.6.10.10. wykaz zadań nie przypisanych do żadnego użytkownika 1.6.10.11. szczegółowy wykaz pamięci podręcznych (cache), archiwów oraz systemów plików - zdefiniowanych w systemie PACS 1.6.10.12. wykaz uprawnień wskazanego użytkownika 1.6.10.13. wykaz podstawowych parametrów opisujących rozmiar bazy danych systemu PACS: liczba badań, badania zapisane wczoraj, liczba badań nie powiązanych ze zleceniem z systemu HIS/RIS, całkowita liczba zleconych procedur, liczba badań wewnętrznych i zewnętrznych, liczba aktywnych i nieaktywnych kartotek pacjentów, liczba użytkowników i kontaktów 1.6.10.14. wzrost rozmiaru bazy danych, przedstawiony w MB lub GB, pomiędzy dwiema wskazanymi datami 1.6.10.15. wykaz wierszy bazy danych zablokowanych przez sesje użytkowników z możliwością odblokowania 1.6.10.16. wykaz pacjentów z największą liczbą badań 1.6.10.17. wykaz instancji badania, z wyszczególnieniem miejsca przechowywania i rozmiaru na dysku 1.6.10.18. wykaz wszystkich miejsc w których badanie jest zapisane 1.6.10.19. wykaz operacji zapisanych w kolejkach systemowych Przez zadanie rozumiane jest jedno z zadań zdefiniowanych w przebiegu pracy nad badaniem od momentu akwizycji do podpisania opisu. Powyższa lista obejmuje tylko najczęściej używane informacje, dostępne przy użyciu narzędzia. Ponadto możliwe jest wykonanie dowolnego, nie zdefiniowanego wcześniej zapytania SQL do bazy danych systemu PACS - z zastrzeżeniem że możliwy jest jedynie odczyt danych.
1.6.11.	Narzędzie umożliwiające zarządzanie ustawieniami pulpitu pojedynczego użytkownika systemu. Wyświetlane są wszystkie ustawienia aplikacji pulpitu systemu PACS, wprowadzone przez użytkownika. Możliwe jest skopiowanie ustawień do innego użytkownika bądź ich usunięcie.

Charakterystyka przeglądarki webowej

Lp.	Charakterystyka (wymagania minimalne)
1.7.1.	System dystrybucji obrazów przez przeglądarkę internetową zarejestrowany w Polsce jako wyrób medyczny w klasie co najmniej II a lub posiadające certyfikat CE właściwy dla

	urządzeń/oprogramowania medycznego w klasie co najmniej II a stwierdzający zgodność z dyrektywą 93/42/EEC.
1.7.2.	Oferowana przeglądarka kliniczna (webowa) tego samego producenta co system PACS (wspólna baza użytkowników)
1.7.3.	Oprogramowanie klienta korzystające wyłącznie z bazy danych badań systemu PACS (architektura klient - serwer)
1.7.4.	Oprogramowane umożliwia nielimitowany dostęp jednocześnie pracujących użytkowników na 120 000 badań z zachowaniem pełnego dostępu do wszystkich zarchiwizowanych badań.
1.7.5.	Możliwość jednoczesnej współpracy z wieloma systemami PACS różnych producentów.
1.7.6.	Oprogramowanie klienta nie przechowuje lokalnie danych obrazowych ani bazy danych wykonanych badań/pacjentów
1.7.7.	Klient systemu dystrybucji obrazów działa w oparciu o przeglądarkę internetową zgodną z HTML 5, Google Chrome (najnowsza wersja), Microsoft Edge, Mozilla FireFox (najnowsza wersja), Apple Safari (najnowsza wersja)
1.7.8.	Brak konieczności instalowania na komputerze klienta jakichkolwiek aplikacji lub dodatków (np. plug in) do obsługiwanych przeglądarek internetowych.
1.7.9.	Klient systemu dystrybucji obrazów działa w systemach operacyjnych min. Windows 10, Windows 11, Mac OS X.
1.7.10.	Możliwość wywołania aplikacji bezpośrednio z systemów trzecich (HIS) z jednoczesnym wyświetleniem obrazów wybranego badania bez możliwości dalszego wyszukiwania (innych) badań
1.7.11.	Aplikacja umożliwia wyświetlanie i oglądanie badań w jakości diagnostycznej
1.7.12.	Aplikacja pozwalająca wyświetlić dowolny rodzaj danych pobranych z systemu/ów PACS (tj. obrazy badań rentgenodiagnostycznych, zdjęcia stomatologiczne wewnątrz ustne, zdjęcia tradycyjne, filmy pochodzące z laparoskopów/endoskopów, raporty strukturalne DICOM, Encapsulated PDF, Basic Voice Audio Waveform)
1.7.13.	Dostęp do systemu tylko po uprzednim zalogowaniu się
1.7.14.	Funkcjonalność ustawienia czasu automatycznego wylogowania z oprogramowania w przypadku braku aktywności
1.7.15.	Interfejs użytkownika oprogramowania w języku polskim
1.7.16.	Oprogramowanie zawiera wbudowany manual kontekstowy dla użytkownika w języku polskim i angielskim
1.7.17.	Możliwość wybrania min. następujących wersji kolorystycznych aplikacji: • dedykowanej dla pomieszczeń o wysokim naświetleniu, • dedykowanej dla pomieszczeń o niskim naświetleniu
1.7.18.	Aplikacja pozwala wyszukać badania na podstawie dowolnej kombinacji warunków, min.: • imię i nazwisko pacjenta, • płeć pacjenta, • data urodzenia, • PESEL, • zlecający badanie, • ID pacjenta,

	• data badania (w tym spośród zdefiniowanych okresów, np. dzisiaj, wczoraj, • ostatni tydzień, ostatni miesiąc) • ID badania/ numer badania • modalność/ rodzaj urządzenia diagnostycznego
1.7.19.	Funkcja wyświetlenia/ukrycia danych demograficznych pacjenta na obrazach
1.7.20.	Funkcja eksportu wybranego obrazu badania bez danych osobowych na lokalne urządzenie w formatach takich jak: png, jpg
1.7.21.	Funkcja eksportu badania (DICOM) do pliku .zip z możliwością szyfrowania danych hasłem dostępu do pliku poprzez manualne wprowadzenie hasła przez użytkownika eksportującego.
1.7.22.	Funkcja udostępniania badań na zewnątrz za pomocą wygenerowanego łącza (adresu www) i przesłanego przez dowolny kanał komunikacji. Dostęp do udostępnionego badania pacjenta jest czasowy (okres ważności linku określa administrator systemu) i jest chroniony hasłem. Dostęp nie wymaga stworzenia nowego konta użytkownika.
1.7.23.	Funkcja wybrania wielu badań tego samego pacjenta wraz z możliwością udostępnienia ich dla zewnętrznego użytkownika za pomocą wygenerowania jednego linku chronionego hasłem.
1.7.24.	Aplikacja udostępnia dla zewnętrznego użytkownika, któremu udostępniono link pełen dostęp do zaawansowanych narzędzi przeglądarki klinicznej umożliwiających ocenę badania - wraz z możliwością dodania i aktywnego porównania udostępnionych badań w jednym widoku (jeśli udostępniono więcej niż jedno).
1.7.25.	Funkcja wspólnej pracy na tym samym badaniu dwóch użytkowników (konsultacja): • zaproszenie uczestnika do konsultacji przez wbudowany czat • współdzielenie ekranu: wyświetlanych obrazów, wykonywanych pomiarów, nanoszonych adnotacji oraz manipulacji obrazami w tym rekonstrukcji w czasie rzeczywistym z wizualizacją położenia kursora myszy udostępniającego • możliwość przejęcia kontroli nad obrazem przez konsultanta
Operacje na obrazach	
1.7.26.	Funkcja powiększania obrazu, min.: • płynne powiększanie oraz pomniejszanie za pomocą myszy; • powiększenie 1:1;
1.7.27.	Funkcja powiększania wybranego fragmentu obrazu, tzw. Lupa - powiększenie x2, x4, x6
1.7.28.	Funkcja pomiaru kątów
1.7.29.	Funkcja pomiaru kąta, w tym także: pomiary kąta Cobba oraz kąta HKA
1.7.30.	Funkcja wyznaczenia linii centralnej
1.7.31.	Funkcja pomiaru różnicy długości pomiędzy dwoma wyznaczonymi prostymi
1.7.32.	Funkcja pomiaru prostopadłego - odległość punktu od wyznaczonej linii
1.7.33.	Funkcja pomiaru równoległego poziomego
1.7.34.	Pomiar odległości pomiędzy dwoma punktami na obrazie
1.7.35.	Funkcja pomiaru stosunku długości dwóch linii zdefiniowanych przez użytkownika (np. wskaźnik sercowo-płucny)
1.7.36.	Funkcja usunięcia pomiarów wprowadzonych przez użytkownika

1.7.37.	Funkcja dodania adnotacji, dowolnego tekstu do obrazu badania o długości min. 16 znaków
1.7.38.	Funkcja usunięcia adnotacji wprowadzonych przez użytkownika
1.7.39.	Funkcja zapisania adnotacji na obrazie przez użytkownika. Zapisane adnotacje są dostępne dla innych użytkowników systemu.
1.7.40.	Funkcja przemieszczania i edycji wszystkich adnotacji wprowadzonych przez użytkownika
1.7.41.	Funkcja wyświetlenia/ukrycia adnotacji wprowadzonych przez użytkownika
1.7.42.	Funkcja dodania strzałki do obrazu badania
1.7.43.	Funkcja przedstawienia przebiegu wartości piksela wzdłuż wyznaczonej prostej
1.7.44.	Funkcja wygenerowania histogramu dla wybranego obszaru oznaczonego na obrazie
1.7.45.	Funkcja wyświetlania wartości dla zaznaczonego piksela wartości gęstości optycznej dla badań CR oraz jednostek Hounsfielda dla badań TK
1.7.46.	Funkcja ukrycia dodanych znaczników na obrazie
1.7.47.	Pomiar odległości za pomocą linii krzywej
1.7.48.	Funkcja oznaczenia regionu zainteresowania (ROI) za pomocą okręgu, elipsy, wielokąta.
1.7.49.	Funkcja obrotu obrazu o 180˚ oraz o 90˚ stopni
1.7.50.	Funkcja odbicia obrazu w poziomie oraz w pionie
1.7.51.	Funkcja płynnego obrotu obrazu o dowolnie wybrany przez użytkownika kąt
1.7.52.	Funkcja kolimacji obrazu badania: prostokątna i eliptyczna
1.7.53.	Funkcja kalibracji liniowej i kołowej obrazu w celu prawidłowego wyświetlania wartości odległości pomiędzy dwoma punktami, kalibracja przeprowadzona przez użytkownika względem obiektu odniesienia na obrazie
1.7.54.	Inwersja pozytyw/negatyw w obrazie badania
1.7.55.	1.7.55.1. Funkcja płynnej regulacji kontrastu na obrazie oraz możliwość wybrania z predefiniowanych ustawień dla: mózgu, kości, śródpiersia, płuc, wątroby, brzucha, miednicy. 1.7.55.2. Funkcja zdefiniowania na poziomie użytkownika skrótów klawiszowych dla uruchomienia wybranych ustawień okna na obrazie.
1.7.56.	Funkcja definiowania własnych predefiniowanych ustawień poziomu okna (W/L) z uwzględnieniem filtra wyostrzającego dla wybranych parametrów okna.
1.7.57.	Funkcja powrotu do oryginalnej (dostępnej w systemie PACS) postaci obrazu.
1.7.58.	Funkcja cofnięcia ostatnio wykonanej zmiany obrazu
1.7.59.	Funkcja jednoczesnego przewijania obrazów wielu wyświetlanych serii badania pacjenta
1.7.60.	Funkcja wyświetlania oraz ukrycia linii referencyjnych na innych płaszczyznach podczas przewijania obrazów z wybranej serii badania
1.7.61.	Funkcja przeglądania animacji wraz z możliwością ustawień: • prędkości animacji; • zakresu obrazów do animacji; • przeglądanie animacji w pętli; • zmiany kierunku animacji;
1.7.62.	Funkcja - przełączanie się pomiędzy obrazami w serii min. Obraz po obrazie (w obie strony)
1.7.63.	Funkcja rekonstrukcji wielopłaszczyznowych MPR, rekonstrukcje MIP

1.7.64.	Funkcja regulacji grubości warstwy w projekcjach MPR z możliwością wyboru spośród zdefiniowanych wartości oraz poprzez manualne dostosowanie
1.7.65.	Funkcja rekonstrukcji 3D
1.7.66.	Funkcja rekonstrukcji po krzywej CPR wyznaczonej wzdłuż linii wskazanej poprzez użytkownika; renderowanie w widokach: straightened CPR, stretched CPR
1.7.67.	Automatyczne usuwanie stołu w wyświetlanych rekonstrukcjach 3D (CT)
1.7.68.	Funkcja usuwania kości w wyświetlanych rekonstrukcjach 3D (CT)
1.7.69.	Funkcja odcinania płaszczyzn w widokach 3D w celu uwidocznienia obszaru zainteresowania.
1.7.70.	Funkcja pomiaru pojemności komory serca
1.7.71.	Funkcja pomiaru przegrody międzykomorowej (IVS), jamy lewej komory (LVID), ściany tylnej lewej komory (LVPW) TAK
1.7.72.	Funkcja pomiaru czasu spadku ciśnienia do połowy (PHT)
1.7.73.	Funkcja pomiaru całki prędkości przepływu w czasie (VTI)
1.7.74.	Funkcja pomiaru odległości w badaniach jednowymiarowych (M-mode)
1.7.75.	Funkcja pomiaru czasu w badaniach jednowymiarowych (M-mode) i dopplerowskich
1.7.76.	Funkcja pomiaru prędkości w badaniach dopplerowskich
1.7.77.	Aplikacja zapewnia wyświetlanie listy poprzednio wykonanych badań pacjenta w postaci: • tekstowej listy badań wraz z miniaturami dostępnych opisów badań • miniatur obrazów badań przedstawionych na osi czasu
1.7.78.	Aplikacja umożliwia wyświetlenie opisu badania w formie pdf.
1.7.79.	Aplikacja pozwala wyświetlić jednocześnie min. 1-8 serii badania
1.7.80.	Aplikacja pozwala wyświetlić jednocześnie min. 4 różne badania tego samego pacjenta w tym samym widoku (na jednym ekranie)
1.7.81.	Funkcja utworzenia i zapisania migawki (zrzutu) oglądanego w danej chwili obrazu do późniejszego odtworzenia widoku, na którym została utworzona migawka do dalszej pracy na badaniu od tego miejsca. W systemie jest widoczne kto i kiedy taki zrzut wykonał.
1.7.82.	Aplikacja posiada możliwość wybrania sposobu prezentacji obrazów zgodnie z wybranym protokołem wyświetlania badania.
1.7.83.	Możliwość wybrania spośród dostępnych (i utworzonych przez użytkownika) protokołów wyświetlania i zapisania ich "jako ulubione" dostępnych na podręcznej liście dla zalogowanego użytkownika.
1.7.84.	System umożliwia szybkie porównanie badań historycznych pacjenta (dla tej samej modalności) wyświetlanych w nawigatorze serii. Możliwość poruszania sie pomiędzy badaniami bez konieczności przeglądania i przeciągania konkretnej serii w wyświetlanym widoku.
1.7.85.	Progresywne wyświetlanie obrazów - szybkie wyświetlanego obrazu i stopniowe przesyłania kolejnych danych (np. pozostałych obrazów serii)
1.7.86.	Dostęp do zaawansowanych protokołów wyświetlania dla badań: USG, RTG, MMG, TK, MR, PET-CT,
1.7.87.	Funkcja oznaczania kręgów i krążków międzykręgowych kręgosłupa. Oznaczenia kolejnych kręgów/krążków na obrazie badania wyświetlane są w rzutach MPR

1.7.88.	Funkcja fuzji dwóch zarejestrowanych serii badań. Możliwość regulacji blendy pomiędzy wyświetlanymi seriami
1.7.89.	Funkcja wyświetlenia topogramu dla badań TK i MR
1.7.90.	Funkcja zdefiniowania skrótów klawiszowych na poziomie zalogowanego użytkownika dla operacji: • pomiar odległości • pomiar stosunku długości 2 wyznaczonych prostych (wskaźnik sercowo-płucny) • pomiar gęstości (ROI) za pomocą narzędzi: okręgu oraz elipsy 2 i 3 punktowej • pomiar kąta (w tym kąta Cobba) • włącz/ukryj linie MPR • utworzenia i zapisania migawki (zrzutu) oglądanego w danej chwili obrazu do późniejszego odtworzenia widoku, na którym została utworzona migawka.
1.7.91.	Możliwość utworzenia na poziomie zalogowanego użytkownika własnych protokołów wyświetlania dla poszczególnych typów urządzeń z uwzględnieniem układu wyświetlania (layout), wskazania, która seria powinna zostać wyświetlona w danym widoku (layoucie). Możliwość utworzenia protokołów wyświetlania zarówno dla badań aktualnych (bieżących) jak i dla badań porównawczych
Import plików non-DICOM	
1.7.92.	Funkcja importu do historii pacjenta plików non-dicom jako nowego badania widocznego bezpośrednio w historii badań z funkcją ich dicomizacji oraz późniejszego wyświetlenia w przeglądarce badań obrazowych. Wsparcie dla formatów plików non-dicom: PDF; zdjęć cyfrowych (JPG i PNG); plików wideo (MP4, AVI, MOV, MP4) oraz audio (MP3, WAV)
1.7.93.	Funkcja importu plików non-dicom do istniejącego badania. Zaimportowany plik/pliki widoczne są jako nowa dodatkowa seria w badaniu
1.7.94.	Podczas importu plików non-dicom istnieje możliwość wybrania oddziału/pracowni, która importuje wybrany plik wraz z wybraniem nazwy procedury (ze zdefiniowanego słownika) oraz określenie daty i godziny badania (np. data o godzina wykonania zdjęcia ran, kontrolowanych znamion, blizn pooperacyjnych itp.) przy czym domyślną wartością daty i godziny jest chwila importu pliku do archiwum systemu.
1.7.95.	Funkcja opisania importowanych plików (w tym serii zdjęć) poprzez wprowadzenie wolnego tekstu przez użytkownika importującego dane. Wprowadzony tekst jest widoczny podczas wyświetlania obrazów w przeglądarce
1.7.96.	Funkcja wyświetlania paska postępu dla importowanych plików non-dicom wraz z komunikatem o zakończeniu importu danych do systemu (w przypadku błędu importu widoczny komunikat o niepowodzeniu importu danych)
1.7.97.	Możliwość wykonania pomiarów rzeczywistych dla importowanych zdjęć, np.: zdjęć ran, znamion wykonanych wraz z punktem odniesienia (miarką, linijką). Funkcji kalibracji pomiarów na obrazie.

Charakterystyka modułu ortopedycznego

Lp.	Charakterystyka (wymagania minimalne)
Endoprotezoplastyka całkowita stawu biodrowego	
1.8.1.	Kreator SmartHip do automatycznego nakładania wzorców

1.8.2.	Automatyczna korekta różnicy długości nóg
1.8.3.	Ustawienie i pomiar kąta nachylenia panewki
1.8.4.	Redukcja jednym kliknięciem w celu wizualizacji wyniku operacji
1.8.5.	Interaktywna prezentacja po redukcji
Endoprotezoplastyka całkowita stawu kolanowego	
1.8.6.	Ocena zdjęć pomiarowych kończyn dolnych
1.8.7.	Automatyczne wykrywanie osi anatomicznej kości udowej i linii stawu kolanowego
1.8.8.	Pomiar miejsc cięcia kości piszczelowej i udowej
1.8.9.	Redukcja jednym kliknięciem w celu wizualizacji wyniku operacji
1.8.10.	Unikalna prezentacja offsetu trzpienia rewizyjnego
Podstawowe zalety wzorców	
1.8.11.	Pełna zgodność z wieloskładnikowymi systemami rewizyjnymi
1.8.12.	Możliwość ustawienia preferowanych przez użytkownika wzorców protez jako domyślnych
1.8.13.	Możliwość usunięcia niepotrzebnych wzorców z serwera za pomocą aplikacji klienckiej
1.8.14.	Zmiana lub dodawanie wielu protez w dowolnym momencie
1.8.15.	Blokowanie pozycji wzorca
1.8.16.	Ukrywanie/pokazywanie wzorca
1.8.17.	Zmiana kolorów poszczególnych wzorców
1.8.18.	Możliwość kontralateralnego ustawienia wzorca
1.8.19.	Możliwość ponownego dopasowania do kreatora
Obsługiwane procedury wymiany stawów	
1.8.20.	Endoprotezoplastyka całkowita stawu biodrowego, endoprotezoplastyka połowiczna i kapoplastyka stawu biodrowego
1.8.21.	Endoprotezoplastyka całkowita i jednoprzedziałowa stawu kolanowego
1.8.22.	Endoprotezoplastyka całkowita stawu barkowego i kapoplastyka kości ramiennej
1.8.23.	Stawy łokciowe, kostki, kolana i nadgarstki
1.8.24.	Artrodeza
1.8.25.	Specjalne kreatory
1.8.26.	Różnica długości nóg
1.8.27.	Skalowanie i pozycjonowanie wzorca w płaszczyznach AP i ML w endoprotezoplastyce całkowitej stawu biodrowego
1.8.28.	Skalowanie i pozycjonowanie wzorca w płaszczyznach AP i ML w kapoplastyce stawu biodrowego
1.8.29.	Pomiar kąta szyjki kości udowej
1.8.30.	Prowadnice do cięcia szyjki (3 typy)
1.8.31.	Skalowanie i pozycjonowanie komponentu udowego w endoprotezoplastyce stawu kolanowego
1.8.32.	Skalowanie i pozycjonowanie komponentu piszczelowego w endoprotezoplastyce stawu kolanowego (dwa typy)
1.8.33.	Ułożenie nóg (szpotawość/koślawość kolana)
1.8.34.	Skalowanie i pozycjonowanie w endoprotezoplastyce całkowitej stawu barkowego (system Zimmer Anatomical Shoulder)
1.8.35.	Skalowanie i pozycjonowanie w kapoplastyce kości ramiennej
Traumatologia	
1.8.36.	Obsługuje wszystkie procedury z zakresu traumatologii, w tym:
1.8.37.	Wszystkie rodzaje płytek, także okołostawowe
1.8.38.	Śruby
1.8.39.	Gwoździe
1.8.40.	Dynamiczny stabilizator biodrowy

1.8.41.	Endoprotezoplastyka połowiczna
1.8.42.	Redukcja złamań widoczna na ekranie:
1.8.43.	Obsługuje złamania wielofragmentowe
1.8.44.	Edytowalne kontury
1.8.45.	Fragmenty z konturami lub bez, przezroczystość i cienie
1.8.46.	Płytki
1.8.47.	Zmiana rozmiaru wzorca za pomocą kliknięcia i przeciągnięcia myszą
1.8.48.	Śruby są automatycznie umieszczane prawidłowo
1.8.49.	Zmiana typu śruby; kolejność wstawiania; ustawienie
1.8.50.	Kreatory
1.8.51.	Kąt złamania wału
1.8.52.	Kąt i przesunięcie
1.8.53.	Możliwość zginania płytki na ekranie w celu wizualizacji położenia śrub
1.8.54.	Możliwość ukrycia wszystkich śrub.
Wysoka osteotomia kości piszczelowej	
1.8.55.	Kreator pozycjonowania kończyn dolnych
1.8.56.	Dodawanie cięć otwartych, zamkniętych lub rotacyjnych
1.8.57.	Odczyt wielkości klina – kąt i rozwarcie w mm.
1.8.58.	Automatyczna redukcja
Ocena dysplazji stawu biodrowego	
1.8.59.	Specjalne kreatory
1.8.60.	Linia Hilgenreinera
1.8.61.	Kąt nachylenia panewki stawu biodrowego
1.8.62.	Kąt biodrowy
1.8.63.	Linia Perkinsa
1.8.64.	Wskaźnik migracji głowy kości udowej wg Reimersa
1.8.65.	Kąt pokrycia głowy Wiberga
1.8.66.	Linia TT
1.8.67.	Kąt Sharpa
Ocena i korekcja deformacji kończyn	
1.8.68.	Zestaw narzędzi pozwalających ocenić deformację kończyny i zaplanować operację korekcyjną metodą CORA.
1.8.69.	Test nieprawidłowego ustawienia w płaszczyźnie czołowej – mierzy odchylenie osi mechanicznej (MAD) i ustala źródło MAD
1.8.70.	Test nieprawidłowego ustawienia w płaszczyźnie strzałkowej - ocena orientacji linii dalszego odcinka kości udowej i bliższej linii stawu piszczelowego
1.8.71.	Wizualizacja graficzna deformacji płaszczyzny skośnej - określenie płaszczyzny, kierunku i wielkości kąta pochylenia płaszczyzny skośnej. Określenie CORA dla deformacji kości piszczelowej i udowej, zarówno poprzez ocenę osi mechanicznej, jak i anatomicznej.
1.8.72.	Redukcja na ekranie dla osteotomii otwierającej, zamykającej i rotacyjnej
1.8.73.	Redukcja automatyczna
1.8.74.	Możliwość ustawienia kąta CORA
1.8.75.	Automatyczne określanie konturów kości przez użytkownika w celu symulacji wyniku operacji
1.8.76.	Obsługa stabilizatora Taylor Spatial Frame - ustalenie pozycji wyjściowej stabilizatora względem kości (dwa kreatory)
1.8.77.	Specjalne narzędzie do pomiaru kąta służące do oceny choroby Blounta
Ocena deformacji kręgosłupa	
1.8.78.	Zestaw narzędzi umożliwiających ocenę deformacji kręgosłupa tj. skoliozy, kifozy, lordozy, kręgozmyków.

1.8.79.	Lista oferowanych pomiarów opiera się na wymaganiach zarówno HARMS, jak i Spinal Deformity Study Group; jednak będą one przydatne dla każdego, kto pracuje w tej dziedzinie.
Kreatory – płaszczyzna czołowa (AP)	
1.8.80.	Krzywa odcinka proksymalnego kręgosłupa piersiowego
1.8.81.	Krzywa odcinka głównego kręgosłupa piersiowego
1.8.82.	Krzywa kręgosłupa lędźwiowego
1.8.83.	Balans czołowy
1.8.84.	Przemieszczenie wierzchołkowe
1.8.85.	Transpozycja tułowia w odcinku piersiowym
1.8.86.	Ocena rotacji kręgów Nash-Moe
1.8.87.	Test Rissera
Kreatory – płaszczyzna strzałkowa (LAT)	
1.8.88.	Kąt Cobba T2-T12
1.8.89.	Kąt Cobba T5-T12
1.8.90.	Kąt Cobba T10-L2
1.8.91.	Kąt Cobba T12-S1
1.8.92.	Balans strzałkowy
1.8.93.	Kąt ustawienia kości krzyżowej względem miednicy
1.8.94.	Kąt nachylenia kości krzyżowej
1.8.95.	Kąt nachylenia miednicy
Inne narzędzia	
1.8.96.	Ogólny kąt Cobba
1.8.97.	Wielokrotny kąt Cobba
1.8.98.	Długość całkowita (kręgosłupa)
1.8.99.	Środek kręgu
1.8.100.	Odległość między dwiema pionowymi liniami
1.8.101.	Graficzny „haczyk” wskazujący położenie haków instrumentu
Specyfikacja ogólna	
1.8.102.	Liczba licencji- 3
1.8.103.	Obsługiwane systemy operacyjne — Windows 10; Windows 11
Interfejs użytkownika	
1.8.104.	Możliwość odkodowania lewego panelu i paneli SmartHelp
1.8.105.	Możliwość ponownego rozpoczęcia sesji planowania (bez ponownego wczytania obrazów)
1.8.106.	Opcja Cofnięcia/ponowienia operacji umieszczenia kreatora
1.8.107.	Moduł ortopedyczny jest zintegrowany z systemem PACS i jest wywoływany z poziomu pulpitu klinicysty za pomocą jednego kliknięcia
1.8.108.	Ulepszony selektor procedur z dostępem do informacji o uzupełniających produktach i usługach 3D.
Importowanie i eksportowanie obrazu	
1.8.109.	DICOM Q/R — pobiera obrazy z systemu PACS
1.8.110.	Import obrazu DICOM z płyty CD
1.8.111.	Import obrazu DICOM z folderu
1.8.112.	Zaakceptuj przesyłanie obrazów DICOM
1.8.113.	DICOM C-Store — wysyłanie obrazów zawierających wzorce z powrotem do systemu PACS
1.8.114.	Eksport obrazów z wzorcem i raportów w formacie *.jpg
1.8.115.	Wydruk obrazów z wzorcem i raportów
Skalowanie obrazu	
1.8.116.	Automatyczne skalowanie Quickscale dla znaczników kulistych i okrągłych

1.8.117.	Ręczne skalowanie za pomocą linijki lub okręgu
1.8.118.	Szacowane skalowanie nadwymiaru w przypadku braku znacznika
1.8.119.	Blokada i ostrzeganie o nieoczekiwanych (poza zakresem 100-150%) wartościach powiększenia
Obsługa obrazu	
1.8.120.	Jednoczesne wczytywanie do 4 obrazów
1.8.121.	Minimalizowanie lub zamykanie okien obrazów
1.8.122.	Możliwość odbicia lustrzanego, odwrócenia i obrócenia obrazu
1.8.123.	Szkło powiększające „Blue Lens”.
1.8.124.	„Mini widok”
1.8.125.	Odwrócenie skali szarości
1.8.126.	Regulacja i reset okna/poziomu
1.8.127.	Wielostopniowy zoom z możliwością dopasowania do okna
1.8.128.	Możliwość wyboru głębi kolorów (kolorowe lub w skali szarości) dla obrazów, które użytkownik chce wysłać do PACS
1.8.129.	Obrót obrazów w oparciu o umieszczoną linię poziomą lub pionową.
1.8.130.	Graficzne przedstawienie widoków rentgenowskich.
Komentowanie i pomiar obrazów	
1.8.131.	Automatyczne i konfigurowalne nakładanie obrazu
1.8.132.	Rysowanie linii
1.8.133.	Rysowanie okręgu
1.8.134.	Dodawanie znacznika w postaci kropki
1.8.135.	Pomiar długość linii
1.8.136.	Pomiar długość linii wieloodcinkowej
1.8.137.	Pomiar kąta
1.8.138.	Pomiar wielu kątów
1.8.139.	Pomiar małego kąta (kąt Cobba)
1.8.140.	Pomiar odległości pomiędzy dwiema pionowymi liniami
1.8.141.	Tworzenie dwóch linii równoległych
1.8.142.	Tworzenie dwóch linii prostopadłych
1.8.143.	Tworzenie linii pod określonym kątem jedna do drugiej
1.8.144.	Znajdowanie środka (kręgu)
Pomoc	
1.8.145.	Pełna pomoc kontekstowa dostępna w aplikacji
1.8.146.	Instrukcje krok po kroku dla najpopularniejszych kreatorów
Ustawienia użytkownika	
1.8.147.	Domyślna proteza dla każdej klasy zabiegu (biodro, kolano itp.)
1.8.148.	Punkt odniesienia dla protezy kolana – przedni lub tylny
1.8.149.	Opcje kreatora SmartHip
1.8.150.	Domyślny kąt nachylenia panewki
1.8.151.	Domyślne ustawienie wartości przeskalowania dla każdego typu obrazu
1.8.152.	Kolor kreatorów, wzorców, wymiarów itp.
Preferencje systemu	
1.8.153.	Zdefiniowanie hasła dostępu do ustawień
1.8.154.	Możliwość ukrycia/pokazania Modułu Oceny Pediatrycznej (PAM); deformacja kończyn; procedury traumatologiczne
1.8.155.	Kontrolowane skalowanie toku pracy; planowanie; redukcja; użycie wzorców
1.8.156.	Możliwość edycji i zapisu wielu połączeń DICOM
1.8.157.	Możliwość konfiguracji zapytania i zapisu DICOM

1.8.158.	Możliwość kontrolowania poziomu poufności plików dziennika pacjenta.

Charakterystyka modułu technika

Lp.	Charakterystyka (wymagania minimalne)
1.9.1.	Funkcja nagrywania na lokalnej nagrywarce stacji roboczej płyt CD/DVD wraz z przeglądarką DICOM uruchamiająca się automatycznie na komputerze klasy PC
1.9.2.	Możliwość nagrania pojedynczego na badania lub wielu badań na płycie CD/DVD. Możliwość załączenia opisu badania (pdf) oraz wyboru zakresu danych, w tym: całego badania, obrazów kluczowych oraz wybranych obrazów wskazanych przez użytkownika w czasie zlecania nagrywania.
1.9.3.	Możliwość oznaczania obrazów kluczowych w wykonanym badaniu, w tym: • dla lekarza radiologa (jako obrazu wymagającego zainteresowania) • do celów szkoleniowych • oznaczenie obrazu jako odrzuconego z powodu jakości wraz z podaniem przyczyny ze zdefiniowanej listy (np. artefakty kratki, pozycjonowanie, podwójna ekspozycja) • Możliwość dodania dodatkowej adnotacji dla obrazu widocznej dla innych użytkowników.
1.9.4.	Możliwość usunięcia błędnie oznaczonego obrazu kluczowego przez użytkownika, który utworzył obraz.
1.9.5.	Dostęp do pełnej historii wykonanych badań pacjenta (z tym samym ID) z możliwością wyświetlania porównawczo badań archiwalnych.
1.9.6.	"Dostęp do narzędzi manipulacji obrazami, w tym: pomiary, rekonstrukcje MPR/3D.

Integracja

Lp.	Charakterystyka (wymagania minimalne)
1.10.1.	Integracja z systemem HIS na za pośrednictwem protokołu HL7.
1.10.2.	Przyjmowanie zleceń z HIS drogą elektroniczną wraz z importem danych zlecenia i pacjenta.
1.10.3.	Wyświetlanie zarejestrowanych badań pacjentów oraz automatyczne aktualizowania danych (w przypadku ich zmiany) po stronie systemu PACS na podstawie przychodzących wiadomości HL7 z nadrzędnego systemu HIS pod warunkiem, że w przypadku ewentualnej awarii system umożliwi osobie uprawnionej naprawienie, scalenie badania, które zostanie wykonane np. bez listy roboczej ze zleconą procedurą po usunięciu awarii.
1.10.4.	Zapewnienie odwołania (anulowania) badania zarejestrowanego.
1.10.5.	Integracja zapewni możliwość automatycznego przyjmowania do realizacji zleceń z HIS.
1.10.6.	Zapewnienie przekazywania przez system do HIS informacji o statusie wykonania badania.
1.10.7.	Zapewnienie wsparcia systemu dla funkcji aktualizacji obiegu informacji – zmiana danych pacjenta w HIS musi generować zmianę w systemie PACS.
1.10.8.	Zapewnienie automatycznej aktualizacji danych pacjenta na podstawie danych przesłanych z HIS.
1.10.9.	Zapewnienie aktualizacji danych zlecenia w systemie PACS przez system HIS.
1.10.10.	Zapewnienie synchronizacji słownika lekarzy zlecających na etapie wdrożenia, który następnie będzie na bieżąco aktualizowany/uzupełniany.
1.10.11.	Zapewnienie możliwości przekazywania przez system PACS do systemu HIS informacji o statusie badania – wykonane.

1.10.12.	Każde zlecenie na badanie zaewidencjonowane w systemie (Oddział, poradnia, RIS) musi trafić na worklistę do danego aparatu włączonego do systemu PACS.
1.10.13.	System PACS ma możliwość przekazywania w lisice roboczej (worklist) do każdego zlecenia unikalnego ID badania z wykorzystaniem, którego możliwa będzie dalej identyfikacja tego badania w obydwu systemach.
1.10.14.	Po wykonaniu badania przez urządzenie jego opis następuje na stacji diagnostycznej (opisowa) z dostępem do systemu RIS i PACS. Opis badania odbywa się w systemie RIS posiadanym przez Zamawiającego. Wywołanie pola opisowego danego badania w RIS implikuje pokazanie na drugim monitorze właściwych obiektów graficznych (zdjęcie, film) stanowiących przedmiot opisu w przeglądarce systemu PACS zainstalowanej na stacji diagnostycznej posiadającej system operacyjny Windows 10/11.

Portal pacjenta

Lp.	Charakterystyka (wymagania minimalne)
1.11.1.	Portal Pacjenta tego samego producenta co system PACS oraz Przeglądarka Kliniczna. Zintegrowany z archiwum systemu PACS.
1.11.2.	Licencja otwarta bez limitu ilości użytkowników.
1.11.3.	3 grupy użytkowników: pacjent, lekarz, administrator.
1.11.4.	Możliwość skonfigurowania grup lekarzy np. lekarze z oddziału neurologii, tak aby istniała możliwość podglądu opisów i badań zleconych w ramach grupy oraz dla każdego z lekarzy osobno.
1.11.5.	Możliwość wyszukania pacjenta za pomocą min. ID z systemu nadrzędnego zintegrowanego z PACS, rodzaju badania oraz imienia, nazwiska pacjenta.
1.11.6.	Możliwość dodania własnego loga (np. logo szpitala) w portalu.
1.11.7.	Możliwość udostępnienia badania przez pacjenta lub lekarza za pomocą linku w wiadomości e-mail z określeniem czasu dostępu do badania oraz autoryzacją pinem w osobnej wiadomości e-mail. Dla bezpieczeństwa wymagane obok kodu PIN jest podanie daty urodzenia pacjenta.
1.11.8.	Możliwość udostępnienia badania przez pacjenta lub lekarza za pomocą dedykowanego kodu QR.
1.11.9.	Możliwość pobrania skompresowanej paczki zawierającej badanie obrazowe w formacie DICOM wraz z przeglądarką DICOM
1.11.10.	Współpraca z przeglądarkami web min. Edge, Chrome, Firefox, Safari w tym dostosowanie widoku do ekranu urządzenia przenośnego typu smartphone lub tablet.
1.11.11.	Możliwość skonfigurowania przez administratora min.: • Treści wiadomości e-mail. • Logowania dwuskładnikowego (2FA) użytkownika za pomocą kodu SMS (bramka SMS po stronie szpitala) lub e-mail. • Informacji powitalnej. • Zarządzania polityką haseł.
1.11.12.	Możliwość automatycznego stworzenia konta pacjenta za pomocą wiadomości HL7 (ADT / ORM / ORU) przychodzącej z systemu nadrzędnego RIS/HIS do PACS oraz możliwość ręcznego zarządzania kontami grup użytkowników przez administratora.
1.11.13.	Przeglądarka kliniczna badań w portalu pacjenta otwierająca w nowej karcie przeglądarki web wybrane badanie obrazowe wraz z obrazami i opisem (jeżeli obrazy są dostępne).
1.11.14.	Możliwość wyświetlenia i pobrania opisu badania wykonanego w systemie RIS podpisanego podpisem kwalifikowanym dzięki integracji systemów PACS i RIS.

1.11.15.	Możliwość wglądu w logi przez pacjenta z informacją min.: • Kto i kiedy otworzył badanie / opis badania. • Kto i kiedy udostępnił badanie / opis badania. • Kto i kiedy pobrał badanie / opis badania.
1.11.16.	Portal pacjenta dla grup lekarzy i pacjentów dostępny w języku polskim.
1.11.17.	Możliwość wyświetlenia wszystkich rodzajów badań obrazowych archiwizowanych w PACS min.: • Badania obrazowe z urządzeń wykorzystujących promieniowanie jonizujące • USG • MR • Badania z zakresu medycyny nuklearnej (PET, PETCT, SPECT, itp.) • Mammografia w tym badania tomosyntezy
1.11.18.	Mechanizm odpierający ataki typu brute force blokujący możliwość zalogowania użytkownika bez zmiany hasła lub czasowo blokujący dostęp po zadanie liczbie nieudanych prób zalogowania.
1.11.19.	Możliwość wyświetlenia na stronie logowania ilości prób logowania.
1.11.20.	Portal pacjenta wystawiony do Internetu za pomocą odwróconego proxy (reverse proxy) zapewnionego przez szpital.

Migracja danych

1.12.1. Cel i zakres migracji

Celem migracji jest przeniesienie wszystkich danych obrazowych oraz powiązanych metadanych z dotychczasowego systemu PACS (Impax w wersji 6.7.0.4008) do nowego systemu PACS (Target PACS) w sposób bezpieczny, zgodny z przepisami oraz minimalizujący przerwy w pracy klinicznej.

Zakres migracji obejmuje:

- obrazy medyczne w standardzie DICOM (studies, series, images),
- metadane pacjentów i badań,

1.12.2. Analiza przedmigracyjna

Przed rozpoczęciem migracji Wykonawca przeprowadzi szczegółową analizę:

- Inwentaryzację danych w źródłowym PACS (liczba badań, zakres dat, typy modalności),
- Określenia wolumenu danych i szacowanego czasu transferu,
- Weryfikacji zgodności standardów DICOM pomiędzy systemami,
- Ustalenia okien serwisowych i strategii minimalizacji przestojów.

1.12.3. Strategia migracji

Przed rozpoczęciem migracji, uwzględniając analizę z punktu 1.12.2., Wykonawca w porozumieniu z Zamawiającym wybierze jedną z poniższych strategii migracji:

- Migracja na poziomie plikowym (file-based)
- Migracja poprzez DICOM C-MOVE / C-STORE
- Migracja hybrydowa

1.12.4. Realizacja migracji – ramy czasowe

- Etap I: do dnia 31 maja 2026 roku muszą zostać zmigrowane wszystkie dane utworzone w „starym” systemie PACS od 01 stycznia 2025 roku

- Etap II: do końca trwania gwarancji (36 miesięcy) muszą zostać zmigrowane wszystkie dane utworzone w „starym” systemie PACS od 01 stycznia 2016 roku.

1.12.5. Bezpieczeństwo i zgodność z przepisami

Cały proces migracji musi być realizowany zgodnie z:

- standardem DICOM,
- zasadami bezpieczeństwa danych medycznych,
- obowiązującymi regulacjami (RODO/GDPR/ISO 27001),
- wewnętrznymi politykami bezpieczeństwa placówki.

Gwarancja, serwis, szkolenia

Lp.	Wymagania minimalne
1.13.1.	Dostarczane oprogramowanie musi być objęte 36 miesięczną asystą techniczną umożliwiającą nielimitowane wsparcie techniczne drogą mailową i systemem zdalnej pomocy w dni robocze w godzinach od 8:00 do 16:00 – bez dodatkowych opłat,
1.13.2.	Wykonawca udostępni Zamawiającemu dedykowany portal zgłoszeniowy umożliwiający śledzenie statusu każdego generowanego zgłoszenia serwisowego.
1.13.3.	Usługi gwarancyjne będą świadczone w systemie 7/24
1.13.4.	Czas reakcji na podjęcie czynności serwisowych (rozumiane jako rozpoczęcie interwencji zdalnej) - 4 h
1.13.5.	Wszystkie usterki oprogramowania nie wymagające naprawy hardware mogą być wykonywane zdalnie.
1.13.6.	Czas reakcji na podjęcie czynności serwisowych (rozumiane jako przyjazd serwisu do Zamawiającego w przypadku braku możliwości usunięcia usterki za pomocą łącza zdalnego) - następny dzień roboczy
1.13.7.	Czas na usunięcie awarii (rozumiane jako przywrócenie pierwotnej funkcjonalności) -24 h
1.13.8.	Wykonawca dostarczy Zamawiającemu komplet instrukcji w języku polskim
1.13.9.	Wykonawca przeszkoli pracowników Zamawiającego w zakresie wykorzystania systemu w poniższym zakresie: • Administratorzy systemu – 4 osoby • Lekarze radiolodzy – 7 osób • Lekarze klinicyści – 200 osób • Technicy – 20 osób
1.13.10.	Szkolenia prowadzone w systemie stacjonarnym i on-line
1.13.11.	Po zakończeniu wdrożenia Wykonawca przeprowadzi szkolenia uzupełniające w wymiarze 2 dni; zakres wdrożenia zostanie ustalony z Zamawiającym

Referencje

Zamawiający wymaga, aby Wykonawca posiadał minimum 1 referencję na dostawę systemu PACS i przeglądarki wraz z migracją danych na kwotę minimum 4 000 000PLN brutto

II.2 Dostawa systemu do monitorowania dawki promieniowania

Opis ogólny

Przedmiotem zamówienia jest zakup dostawa, instalacja, uruchomienie i szkolenie personelu dla systemu / oprogramowania do pomiaru dawki rentgenowskiej pochłanianej przez pacjenta podczas badań rentgenowskich bezpośrednio z urządzeń do obrazowania różnych producentów i przeznaczonych do wykonywania różnych rodzajów badań. wraz zapewnieniem wsparcia serwisowego. System ma umożliwiać ciągły i/lub punktowy pomiar dawki, analizę, archiwizację, raportowanie oraz ocenę efektywności i bezpieczeństwa procedur diagnostycznych.

Cel zamówienia

- Zapewnienie pomiaru dawki pochłanianej przez pacjenta w procedurach rentgenowskich (radiografia, fluoroskopia, badania kontrastowe, RTG stomatologiczne).
- Spełnienie wymogów prawnych i norm dotyczących ochrony radiologicznej pacjentów.
- Możliwość monitorowania i optymalizacji dawek w celu zmniejszenia narażenia pacjentów.
- Tworzenie dokumentacji i raportów dla potrzeb wewnętrznych i nadzorczych.

Zakres zamówienia

- System / oprogramowanie do akwizycji, analizy i raportowania danych, z możliwością eksportu (CSV, PDF, Excel).
- Instalacja, konfiguracja i testy odbiorcze w placówce Zamawiającego.
- Szkolenie użytkowników oraz przekazanie dokumentacji technicznej w języku polskim.
- Gwarancja i serwis powdrożeniowy.

Urządzenia objęte systemem

Zamawiający posiada następujące aparaty/urządzenia, które mają być objęte System z tego zadania (7 szt.):

II.4.1. Cyfrowy mobilny aparat RTG Solutions for tomorrow !M1
II.4.2. Aparat Rentgenowski Dri NRT
II.4.3. Aparat Rentgenowski Dri NRT
II.4.4. Aparat Rentgenowski Drfi NRT
II.4.5. Angiograf mobilny ZIEHM VISION RFD HE
II.4.6. Aparat mobilny RTG z ramieniem C BV VECTRA
II.4.7. Aparat mobilny RTG z ramieniem C ZIEHM VISION

Warunki minimalne dotyczące systemu

Lp.	Charakterystyka (wymagania minimalne)
2.5.1.	Automatyczne monitorowanie dawki w przypadku różnych systemów obrazowania i urządzeń różnych producentów: • Systemy tomografii komputerowej (CT) • Wstrzykiwacze/systemy wstrzykiwania środka kontrastowego • Systemy do radiologii interwencyjnej (IR) • Systemy do obrazowania sercowo-naczyniowego (CV) Systemy mammograficzne • Systemy radiograficzne

	• Systemy do radiografii podczas zabiegów operacyjnych/systemy z ruchowym ramieniem C • Systemy medycyny nuklearnej
2.5.2.	Elastyczna akwizycja danych z całej placówki
2.5.3.	Lista robocza badań zaplanowanych i wykonanych
2.5.4.	Automatyczne powiadomienia o dawce: • oprogramowanie musi zawierać system zarządzania powiadomieniami umożliwiający ostrzeganie użytkowników w przypadku, gdy dla badania lub pacjenta zostanie przekroczona wstępnie zdefiniowana wartość progowa dawki
2.5.5.	Przegląd jakości akwizycji CT
2.5.6.	Przesunięcie izocentrum: • oprogramowanie musi wyświetlać wykres przedstawiający wyśrodkowanie pacjenta i dokonywać oceny przesunięcia względem izocentrum.
2.5.7.	Modulacja wartości mA: • oprogramowanie musi wyświetlać na obrazie przeglądowym gęstość ciała pacjenta i poziom mA dla poszczególnych warstw.
2.5.8.	Szacowana wartość dawki zależna od rozmiaru (ang. Size-Specific Dose Estimate, SSDE) w tomografii komputerowej
2.5.9.	Oprogramowanie musi szacować wartość SSDE automatycznie, zgodnie z wytycznymi AAPM TG204 oraz TG220 (SSDE ekwiwalentu wody).
2.5.10.	Szacowanie dawki przyjmowanej przez narządy na podstawie 110 fantomów podczas badań
2.5.11.	Oprogramowanie musi automatycznie wykrywać skanowane obszary i obliczać dawkę przyjmowaną przez narządy podczas badań TK klatki piersiowej i jamy brzusznej u dzieci i dorosłych
2.5.12.	Szacowanie dawki promieniowania w oparciu o 50 fantomów przyjmowanej przez płód podczas badań TK
2.5.13.	Oprogramowanie musi ułatwiać fizykom medycznym tworzenie raportów dotyczących badania TK u pacjentek ciężarnych, udostępniając po badaniu szacunkową dawkę dla płodu
2.5.14.	Mapy występowania w badaniach sercowo-naczyniowych/ interwencyjnych
2.5.15.	Wskaźniki pomiaru: • oprogramowanie musi zapewniać dostęp do podsumowania danych dotyczących dawek według rodzaju sekwencji (fluoroskopia lub rejestracja) oraz wskaźników pomiarowych umożliwiających wizualizację dawki przyjętej podczas badania względem wartości progowych.
2.5.16.	Mapa występowania RPAK: • w oprogramowaniu musi być wyświetlana dwuwymiarowa mapa udziału wartości RPAK (ang. Referential Point Air Kerma, kerma w powietrzu w punkcie referencyjnym wg normy IEC 60601-2-43) według występowania. Wskazywana musi być również wartość i pozycja punktu o najwyższej skumulowanej wartości RPAK.
2.5.17.	Maksymalna dawka na powierzchnię skóry: • oprogramowanie musi automatycznie szacować maksymalną dawkę na powierzchnię skóry w przypadku zabiegów interwencyjnych przeprowadzonych z użyciem systemów zgodnych z raportami RDSR
2.5.18.	Monitorowanie danych z badań medycyny nuklearnej podaną substancję (radiofarmaceutyk plus izotop), drogę podania oraz operatora; czas badania (godzina wstrzyknięcia, godzina skanowania itp.) oszacowaną dawkę efektywną (na podstawie współczynników z publikacji ICRP 106).
2.5.19.	Dostęp do narzędzi umożliwiających analizę trendów dawki i analizę badania
2.5.20.	Podział dawki według badania/protokołu (TK) przedstawiający średnie, minimalne i maksymalne dawki dla danego opisu badania

2.5.21.	Badania z wykorzystaniem najwyższej dawki oraz dawka skumulowana pacjenta ukazujące badania, w których została zastosowana najwyższa dawka, oraz pacjentów o najwyższej dawce skumulowanej
2.5.22.	Mapa występowania RPAK: • w oprogramowaniu musi być wyświetlana dwuwymiarowa mapa udziału wartości RPAK (ang. Referential Point Air Kerma, kerma w powietrzu w punkcie referencyjnym wg normy IEC 60601-2-43) według występowania. Wskazywana musi być również wartość i pozycja punktu o najwyższej skumulowanej wartości RPAK.
2.5.23.	Maksymalna dawka na powierzchnię skóry: • Oprogramowanie musi automatycznie szacować maksymalną dawkę na powierzchnię skóry w przypadku zabiegów interwencyjnych przeprowadzonych z użyciem systemów zgodnych z raportami RDSR
2.5.24.	Monitorowanie danych z badań medycyny nuklearnej podaną substancję (radiofarmaceutyk plus izotop), drogę podania oraz operatora; czas badania (godzina wstrzyknięcia, godzina skanowania itp.) oszacowaną dawkę efektywną (na podstawie współczynników z publikacji ICRP 106).
2.5.25.	Dostęp do narzędzi umożliwiających analizę trendów dawki i analizę badania
2.5.26.	Podział dawki według badania/protokołu (TK) przedstawiający średnie, minimalne i maksymalne dawki dla danego opisu badania
2.5.27.	Oprogramowanie musi zapewniać proste narzędzie opiniowania jakości obrazu w danym badaniu — użytkownicy aplikacji mogą przyznać ocenę każdemu wykonanemu badaniu.
2.5.28.	Krajowe poziomy referencyjne - aby zapewnić zgodność z lokalnymi poziomami referencyjnymi dawki, oprogramowanie musi umożliwiać dostosowywanie poziomów DRL (ang. Diagnostic Reference Levels, diagnostyczne poziomy referencyjne) w poszczególnych krajach i w przypadku określonych urządzeń oraz konfigurować alarmy w oparciu o te poziomy; eksportowanie danych w formacie Microsoft® Excel®.
2.5.29.	Zgodność ze standardami IHE oraz rejestrami ACR
2.5.30.	Oprogramowanie musi być zgodne z opracowanym przez IHE profilami Radiation Exposure Monitoring (REM) gromadzenia informacji na temat dawek oraz ich raportowania (w celu publikowania raportów dotyczących dawek w krajowych/regionalnych rejestrach, np. ACR DIR).
2.5.31.	Tworzenie raportów: • system musi pozwalać ns korzystanie z dwóch rodzajów raportów
2.5.32.	Raporty dotyczące parametrów dawki w badaniach TK, CV/IR: • szczegółowe raporty w zakresie zarządzania dawką, które można całkowicie dostosować do upodobań placówki, obejmujące między innymi dane na temat populacji pacjentów, wykonanego obrazowania, uzasadnienie dla alarmów oraz standaryzację i optymalizację protokołów.
2.5.33.	Raport dotyczący wyzwolonych alarmów: • raport musi zawierać odsetek alarmów w odniesieniu do liczby badań, odsetek skontrolowanych alarmów, wykaz parametrów dawki promieniowania, które wyzwoliły oraz wszystkie komentarze z etapu kontroli alarmu.
2.5.34.	Raport wieloośrodkowy z badań TK i CV/IR: • podsumowanie dotyczące kluczowych wskaźników wydajności (ang. Key Productivity Indicator, KPI) placówek korzystających z tej samej instalacji oprogramowania; wskaźniki wydajności w przypadku badań CT obejmują liczbę badań, liczbę alarmów dotyczących wartości DLP oraz liczbę i odsetek alarmów; w przypadku badań CV/IR podane muszą być również stopnie gradacji w oparciu o parametry powodujące wystąpienie alarmów (czas fluoroskopii, wartość DAP lub kerma w powietrzu.
2.5.35.	Moduł zarządzania danymi dotyczącymi środka kontrastowego:

	• w oprogramowaniu musi być dostępny moduł zarządzania danymi dotyczącymi środka kontrastowego przeznaczonego do monitowania i raportowania dawek promieniowania oraz jodu z myślą o ich ograniczeniu; • moduł musi automatycznie gromadzić i scalać dane dotyczące wstrzyknięć środka kontrastowego pochodzącego ze zintegrowanych wstrzykiwaczy klasy 4 lub bezpośrednio z innych systemów wstrzykiwania systemów TK; • dane dotyczące wstrzyknięć środka kontrastowego i badań kontrastowych muszą być wyświetlane na liście roboczej badań TK; • w przypadku innych systemów obrazowania korzystających z podobnego oprogramowania z modułem zarządzania danymi dotyczącymi środka kontrastowego dane dotyczące wstrzykiwanego środka kontrastowego można będzie wprowadzić ręcznie
2.5.36.	Powiadomienia dotyczące kontekstu klinicznego i skumulowanej dawki jodu
2.5.37.	Dane dotyczące wstrzyknięć (środek kontrastowy, objętość, protokół wstrzyknięcia)
2.5.38.	Dane kliniczne
2.5.39.	Analiza środka kontrastowego
2.5.40.	Analiza objętości względem stężenia
2.5.41.	Ujednolicony rekord dawki pacjenta: • w placówkach, w których badania tego samego pacjenta wykonuje się z użyciem różnych identyfikatorów w różnych pracowniach diagnostyki obrazowej lub placówkach, oprogramowanie musi umożliwiać ujednolicenie wszystkich badań w jednym rekordzie dawki pacjenta; • warunkiem będzie przekazanie do oprogramowania powiązań między tymi identyfikatorami np. za pośrednictwem interfejsu zgodnego ze standardem IHE PIX.
2.5.42.	Dostęp do historii dawki pacjenta - przeglądanie historii dawki w rozbiciu na pacjentów, regiony anatomiczne oraz rodzaje badań RTG
2.5.43.	Integracja z katalogiem użytkownika w placówce
2.5.44.	Oprogramowanie musi obsługiwać integrację LDAP5 za pośrednictwem protokołu open LDAP lub usługi Microsoft Active Directory®, umożliwiając scentralizowane uwierzytelnianie użytkownika w oparciu o jego dane uwierzytelniające. Obsługiwane muszą być wersje 2 i 3 protokołu LDAP.
2.5.45.	Interfejs danych przychodzących i wychodzących: • oprogramowanie musi obsługiwać interfejs danych przychodzących i wychodzących dla różnych systemów informacyjnych w placówce; • interfejs danych przychodzących: ➢ musi być zgodny ze standardem HL7; ➢ umożliwiać odbieranie aktualnych danych pacjentów, scalonych danych pacjentów oraz aktualnych danych procedur obrazowania z systemu RIS, CVIS (ang. Cardiovascular Information System, system informacji kardiologicznych) lub dowolnego systemu zgodnego ze standardem HL7; • interfejs danych wychodzących musi umożliwiać wysyłanie informacji dotyczących dawki do systemów RIS, CVIS, systemów raportowania lub systemów EMR.

Wdrożenie

Lp.	Wymagania minimalne
2.6.1.	Wykonawca zobowiązany będzie dostarczyć do siedziby Zamawiającego dedykowany serwer (wersja RACK), na którym zostanie zaimplementowany System i zainstalować go w wyznaczonej przez Zamawiającego szafie RACK.

2.6.2.	Instalacja i konfiguracja oprogramowania na dostarczonym i zainstalowanym sprzęcie oraz podłączenie urządzeń wskazanych w punkcie II.2.4 do Systemu.
2.6.3.	Wykonawca musi uwzględnić koszt integracji Systemu z urządzeniami wskazanymi w punkcie II.2.4 (koszt udziału inżynierów serwisu poszczególnych urządzeń).
2.6.4.	Wykonawca zobowiązany będzie do przeprowadzenia w siedzibie Zamawiającego lub zdalnie szkolenia z obsługi oprogramowania wytypowanych pracowników Zamawiającego (5 osób) połączonego z przedstawieniem wstępnej analizy danych zebranych z urządzeń.
2.6.5.	Wszystkie prace będą realizowane przy udziale lub w konsultacji z pracownikami Zamawiającego

Kryteria odbioru

- Pozytywne wyniki testów kalibracyjnych i walidacyjnych.
- Sprawdzenie obliczeń dawek dla standardowych procedur.
- Weryfikacja raportów i archiwizacji danych.
- Dostarczenie dokumentacji i ewentualnych certyfikatów.
- Przeszkolenie użytkowników potwierdzone protokołem.

Gwarancja oraz zakres usług serwisowych

Lp.	Wymagania minimalne
2.8.1.	Dostarczane oprogramowanie musi być objęte 36 miesięczną asystą techniczną umożliwiającą nielimitowane wsparcie techniczne drogą mailową i systemem zdalnej pomocy w dni robocze w godzinach od 8:00 do 18:00 – bez dodatkowych opłat,
2.8.2.	Możliwość zgłaszania problemów technicznych drogą mailową przez 24 godziny na dobę.
2.8.3.	Czas reakcji na zgłoszenie (zdalne) - maksymalnie 24 godziny
2.8.4.	Wszystkie usterki oprogramowania nie wymagające naprawy hardware (serwera) mogą być wykonywane zdalnie.
2.8.5.	W okresie ważności asysty technicznej Wykonawca zobowiązuje się usuwać, wszelkie problemy techniczne w działaniu ww. oprogramowania, bez dodatkowych opłat,
2.8.6.	6 miesięcy po podpisaniu Protokołu zdawczo-odbiorczego Wykonawca przeprowadzi dogłębną analizę uzyskanych przez System danych i przedstawi rekomendacje dotyczące optymalizacji dawek RTG oraz usprawnienia procesu badań pacjentów.
2.8.7.	Działania z punktu II.2.8.6 Wykonawca będzie przeprowadzał cykliczne spotkania co 6 miesięcy do końca trwania gwarancji/kontraktu serwisowego
2.8.8.	W trakcie okresu gwarancji Wykonawca zapewni dostęp do bezpłatnych update`ów oraz upgrade`ów systemu.

II.3 Zakup przełączników wielowarstwowych

Opis ogólny

Przedmiotem zamówienia jest zakup dostawa, instalacja, uruchomienie 20 szt. przełączników LAN wielowarstwowych z osprzętem.

Cel zamówienia

Celem zadania jest modernizacja sieci szkieletowej szpitala w celu uzyskania pełnej segmentacji sieci komputerowej.

Zakres zamówienia

- Dostawa 20 szt. przełączników z osprzętem do siedziby Zamawiającego.
- Instalacja w ustalonym z Zamawiającym miejscu.
- Połączenie z istniejącymi elementami infrastruktury.
- Stworzenie stosu przełączników.
- Konfiguracja uzgodnionej funkcjonalności L2 (VLANy, agregacjie, UDLD/DLDP, STP).
- Konfiguracja uzgodnionej funkcjonalności L3 (adresy, bramy, DNSy, NTP, syslog).
- Konfiguracja uzgodnionych funkcjonalności bezpieczeństwa (arp protect, dhcp snooping).
- Szkolenie administratorów.
- Gwarancja i serwis.

Wymagania dotyczące sprzętu

Lp.	Parametr (wymagania minimalne)
3.4.1.	Wysokość urządzenia 1U
3.4.2.	Przełącznik wyposażony w: 3.4.2.1. minimum 48 interfejsów 10/100/1000Base-T RJ45 3.4.2.2. minimum 8 interfejsów 10GB Base-X SFP+
3.4.3.	Nieblokująca architektura o wydajności przełączania min. 256 Gbps i matrycy przełączającej z szybkością minimum 190 milionów pakietów na sekundę (Mpps)
3.4.4.	Pojemność tablicy ARP: minimum 15000 wpisów
3.4.5.	Minimum 12000 wpisów w tablicy routingu IPv4 oraz minimum 6000 wpisów w tablicy routingu IPv6
3.4.6.	Minimum 4000 wpisów multicast (S,G,V)
3.4.7.	Wbudowany port konsoli szeregowej RJ45 oraz USB/Micro-USB
3.4.8.	Możliwość łączenia do 8 urządzeń w stos z posiadanymi przełącznikami Extreme Networks 5320 , stos zarządzany z pojedynczego adresu IP, połączenie pomiędzy poszczególnymi urządzeniami musi być możliwe z przepustowością minimum 40Gbps.
3.4.9.	Wbudowany system zasilania 230VAC
3.4.10.	Obsługa sieci wirtualnych IEEE 802.1Q – min. 4000
3.4.11.	Wsparcie dla ramek Jumbo Frames (min. 9K bajtów)
3.4.12.	Obsługa Quality of Service (IEEE 802.1p, DiffServ, 8 kolejek priorytetów na każdym porcie wyjściowym)
3.4.13.	Modularny system operacyjny z ochroną pamięci, procesów oraz zasobów procesora
3.4.14.	Możliwość monitorowania zajętości CPU
3.4.15.	Pojemność tablicy adresów MAC: minimum 32 000 wpisów
3.4.16.	Możliwość przypisania minimum 1000 ACL (sumarycznie wejściowe i wyjściowe)

3.4.17.	Obsługa routingu IPv4/IPv6 minimum w zakresie tras statycznych oraz protokołów RIP i OSPF
3.4.18.	Obsługa protokołów IS-IS, BGP4, MBGP - jeżeli funkcjonalność ta wymaga dodatkowej licencji Zamawiający nie wymaga jej dostarczenia w ramach tego postępowania
3.4.19.	Policy Based Routing dla IPv4 oraz IPv6
3.4.20.	Obsługa MLDv1 oraz MLDv2, filtrowanie IGMP, obsługa MVR (Multicast VLAN Registration)
3.4.21.	Obsługa IGMP v1v2/v3 oraz IGMP v1/v2/v3 snooping
3.4.22.	Obsługa protokołu PIM-SM
3.4.23.	Obsługa protokołów PIM DM oraz PIM SSM - jeżeli funkcjonalność ta wymaga dodatkowej licencji Zamawiający nie wymaga jej dostarczenia w ramach tego postępowania
3.4.24.	Obsługa uwierzytelniania do sieci z wykorzystaniem: 3.4.24.1. protokołu IEEE 802.1x 3.4.24.2. formularza www 3.4.24.3. adresu MAC
3.4.25.	Funkcjonalność elastycznego uwierzytelniania z możliwością wyboru kolejności stosowanych mechanizmów – 802.1X/uwierzytelnianie w oparciu o MAC adres/uwierzytelnianie w oparciu o portal www)
3.4.26.	Obsługa wielu sesji uwierzytelniania (min. 12) na jednym porcie (multiple supplicants)
3.4.27.	Możliwość integracji funkcjonalności uwierzytelniania z systemem klasy NAC (Network Access Control) oraz obsługa funkcjonalności CoA pozwalającej na wymuszenie reautentykacji dołączonego klienta z poziomu systemu NAC
3.4.28.	Przydział sieci VLAN, ACL/QoS podczas autentykacji
3.4.29.	Urządzenie musi wspierać profile bezpieczeństwa definiowane per użytkownik. Profil bezpieczeństwa oznacza połączenie: 3.4.29.1. definicji sieci VLAN, 3.4.29.2. reguły filtrowania w warstwach L2-L4 dla IPv4 i IPv6, 3.4.29.3. realizację zasad jakości usług w warstwach L2-L4 dla IPv4 i IPv6, 3.4.29.4. realizację zasad ograniczania prędkości dla IPv4 i IPv6 w warstwach L2-L4.
3.4.30.	Obsługa TACACS+ (RFC 1492), RADIUS Authentication (RFC 2865) i Accounting (RFC 2866) wraz z funkcjonalnością *per-command authentication*
3.4.31.	Bezpieczeństwo adresów MAC: 3.4.31.1. ograniczenie liczby MAC adresów na porcie 3.4.31.2. zatrzaśnięcie MAC adresu na porcie 3.4.31.3. możliwość wpisania statycznych MAC adresów na port/vlan 3.4.31.4. możliwość wyłączenia uczenia MAC adresów
3.4.32.	Zabezpieczenie przełącznika przed atakami DoS 3.4.32.1. Networks Ingress Filtering RFC 2267 3.4.32.2. SYN Attack Protection Zabezpieczenie CPU przełącznika poprzez ograniczenie ruchu do systemu zarządzania
3.4.33.	Dwukierunkowe (ingress/egress) listy kontroli dostępu ACL pracujące na warstwie 2, 3 i 4 (ACL realizowane w sprzęcie bez zmniejszenia wydajności przełącznika)
3.4.34.	Obsługa Trusted DHCP Server, DHCP Snooping, DHCP Secured ARP/ARP Validation
3.4.35.	Obsługa Gratuitous ARP Protection, Source IP Lockdown oraz IP Source Guard
3.4.36.	Obsługa redundancji routingu VRRP (RFC 2338) i VRRPv2 (RFC 3768)

3.4.37.	Wsparcie dla technologii Ethernet VPN (EVPN) oraz tunelowania GRE - jeżeli funkcjonalność ta wymaga dodatkowej licencji Zamawiający nie wymaga jej dostarczenia w ramach tego postępowania
3.4.38.	Obsługa protokołów drzewa rozpinającego (spanning Tree) w zakresie STP, RSTP, MSTP, PVST+
3.4.39.	Obsługa protokołu MVRP
3.4.40.	Obsługa protokołu EAPS (RFC 3619), ERPS (ITU G.8032) lub równoważnego
3.4.41.	Obsługa Link Aggregation IEEE 802.3ad wraz z mechanizmem LACP
3.4.42.	Obsługa IEEE 802.3ah Ethernet OAM
3.4.43.	Obsługa mechanizmu MC-LAG/VSS/MLAG/IRF lub równoważnego umożliwiającego agregację połączeń do dwóch niezależnych przełączników. Urządzenia dołączające się do pary przełączników muszą widzeń je jako pojedyncze urządzenie z punktu widzenia warstwy L2. Nie dopuszcza się stosowania mechanizmów łączenia w stos jako równoważnych.
3.4.44.	Zarządzany za pomocą SSH/Telnet, SNMP v1/v2/v3, oraz systemu zarządzania dostarczonego przez producenta
3.4.45.	Obsługa SYSLOG z możliwością definiowania wielu serwerów
3.4.46.	Sprzętowa obsługa sFlow lub protokołu równoważnego
3.4.47.	Obsługa RMON (RFC 1757) i RMON2 (RFC 2021)
3.4.48.	Obsługa skryptów CLI (możliwość edycji skryptów i ACL bezpośrednio na urządzeniu - system operacyjny musi zawierać edytor plików tekstowych)
3.4.49.	Możliwość uruchamiania skryptów: 3.4.49.1. Ręcznie 3.4.49.2. o określonym czasie lub co wskazany okres czasu 3.4.49.3. na podstawie wpisów w logu systemowym
3.4.50.	Obsługa XML API poprzez Telnet/SSH i HTTP/HTTPS
3.4.51.	Obsługa protokołu MACSEC (IEEE 802.1AE) na wszystkich portach urządzenia (zarówno porty miedziane jak i światłowodowe) – jeżeli funkcjonalność ta wymaga dodatkowych modułów lub licencji Zamawiający nie wymaga ich dostarczenia w ramach tego postępowania
3.4.52.	3.4.52.1. Usługi wirtualizacji warstwy L2 i L3 (Fabric Network) 3.4.52.2. Przełącznik musi udostępniać możliwość wirtualizacji usług sieciowych w warstwie L2 i L3 modelu OSI. 3.4.52.3. Przełącznik musi zapewniać „multi-tennancy” dla usług sieciowych zarówno w L2 jak i L3. Rozumiemy przez to przypadek, w którym do przełącznika doprowadzone są nakładające się numery VLAN (vlan overlap) lub podsieci IP (subnet overlap). W takim przypadku przełącznik musi zapewniać izolację tego ruchu od siebie. 3.4.52.4. Przełącznik musi zapewniać usługi zwirtualizowane L2 i L3 w oparciu o standardowe protokoły sieciowe (SPB 802.1aq lub EVPN) 3.4.52.5. Przełącznik musi umożliwiać skonfigurowanie usług wirtualizacji w L2 3.4.52.6. Przełącznik musi umożliwiać obsługę usług multicast dla L2 jak i L3 bez konieczności używania protokołu PIM.

	3.4.52.7. Przełącznik musi zapewniać możliwość zastosowania dowolnej topologii połączeń przy współpracy z innymi urządzeniami tworzącymi węzły sieci szkieletowej. 3.4.52.8. Przełącznik musi zapewniać możliwość dokładania nowych węzłów w sieci bez wpływu na już działające usługi sieciowe.
3.4.53.	Dożywotnia gwarancja producenta (rozumiana co najmniej jako data zakończenia sprzedaży (EOS) + dodatkowe 5 lat) uwzględniająca: 3.4.53.1. wymianę uszkodzonego urządzenia z wysyłką następnego dnia roboczego, 3.4.53.2. aktualizacje oprogramowania układowego (firmware), 3.4.53.3. dostęp do bazy wiedzy oraz dokumentacji technicznej producenta.
3.4.54.	Wraz z przełącznikami należy dostarczy kompatybilne: • 20 szt. moduł optyczny SFP+ SR 10Gbp 850nm LC SMF • 30 szt. moduł optyczny SFP+ SR 10Gbp 850nm LC MMF • 1 szt. przełącznica światłowodowa Rack 19" 1U PLC 1x32 SC/APC • 7 szt. przełącznica światłowodowa Rack 19" 1U 12xSC • 10 szt. patchcord SC/APC-LC/UPC, SM - 1m • 10 szt. patchcord SC/APC-LC/UPC, SM - 2m • 20 szt. patchcord LC/UPC-LC/UPC, MM, 50/125 – 3m • 20 szt. patchcord LC/UPC-LC/UPC, MM, 50/125 – 10m • 12 szt. przewód do łączenie przełączników w stos typu DAC 10GB SFP+ o długości 1m • 3 szt. przewód do łączenia przełączników w stos typu DAC 10GB SFP+ o długości 3m

II.4 Wsparcie serwisowe radiologicznego systemu informatycznego RIS

II.4.1. Stan obecny

Zamawiający posiada i użytkuje Radiologiczny System Informatyczny RIS Vizo firmy TMS-Soft.
System ten jest zintegrowany z systemami informatycznym pracującymi w szpitalu:

- głęboka integracja z HIS AMMS firmy ASSECO POLSKA S.A.
- integracja HL7 CDA z EDM firmy ASSECO POLSKA S.A.
- integracja HL7 z PACS firmy AGFA HealthCare
- integracja ze stacjami diagnostycznymi Impax firmy Agfa i VIZO+ firmy SoftMed
- integracja HL7 z Teleradiologią

Lp.	Element Systemu	Liczba użytkowanych elementów
4.1.1.	Moduł Bazowy (Pracownie: RTG/ Tomografii Komputerowej / USG)	--1--
4.1.2.	Moduł integracji HL7 z HIS	--1--
4.1.3.	Moduł integracji HL7 CDA z EDM	--1--
4.1.4.	Moduł integracji HL7 z PACS	--1--
4.1.5.	Moduł integracji HL7 z zewnętrznym systemem Teleradiologii	--1--

4.1.6.	Moduł raportowy	--1--
4.1.7.	Moduł weryfikacji eWUS	--1--
4.1.8.	Licencje stanowiskowe	--14--

II.4.2. Ogólny opis

Przedmiotem zamówienia jest przedłużenie wsparcia serwisowego Radiologicznego Systemu Informatycznego RIS wykorzystywanego przez Zamawiającego na okres 36 miesięcy

II.4.3. Zakres usług serwisowych

II.4.3.1. Zakres usług podstawowych wykonywanych przez Wykonawcę

Lp.	Wymagania minimalne
4.3.1.19.	Udostępnianie poprawek do Oprogramowania Aplikacyjnego , w przypadku stwierdzenia przez Zamawiającego błędu Oprogramowania Aplikacyjnego (tzn. nie spowodowanego przez Zamawiającego powtarzalnego działania Oprogramowania Aplikacyjnego, w tym samym miejscu programu, prowadzącego w każdym przypadku do otrzymania błędnych wyników jego działania)
4.3.1.20.	Udostępnianie bieżących aktualizacji wersji aplikacji w przypadku pojawienia się poprawek dla funkcjonalności zakupionych i wykorzystywanych przez Zamawiającego.
4.3.1.21.	Aktualizowanie bazy danych do najnowszej obsługiwanej przez system RIS
4.3.1.22.	Dostosowywanie aplikacji do obowiązujących norm prawnych zgodnie ze zmieniającymi się przepisami ogólnymi, rozporządzeniami, ustawami, obowiązującymi wykładniami prawnymi lub wskazówkami jednostek nadrzędnych (np. Narodowy Fundusz Zdrowia, Ministerstwo Zdrowia, Samorządowy Wydział Zdrowia, inne), w tym na bieżąco dostosowywanie aplikacji do rozliczeń z NFZ w ramach funkcjonalności zakupionych i wykorzystywanych przez Użytkownika
4.3.1.23.	Przyjmowanie i rozpatrywanie w czasie prac analitycznych przy rozwoju oprogramowania pisemnych zgłoszeń, uwag oraz propozycji Zamawiającego dotyczących modyfikacji Oprogramowania Aplikacyjnego.
4.3.1.24.	Udzielanie zdalnego wsparcia dla administratora i użytkownika kluczowego, bezpośrednich konsultacji telefonicznych w zakresie: czynności operatorskich, diagnostyki problemów, konfiguracji, analizy danych
4.3.1.25.	Przeprowadzenie bezpłatnych szkoleń administratorów i użytkownika kluczowego w przypadku zmian w aplikacji.
4.3.1.26.	Analiza potrzeb i przekazywanie Zamawiającemu zaleceń w zakresie modernizacji, ewentualnie wymiany sprzętu komputerowego niezbędnego do prawidłowego funkcjonowania systemu
4.3.1.27.	Instalowanie i wdrażanie poprawek aplikacji wynikających ze zgłoszeń błędów w ramach usługi serwisu
4.3.1.28.	Wykonywanie ponownych zdalnych instalacji Oprogramowania Bazodanowego w przypadkach modyfikacji infrastruktury informatycznej Użytkownika.
4.3.1.29.	Udzielanie, na wniosek Zamawiającego, zdalnej pomocy w awaryjnym odtwarzaniu Oprogramowania Bazodanowego, stanu Oprogramowania Aplikacyjnego i zgromadzonych danych archiwalnych.

4.3.1.30.	Usuwanie awarii Oprogramowania Aplikacyjnego powstałych z winy Użytkownika lub wskutek zdarzeń losowych niezależnych od żadnej ze Stron
4.3.1.31.	Utrzymanie integracji po stronie RIS z: HIS/EDM Asseco, PACS AGFA, systemem Teleradiologii, stacjami diagnostycznymi Impax-Agfa oraz VIZO+ Softmed,

II.4.3.2. Zakres usług pozostałych wykonywanych przez Wykonawcę:

Lp.	Wymagania minimalne
4.3.2.1.	Niezbędne reinstalacje serwera. W przypadku maszyn fizycznych reinstalacje będą wykonywane w siedzibie Zamawiającego lub w miarę możliwości zdalnie.
4.3.2.2.	Analizy, diagnozowanie przyczyn i lokalizacja awarii Systemu, wyjaśnianie zgłoszeń i wsparcie Zamawiającego w zakresie interpretacji funkcjonalności, zmian konfiguracji, organizacji pracy i działania Systemu
4.3.2.3.	Możliwość konfiguracji wykonywania kopii bezpieczeństwa bazy danych Systemu na zasobie udostępnionym przez Zamawiającego w tym zakresie.
4.3.2.4.	Konfiguracje aplikacji na stacjach roboczych w przypadku konieczności ich wymiany, naprawy lub po reinstalacji systemu operacyjnego.

II.4.3.3. Warunki prowadzenia prac serwisowych:

Lp.	Wymagania minimalne
4.3.3.1.	Przygotowanie i instalacja oprogramowania serwerów oraz stanowisk klienckich odbywa się w siedzibie Zamawiającego.
4.3.3.2.	Kontakty Zamawiającego z Wykonawcą dokonywane są wyłącznie za pośrednictwem wyznaczonego przez Zamawiającego Administratora Systemu lub Użytkownika Kluczowego. W wyjątkowych wypadkach (w przypadku zgłoszenia awarii krytycznej), dopuszcza się kontakt innej osoby.
4.3.3.3.	Zamawiający, korzystając z Systemu, zobowiązany jest do przestrzegania zasad zawartych w przekazanych instrukcjach, wskazówkach eksploatacyjnych, zaleceniach i warunkach prowadzenia serwisu.
4.3.3.4.	W przypadku tzw. **błędu krytycznego**, tj. takiego, który uniemożliwia użytkowanie Oprogramowania Aplikacyjnego w zakresie jego podstawowej funkcjonalności (wskazanej w dokumentacji użytkownika), a w szczególności nieprawidłowe działanie Oprogramowania Aplikacyjnego, które prowadzi do zatrzymania jego eksploatacji, utraty danych lub naruszenia ich spójności w wyniku której, niemożliwe jest prowadzenie działalności z użyciem Oprogramowania Aplikacyjnego: • czas reakcji Wykonawcy na zgłoszenie Zamawiającego (tj. czas od przyjęcia zgłoszenia do chwili podjęcia przez Wykonawcę czynności zmierzających do naprawy zgłoszonego "błędu krytycznego") wynosi 24 godziny, • czas dokonania i udostępnienia Zamawiającemu/Użytkownikowi odpowiednich korekt Oprogramowania Aplikacyjnego wynosi do 3 dni roboczych, od chwili przyjęcia zgłoszenia

4.3.3.5.	W przypadku tzw. **błędu zwykłego** (nie krytyczne): • czas reakcji Wykonawcy na zgłoszenie Zamawiającego (tj. czas od przyjęcia zgłoszenia do chwili podjęcia przez Wykonawcę czynności zmierzających do naprawy zgłoszonego błędu zwykłego) wynosi do 15dni roboczych; • czas dokonania i udostępnienia Zamawiającemu/Użytkownikowi odpowiednich korekt Oprogramowania Aplikacyjnego wynosi do 30 dni roboczych od chwili przyjęcia zgłoszenia
4.3.3.6.	W przypadku wystąpienia "błędu krytycznego" Wykonawca może wprowadzić tzw. rozwiązanie tymczasowe, doraźnie rozwiązujące problem błędu krytycznego, w takim przypadku dalsza obsługa usunięcia dotychczasowego błędu krytycznego będzie traktowana jako błąd zwykły. W wyjątkowych wypadkach, za zgodą Zamawiającego, czas dokonania korekt będzie uzgodniony pomiędzy Wykonawcą i Zamawiającym.
4.3.3.7.	Przyjmowanie zgłoszeń przez Wykonawcę. Zgłoszenie traktowane jest jako przyjęte: • w dni robocze do godziny 17:00 - danego dnia roboczego; • w dni robocze po godzinie 17:00 - następnego dnia roboczego; • w dniu ustawowo lub dodatkowo wolnym od pracy - o godz. 9:00 - najbliższego dnia roboczego.
4.3.3.8.	Zgłoszenia błędów przez Zamawiającego odbywać się będą za pomocą poczty elektronicznej oraz/lub na wskazany numer telefonu wsparcia bezpośredniego
4.3.3.9.	Usługi serwisowe, z wyjątkiem usług związanych z usuwaniem awarii i ich bezpośrednich skutków, konsultacji, analiz wykonywane są w dni robocze w godzinach 09:00 – 17:00 Realizacja prac planowych poza wskazanymi godzinami wymaga oddzielnych ustaleń.
4.3.3.10.	Po okresie wdrożenia Systemu administratorem danych jest Zamawiający, W ramach usługi serwisu pogwarancyjnego Wykonawca nie wykonuje żadnych prac związanych z bieżącą działalnością administracyjną systemu (modyfikacje danych w bazie, dodawanie nowych danych do bazy danych)
4.3.3.11.	Wszelkie ingerencje Wykonawcy w dane administrowane przez Zamawiającego, niezależnie od warunków takich ingerencji, wymagają pisemnego (np. e-mail) zlecenia uprawnionego przedstawiciela Zamawiającego. Wyjątkiem jest ingerencja związana z usunięciem awarii, dla której podstawą jest zgłoszenie awarii, jednak i w tym przypadku pracownik serwisu realizujący zgłoszenie serwisowe może zażądać pisemnej dyspozycji.
4.3.3.12.	Aktualizacje Systemu wykonywane są przez Wykonawcę, z powiadomieniem Zamawiającego w uzgodnionych wspólnie terminach.
4.3.3.13.	Zamawiający dopuszcza prawo do przerwy w pracy Systemu dwa razy w roku na niezbędny czas, w terminie uzgodnionym z Zamawiającym, w celu przeprowadzenia prac konserwacyjno-aktualizacyjnych.
4.3.3.14.	Usługi serwisowe realizowane są w sposób zdalny, z wykorzystaniem udostępnionego przez Zamawiającego łącza serwisowego. Połączenie jest realizowane przez szyfrowany tunel pakietu OpenVPN. Serwer VPN znajduje się w siedzibie Zamawiającego, a na serwerze Zamawiającego zainstalowany będzie klient usługi. Zamawiający na potrzeby utrzymania tunelu serwisowego zapewni Wykonawcy łącze internetowe o odpowiedniej przepustowości oraz wspólnie uzgodnione adresy i porty

4.3.3.15.	W przypadku zgłoszeń z zakresu komunikacji aplikacji RIS z systemami zewnętrznymi (HIS, PACS, aparaty diagnostyczne) Wykonawca nie ponosi odpowiedzialności za czas reakcji/naprawy - po stronie systemów zewnętrznych, a koszty ewentualnego wsparcia lub działań ich serwisu pokrywa Zamawiający
4.3.3.16.	Wykonawca nie odpowiada za niewykonanie, częściowe wykonanie oraz opóźnienie w wykonaniu usługi serwisu pogwarancyjnego nie powstałe z jego winy a spowodowane błędnym działaniem sieci komputerowej lub sprzętu komputerowego pracującego u Zamawiającego
4.3.3.17.	Zamawiający jest zobowiązany do udzielenia Wykonawcy pomocy w wykonaniu czynności serwisowych w formie udziału oddelegowanych do tego celu pracowników Zamawiającego, w tym administratora Systemu i/lub pracowników odpowiednich służb technicznych.
4.3.3.18.	Interwencje serwisowe w warunkach braku zdalnego dostępu do Systemu, jak również braku możliwości dostępu (do danych lub sprzętu), w przypadku, gdy jest on niezbędny do usunięcia awarii, zwalnia Wykonawcę z dotrzymania terminu jej usunięcia i obliguje Zamawiającego do zwrotu kosztów ewentualnego dojazdu serwisowego.
4.3.3.19.	Wykonawca nie odpowiada za nie wykonanie, częściowe wykonanie oraz opóźnienie w wykonaniu usługi serwisu pogwarancyjnego nie powstałe z jego winy a spowodowane siła wyższą oraz skutkami tejże siły wyższej.
4.3.3.20.	Zamawiający odpowiada za poprawność działania sieci komputerowej oraz sprzętu komputerowego na którym lub w obszarze, którego działa system RIS

II.4.4. Rozwiązanie równoważne

Zamawiający dopuszcza wymianę obecnie wykorzystywanego Radiologicznego Systemu Informatycznego RIS na rozwiązanie równoważne, które zachowa wszystkie funkcjonalności i integracje obecnie wykorzystywanego systemu z okresem wsparcia serwisowego, które jest przedmiotem tego postępowania. Oferent na własny koszt zapewni sobie wsparcie, dostawy niezbędnych licencji i wykonanie prac integracyjnych oraz podłączeniowych po stronie HIS/EDM Asseco, PACS Agfa, stacji diagnostycznych SoftMed, stacji diagnostycznych Impax-Agfa oraz Teleradiologii.

Wymagania minimalne dla Radiologicznego Systemu Informatycznego (RIS):

Lp.	Wymagania funkcjonalne
Właściwości systemu	
4.4.1.	Polski interfejs użytkownika w aplikacjach
4.4.2.	Baza danych SQL, relacyjna, transakcyjna, darmowa lub płatna z zagwarantowaną 10letnią aktualizacją bez ponoszenia dodatkowych kosztów
4.4.3.	System uruchamiany na stacjach klienckich w przeglądarce WEB lub jako aplikacja portable (bez konieczności instalowania na komputerach klienckich)
4.4.4.	System posiada wspólny dla wszystkich użytkowników moduł rejestracji pacjentów
4.4.5.	Możliwość tworzenia w systemie, struktury zakładu na zasadzie definiowania dowolnej liczby pracowni z przypisanymi do nich dowolnej liczby aparatów diagnostycznych.

4.4.6.	Walidacja poprawności wpisu numeru PESEL wraz z kontrolą wprowadzania danych uniemożliwiająca dwukrotne wprowadzenie do systemu pacjenta z tym samym numerem PESEL, za wyjątkiem pacjenta z zerowym numerem PESEL
4.4.7.	Możliwość rejestracji wymaganych danych osobowych pacjentów
4.4.8.	Szybki dostęp do pełnej historii wizyt pacjenta
4.4.9.	Możliwość wyszukiwania pacjentów w bazie – min 12 kryteriów z dowolnego przedziału czasowego wybranego przez użytkownika w tym: według pracowni , rodzaju badania, jednostek zlecających, lekarzy opisujących, zlecających
4.4.10.	Definiowanie harmonogramu pracy poszczególnych pracowni / gabinetów diagnostycznych z uwzględnieniem dni świątecznych, przerw serwisowych.
4.4.11.	Podczas umawiania badania – szybkie wyszukiwanie pacjenta poprzez jedno uniwersalne okno do wpisywania nazwiska / numeru PESEL
4.4.12.	Możliwość umawiania badań na wyznaczone godziny według harmonogramu a także z jego pominięciem
4.4.13.	Możliwość wstępnej rezerwacji terminu badania, ustalanie stałych pasm w harmonogramach dla poszczególnych zleceniodawców i serwisów
4.4.14.	Wyświetlanie harmonogramów z rozróżnieniem terminów wstępnie zarezerwowanych i terminów z badaniami zarejestrowanymi
4.4.15.	Możliwość zmiany umówionego wcześniej terminu lub anulowania wizyty
4.4.16.	Możliwość rejestrowania dla danego pacjenta kilku procedur jednocześnie
4.4.17.	Szybkie „dorejestrowywanie” kolejnych badań poprzez wykorzystanie danych pacjenta wskazanego w harmonogramie
4.4.18.	Obsługa przez system e-skierowań (P1). Możliwość wykorzystania danych z e-skierowań podczas umawiania zlecenia.
4.4.19.	Możliwość dołączania do rejestrowanego badania: - skanów skierowań i innych dokumentów - dokumentów PDF z dysku twardego
4.4.20.	Obsługa drukarek i czytników kodów kreskowych – pozwalająca na etykietowanie papierowych skierowań i szybkiego wyszukiwania zarejestrowanego badania na liście roboczej lekarza opisującego
4.4.21.	Program RIS pozwala na łączenie badań w zestawy badań dzięki czemu kilka badań jednego pacjenta jest widoczne jako zestaw na każdym etapie
4.4.22.	Możliwość zapisywania w słownikach danych zleceniodawców wraz z wyszukiwaniem jednostki zlecającej na podstawie numeru umowy z NFZ, NIP-u, Regonu
4.4.23.	Możliwość zapisywania w słownikach lekarzy kierujących wraz z walidacją poprawności numerów praw wykonywania zawodu i zabezpieczeniem przed powtórnym wprowadzeniem do słownika lekarza o tym samym numerze
4.4.24.	Możliwość podziału zleceniodawców na dowolne grupy (aby np. w ramach danej grupy tworzyć statystyki)
4.4.25.	Możliwość wydruku potwierdzenia umówienia wizyty, wraz z dowolnym tekstem np. instrukcja przygotowania się do badania. Szablony potwierdzeń przypisywane do konkretnego aparatu
4.4.26.	Możliwość podglądu i wydruku listy pacjentów umówionych do danego gabinetu

4.4.27.	Generowanie skróconego ID pacjenta na potrzeby jego identyfikacji podczas badań , widoczny w systemie na każdym etapie badania – rejestracja, realizacja, opisywanie
4.4.28.	Możliwość potwierdzenia w systemie przybycia pacjenta na badanie (dla wcześniej rejestrowanych pacjentów) z możliwością filtracji listy
4.4.29.	Integracja z systemem eWUŚ – automatyczne pobieranie informacji o ubezpieczeniu pacjenta, podczas procesu rejestracji badania.
4.4.30.	W przypadku negatywnej weryfikacji eWUŚ – możliwość wpisania do systemu danych oświadczenia pacjenta
4.4.31.	Wymuszanie przez program konieczności wprowadzenia danych lekarza kierującego (nazwisko, imię, numer prawa wyk. zawodu)
4.4.32.	Możliwość cofnięcia statusu badania przez uprawnionego użytkownika – np. z badania do opisu na badanie do wykonania.
4.4.33.	Możliwość wprowadzania wielkości dawki/ danych ekspozycji
4.4.34.	Rejestrowanie ilości zużytych materiałów eksploatacyjnych
4.4.35.	Automatyczne przesyłanie danych pacjenta i zleceń badań poprzez HL7 do systemu PACS (AGFA) na potrzeby wygenerowania list roboczych do aparatów diagnostycznych (DICOM WorkList)
4.4.36.	Automatyczne pobieranie informacji o zakończeniu badania przez aparat diagnostyczny – odbiór komunikatów HL7 z systemu PACS na podstawie którego system zmienia status badania (informacja dla lekarza że badanie jest wykonane i czeka na opis)
4.4.37.	Możliwość przydzielenia wykonania opisu do danego radiologa – radiolog po zalogowaniu się do systemu widzi tylko badania które zostały mu przydzielone do opisu. Możliwość konfiguracji systemu w taki sposób aby radiolog widział również badania do których nikogo nie przydzielono.
4.4.38.	Możliwość przypisywania priorytetów opisów, które są widoczne dla lekarza na jego liście roboczej
4.4.39.	Funkcja przeglądania przez lekarza podczas opisywania dołączonych do zlecenia przez rejestrację dodatkowych dokumentów
4.4.40.	Zapewnienie indywidualnych wzorców opisów widocznych tylko dla określonego użytkownika wraz z możliwością ich zarządzania w tym dodawanie , edycja i modyfikacja , oraz zapewnienie wzorców ogólnie dostępnych, modyfikowanych tylko przez uprawnionych użytkowników
4.4.41.	Automatyczna preselekcja wzorców opisów do danego rodzaju badań
4.4.42.	Szybki dostęp do wszystkich wyników wcześniejszych badań diagnostycznych pacjenta z możliwością bezpośredniego kopiowania wcześniejszych opisów do bieżącego wyniku
4.4.43.	Monitorowanie wszelkich modyfikacji opisów badań z zaznaczeniem kto, kiedy i jakich zmian w opisie dokonał
4.4.44.	Możliwość przypisania jednego opisu kilku badaniom tego samego pacjenta w trakcie jednoczesnego opisywania
4.4.45.	Możliwość jednoczesnego opisywania i przeglądania wcześniejszych wyników w jednym oknie
4.4.46.	Możliwość przerwania opisu i pozostawienia badania do konsultacji z nadanym specjalnym statusem w celu szybkiego późniejszego odnalezienia w systemie

4.4.47.	Możliwość współpracy pomiędzy programem RIS a lekarską stacją diagnostyczną (Impax-Agfa, Vizo-Softmed) działającymi jednocześnie na opisowej stacji lekarskiej. Współpraca polegająca na automatycznym otwarciu obrazów w programie diagnostycznym przy otwarciu opisu w RIS
4.4.48.	Skalowanie powiększenia okna opisowego – umożliwiające powiększenie wprowadzanego tekstu dla ułatwienia pracy/czytelności radiologowi.
4.4.49.	Możliwość wprowadzania opisów przez sekretarki lub stażystów z opcją ich późniejszego zatwierdzania przez uprawnionych lekarzy
4.4.50.	Możliwość wydruku opisu wraz z podstawowymi danymi dotyczącymi pacjenta, zlecenia, nazwą aparatu, datą, identyfikacją lekarza opisującego
4.4.51.	Możliwość jednoczesnego – „hurtowego" wydruku opisów dowolnej liczby badań np. z danego okresu lub określonego gabinetu, bez konieczności otwierania poszczególnych kart badań
4.4.52.	Funkcja automatycznego wydruku na wskazanej drukarce po zatwierdzeniu/podpisaniu elektronicznym przez lekarza (bez dodatkowego klikania)
4.4.53.	Konfiguracja wydruków, pozwalającym na zamieszczanie logo, definiowanie pogrubień, znaków specjalnych, wstawianie automatycznie uzupełnianych pól takich jak nazwy urządzeń, nazwy pracowni itp.)
4.4.54.	Możliwość formatowania wprowadzanego tekstu – w tym minimum: - zmiana czcionki (rodzaj, pogrubienie, kursywa, podkreślenie, wielkość) - punktowanie/numerowanie
4.4.55.	Sprawdzanie przez program pisowni wprowadzonego wyniku badania, z możliwością dodania występującego wyrażenia do słownika
4.4.56.	Zabezpieczenie informujące o lekarza o próbie edycji otwartego na innym stanowisku wyniku badania – z informacją kto i na którym stanowisku edytuje ten sam wynik
4.4.57.	Możliwość przywołania treści ostatnio wprowadzanego tekstu opisu pozwalające na odzyskanie wyniku w razie przypadkowego wylogowania, anulowania, awarii sieci komputerowej itp. lub „cofnięcia się" do wcześniejszej wersji wprowadzanego tekstu
4.4.58.	Wydruki z wykorzystaniem opcji duplex
4.4.59.	Możliwość podpisywania elektronicznego podczas zatwierdzania opisów przez lekarza (minimum podpis ZUS)
4.4.60.	Zatwierdzone przez lekarza opisy badań, dostępne w formie podpisanego elektronicznie PDF
4.4.61.	System odnotowuje wydawanie wyników pacjentów (kto, kiedy i w jakiej formie odebrał wynik: papierowy-oryginał, papierowy-kopia, CD/DVD itp.)
4.4.62.	Generowanie statystyk za dowolny okres: badań wykonanych z podziałem na poszczególnych zleceniodawców
4.4.63.	Zestawienie ilości zleceń z podziałem na poszczególne pracownie i aparaty diagnostyczne
4.4.64.	Generowanie statystyk pracy personelu (liczby opisanych, zrealizowanych badań przez poszczególnych pracowników)
4.4.65.	Możliwość zapisu danych osoby odbierającej wynik badania (nazwisko, imię, nr dowodu osobistego lub prawa jazdy)
4.4.66.	Zabezpieczenie przed usunięciem badań lub danych pacjenta przez osoby nieuprawnione

4.4.67.	Możliwość przydzielania uprawnień dostępu do poszczególnych funkcji programu dla poszczególnych grup użytkowników
4.4.68.	Możliwość przydzielania uprawnień dostępu do danych osobowych pacjentów w programie dla poszczególnych grup użytkowników
4.4.69.	Możliwość tworzenia i przydzielania różnych cenników badań poszczególnym zleceniodawcom wraz z czasem ich obowiązywania
4.4.70.	Instrukcje obsługi w języku polskim w formie elektronicznej – przy dostawie
4.4.71.	Zgoda na przeprowadzenie prezentacji oprogramowania z wszystkimi funkcjami wymienionymi w SIWZ dokonana u Zamawiającego
4.4.72.	Logi zdarzeń zachodzących w systemie dostępne dla administratora systemu
4.4.73.	Zamawiającemu zostaną przekazane wszystkie niezbędne hasła/kody umożliwiające pełny dostęp administracyjny do systemu operacyjnego, systemu RIS.
4.4.74.	Uruchomienie systemu minimum na 14 wskazanych przez Zamawiającego stanowiskach
INTEGRACJA HL7 Z PACS	
4.4.75.	Zintegrowanie dostarczonego rozwiązania informatycznego z systemem PACS poprzez protokół HL7 spełniający poniższe wymagania: • Automatyczne udostępnianie opisów badań programom archiwizującym obrazy • Automatyczne udostępnianie opisów badań w programach typu WEB dystrybuujących obrazy poza zakład radiologii • Automatyczne przesłanie do PACS danych zlecenia odebranych przez RIS z systemu HIS AMMS • Uaktualnienia w obiegu danych: Pacjent-Opisy-Badanie, min. zmiana imienia i nazwiska pacjenta, rodzaju badania oraz opisu w systemie RIS powoduje automatycznie wysłane informacji do PACS w celu aktualizacji danych. • Automatyczna realizacja badania przez system RIS (zmiana statusu badania) na podstawie informacji otrzymanych z serwera PACS o dostarczeniu obrazów • W przypadku łączenia kart pacjenta w RIS wysyłanie odpowiednich informacji umożliwiających automatyczne połączenie i aktualizację rekordów pacjenta przez system PACS
INTEGRACJA HL7 Z TELERADIOLOGIĄ	
4.4.76.	Funkcja przesłania zlecenia opisu badania z systemu RIS do zewnętrznego systemu Teleradiologii (HL7). Możliwość konfiguracji kilku systemów Teleradiologii
4.4.77.	Funkcja odbioru opisów badań z systemu Teleradiologii (HL7) i automatycznego przesłania ich do systemu HIS AMMS. Odbiór opisów w jako zwykły tekst w HL7, jako podpisany elektronicznie pdf oraz jako HL7 CDA PIK umożliwiający przesłanie do EDM i indeksowanie w P1
INTEGRACJA GŁĘBOKA Z SYSTEMEM HIS – AMMS ASSECO ORAZ HL7 Z EDM	
4.4.78.	Przyjmowanie zleceń HL7 drogą elektroniczną wraz z importem danych zlecenia i pacjenta
4.4.79.	Automatyczne odsyłanie informacji o terminie umówienia badania
4.4.80.	Możliwość odrzucenia zlecenia (badania nie zarejestrowanego).
4.4.81.	Możliwość odwołania badania zarejestrowanego.
4.4.82.	W przypadku braku zlecenia elektronicznego z oddziału szpitalnego – możliwość rejestracji badania przez rejestratorkę RIS „na konto / w imieniu” takiego oddziału

4.4.83.	Automatyczne odsyłanie do systemu HIS opisu badania zleconego elektronicznie , aktualizacja po zmianie opisu w RIS
4.4.84.	Odsyłany do HIS komunikat HL7 z opisem badania, oprócz tekstu opisu zawiera dokument PDF z podpisem elektronicznym radiologa
4.4.85.	Możliwość przeglądania historii leczenia szpitalnego udostępnionej przez system HIS w systemie RIS poprzez wywołanie kontekstowe
4.4.86.	Możliwość wyszukania i wykorzystania danych pacjenta z bazy danych systemu HIS podczas umawiania badania w RIS
4.4.87.	Automatyczne dodawanie pacjenta do bazy danych HIS podczas zakładania kartoteki w systemie RIS, z możliwością zmiany danych pacjenta w HIS z poziomu systemu RIS
4.4.88.	Automatyczny bezpośredni zapis danych pacjenta w systemie HIS podczas rejestracji w RIS. Dane każdego zarejestrowanego badania w RIS (również ambulatoryjnego) muszą zostać zapisane w systemie HIS
4.4.89.	Synchronizacja słowników (jednostek zlecających, lekarzy kierujących) między systemami HIS-RIS
4.4.90.	Podczas pracy dyżurowej, automatyczne przyjmowanie do realizacji zleceń z systemu HIS
4.4.91.	Przekazywanie przez system RIS do systemu HIS informacji o stanie realizacji badania – wykonane ale nie opisane, zatwierdzone przez radiologa
4.4.92.	Wsparcie systemu RIS dla funkcji aktualizacji obiegu informacji – zmiana danych pacjenta w systemie HIS musi automatycznie generować zmianę w systemie RIS, oraz PACS/WEB
4.4.93.	Równolegle z odsyłaniem opisu badania do HIS, system RIS przesyła w standardzie HL7 CDA podpisany elektronicznie opis, do systemu EDM, na potrzeby indeksowania w P1

II.5 AI Dokumentacja obrazowa - interfejs do systemu CeZ integracja z PUI

Ogólny opis

Przedmiotem zamówienia jest zakup interfejsu do tworzenia, przechowywania i wymiany dokumentacji obrazowej (DICOM + opisy) z wykorzystaniem AI oraz integracją z ekosystemem CeZ (Centrum e-Zdrowia) i warstwą PUI (Platforma Usług Integracyjnych).

Cel zamówienia

Celem zamówienia jest pozyskanie kompleksowego rozwiązania do integracji z Platformą Usług Inteligentnych (PUI) Centrum e-Zdrowia. Umożliwi ono zautomatyzowane zlecanie analiz AI dla badań obrazowych oraz pełną obsługę procesu diagnostycznego — od wykonania badania obrazowego, przez analizę AI, aż po udostępnienie wyników personelowi medycznemu Zamawiającego.

Wymagania minimalne

Lp.	Wymagane parametry techniczno-użytkowe
5.3.1.	System dostarczony z kompletem bezterminowych licencji niezbędnych do działania, w tym dla: systemu operacyjnego, systemu bazy danych oraz innych modułów.

5.3.2.	Dostarczony Moduł Zarządzania Opisami (MZO) i integracji z PUI musi zostać zintegrowany z użytkowanym przez Zamawiającego systemem RIS i PACS. Lity robocze zleceń z HIS, statusy i opisy badań musza być zsynchronizowane między modułem MZO i systemem RIS (przykładowo: opisy badań wprowadzane w module MZO musza być widoczne w systemie RIS i odwrotnie – opisy wprowadzane w systemie RIS musza być widoczne w module MZO.
5.3.3.	MZO nie wymaga instalacji na stanowisku, uruchamiany jest poprzez standardową przeglądarkę internetową (zero footprint)
5.3.4.	Logowanie do interfejsu MZO odbywa się przy użyciu kont/haseł (synchronizacja z RIS). Zarzadzanie kontami przez lokalnego administratora
5.3.5.	MZO umożliwia filtrację listy badań z uwzględnieniem minimum: • Dane pacjenta: Nazwisko, Imię, Pesel, płeć • Dane badania: Id. zlecenia, data wykonania, nazwa, aparat, lekarz zlecający, zleceniodawca, lekarz opisujący
5.3.6.	Interfejs pozwalający na przypisanie określonego badania do opisu przez lokalnego radiologa, grupy radiologów, zewnętrznego systemu teleradiologii – z zaznaczeniem priorytetu/pilności wykonania opisu
5.3.7.	Interfejs pozwalający po przypisaniu zadań opisu poszczególnym radiologom, na filtrowanie zadań dla poszczególnych radiologów. Funkcja ograniczenia widoczności dla danego radiologa badań do opisu - tylko przypisanych do jego konta.
5.3.8.	Interfejs pozwalający po przypisaniu zadań opisu poszczególnym systemom teleradiologii, na filtrowanie zadań dla poszczególnych usługodawców teleradiologii. Funkcja ograniczenia możliwości opisania badania – badania przypisane do teleradiologii nie mogą być opisane przez radiologów lokalnych.
5.3.9.	Integracja MZO z zewnętrznymi systemami Teleradiologii, pozwalająca na: • automatyczne wysyłanie zlecenia HL7 do systemu teleradiologii po przypisaniu do niego zadania opisu • automatyczne pobieranie z PACS użytkowanego przez Zamawiającego i wysyłanie obrazów DICOM do węzła DICOM systemu teleradiologii • odbieranie komunikatów HL7 z opisami badań (w tym również komunikatów zawierających PDF, HL7CDA • przekazywanie odebranych opisów /PDF/CDA do zintegrowanych systemów RIS/HIS/EDM
5.3.10.	Funkcja zdefiniowania kilku systemów Teleradiologii. Dla wybranego systemu teleradiologicznego możliwość ustawienia czy w momencie inicjowania zlecenia ma być wysłany komunikat HL7 lub obrazy DICOM lub zarówno HL7 jak i obrazy DICOM
5.3.11.	Interfejs pozwalający do danego badania dołączyć dodatkową dokumentację dostarczoną w postaci PDF oraz pozwalający na skanowanie dokumentów dostarczonych w postaci papierowej

5.3.12.	Interfejs pozwalający na zaimportowanie obrazów z płyty CD/DVD (np. przyniesione przez pacjenta do porównania z badaniem bieżącym) i wysłanie do PACS
5.3.13.	Interfejs pozwalający na zaznaczenie przez radiologa odmowy opisu badania (z możliwością dodania odpowiedniego komentarza/informacji). Odmowa widoczna w interfejsie dla techników / rejestracji.
5.3.14.	Interfejs wyświetlający informacje otrzymywane w zleceniu badania z systemu HIS (rozpoznanie, cel badania)
5.3.15.	Zapewnienie indywidualnych wzorców opisów widocznych tylko dla określonego użytkownika wraz z możliwością ich zarządzania w tym dodawanie, edycja i modyfikacja w trakcie wprowadzania opisu. Zapewnienie wzorców ogólnie dostępnych, modyfikowanych tylko przez uprawnionych użytkowników
5.3.16.	Szybki dostęp do wszystkich wyników wcześniejszych badań diagnostycznych pacjenta z możliwością bezpośredniego kopiowania wcześniejszych opisów do bieżącego wyniku
5.3.17.	Możliwość przerwania opisu i pozostawienia badania do konsultacji z nadanym specjalnym statusem (wynik nie jest odsyłany do systemu zewnętrznego HIS) w celu szybkiego późniejszego odnalezienia w systemie i zatwierdzenia
5.3.18.	Monitorowanie wszelkich modyfikacji opisów badań z zaznaczeniem kto, kiedy i jakich zmian w opisie dokonał
5.3.19.	Możliwość przypisania jednego wspólnego opisu kilku badaniom tego samego pacjenta w trakcie jednoczesnego opisywania
5.3.20.	Współpraca pomiędzy MZO a przeglądarką diagnostyczną obrazów (Impax, VIZO+) działającymi jednocześnie na opisowej stacji lekarskiej. Współpraca polegająca na otwarciu obrazów w programie diagnostycznym wywoływanym z poziomu okna edycji opisu
5.3.21.	Współpraca pomiędzy MZO a systemem HIS-AMMS działającymi jednocześnie na opisowej stacji lekarskiej. Współpraca polegająca na otwarciu danych leczenia pacjenta w programie HIS wywoływanym z poziomu okna edycji opisu (wywołanie kontekstowe). Koszt licencji i wdrożenia wywołania kontekstowego po stronie systemu HIS pokrywa Wykonawca.
5.3.22.	Sprawdzanie przez program pisowni wprowadzonego wyniku badania, z możliwością dodania występującego wyrażenia do słownika
5.3.23.	Możliwość podpisywania elektronicznego podczas zatwierdzania opisów przez lekarza (min. podpis ZUS)
5.3.24.	Zatwierdzone przez lekarza opisy badań, dostępne w formie podpisanego elektronicznie PDF
5.3.25.	Zabezpieczenie systemu przed możliwością opisywania tego samego badania w tym samym czasie przez różnych radiologów
5.3.26.	Możliwość oceny przez lekarza jakości wykonanego badania z użyciem danych słownikowych ocen w celu wykonania późniejszej statystyki,

	oraz komunikacja pomiędzy lekarzem a technikiem wykonującym badanie (chat)
5.3.27.	Możliwość wydruku opisu wraz z podstawowymi danymi dotyczącymi pacjenta, zlecenia, nazwą aparatu, datą, identyfikacją lekarza opisującego – edytowalny szablon wydruków opisów
5.3.28.	Generowanie statystyk (liczby opisanych badań przez radiologów, systemy Teleradiologii, PUI)
5.3.29.	Podłączenie MZO do centralnego repozytorium danych medycznych w Centrum e-Zdrowia w zakresie AI (PUI), spełniające wszystkie wymagania CeZ oraz poniższe założenia.
5.3.30.	Komunikacja z platformą PUI CeZ - Autoryzacja i uwierzytelnianie (OAuth 2.0).
5.3.31.	Komunikacja z platformą PUI CeZ - Pobieranie katalogu usług.
5.3.32.	Komunikacja z platformą PUI CeZ - Przesyłanie zlecenia do AI (metadane + dane binarne). Dane obrazowe przesyłane do PUI pobierane automatycznie z podłączonego systemu PACS
5.3.33.	Komunikacja z platformą PUI CeZ - Monitorowanie statusów przetwarzania zleceń na analizę AI w PUI.
5.3.34.	Komunikacja z platformą PUI CeZ - Pobieranie wyników analiz z AI (DICOM z warstwą AI, pliki np. PDF, dane tekstowe).
5.3.35.	Komunikacja z platformą PUI CeZ – Możliwość odbioru analizy AI : sygnalizacja ryzyka zagrożenia życia (TRIAGE) i prezentacja ostrzeżenia w interfejsie MZO
5.3.36.	Komunikacja z platformą PUI CeZ - Możliwość ewidencji danych oceny jakości działania modelu AI w ramach konkretnego badania obrazowego oraz wysyłka tej informacji zwrotnej do PUI (feedback API).
5.3.37.	Komunikacja z platformą PUI CeZ – możliwość prezentacji informacji o rodzaju i szczegółach błędu jeśli operacja zlecenia analizy AI lub samej analizy zakończyła się niepowodzeniem.
5.3.38.	Zapis i prezentacja wyników analiz AI platformy PUI CeZ - Dane opisowe (HL7 MSG ORU)
5.3.39.	Zapis i prezentacja wyników analiz AI platformy PUI CeZ - Dokumenty np. raporty PDF
5.3.40.	Zapis wyników analiz AI platformy PUI CeZ – odbiór przetworzonych przez AI obrazów DICOM badania z dodatkowymi adnotacjami – np. z zaznaczonymi obszarami podejrzanymi o zmiany chorobowe (C-STORE). Odebrane z PUI dane obrazowe mogą być automatycznie przesyłane do PACS użytkowanego przez Zamawiającego i/lub jeśli z jakichś powodów wyniki analiz AI nie mogą być przechowywane na lokalnym serwerze PACS, to rozwiązanie powinno zapewnić podręczny magazyn na wyniki obrazowe analiz AI z konfigurowalnym okresem retencji np. 30 dni.
5.3.41.	Integracja MZO z platformą PUI Cez – możliwość wskazania ręcznego przez uprawnionego użytkowania, badania które ma zostać wysłane do analizy AI, oraz możliwość zdefiniowania

	algorytmu na potrzeby wysyłania automatycznego (np. wszystkie badania klatki piersiowej TK)
5.3.42.	Interfejs MZO umożliwiający wyświetlenie proponowanego przez AI opisu badania wygenerowanego przez PUI, oraz wykorzystanie/uwzględnienie jego treści przy tworzeniu własnego opisu przez radiologa. Po ewentualnej zmianie i zatwierdzeniu przez radiologa wykonany w MZO opis badania jest przesyłany do systemów RIS/HIS/EDM
5.3.43.	Interfejs MZO umożliwiający wywołanie przeglądarki DICOM użytkowanej przez Zamawiającego w kontekście konkretnego badania obrazowego i przeglądu obrazowych wyników analiz AI.
5.3.44.	Koszty integracji z RIS / PACS / HIS / EDM / Teleradiologia (obecnie używana) - leżą po stronie oferenta.

II.6 Rozbudowa posiadanego systemu do zarządzania infrastrukturą IT

Stan obecny

Zamawiający posiada oprogramowanie Axence nVision w wersji 13, które umożliwia zarządzanie infrastrukturą IT Zamawiającego. Zamawiający posiada licencje na następujące moduły:

Lp.	Element Systemu	Liczba posiadanych licencji
4.1.1.	Moduł **Network**, który monitoruje serwery pocztowe i adresy WWW, serwisy TCP/IP i Windows, stan i działanie aplikacji oraz switche i routery	Nielimitowana liczba urządzeń
4.1.2.	Moduł **HelpDesk**, który zapewnia interaktywną bazę zgłoszeń dla użytkowników, która ułatwia zgłaszanie i rozwiązywanie problemów.	350 stanowisk
4.1.3.	Moduł **DataGuard**, który umożliwia zarządzanie prawami dostępu do danych i ich ochroną.	350 stanowisk

Ogólny opis

Przedmiotem zamówienia jest:

6.2.1. zakup dodatkowych 50 licencji na stacje robocze, dla posiadanych już modułów;
6.2.2. zakup 400 licencji na stacje robocze na modułu inwentaryzacyjnego **Invectory**
6.2.3. upgrade do najnowszej wersji oprogramowania
6.2.4. wsparcie serwisowe przez okres kolejnych 3 lat

Wymagania dotyczące Modułu Invectory

Lp.	Wymagania minimalne
6.3.1.	W zakresie inwentaryzacji program automatycznie gromadzi informacje o sprzęcie i oprogramowaniu na stacjach roboczych oraz: 6.3.1.1. Prezentuje szczegóły dotyczące sprzętu: modelu, procesora, pamięci, płyty głównej, napędów, kart itp.

	6.3.1.2. Umożliwia odczyt parametrów S.M.A.R.T. dysków twardych, dysków SSD, w tym NVMe. 6.3.1.3. Obejmuje m.in.: zestawienie posiadanych konfiguracji sprzętowych, wolne miejsce na dyskach, średnie wykorzystanie pamięci, informacje pozwalające na wytypowanie systemów, dla których konieczny jest upgrade. 6.3.1.4. Informuje o zainstalowanych aplikacjach oraz aktualizacjach Windows co bezpośrednio umożliwia audytowanie i weryfikację użytkowania licencji w organizacji. 6.3.1.5. Zbiera informacje w zakresie wszystkich zmian przeprowadzonych na wybranej stacji roboczej: instalacji/deinstalacji aplikacji, zmian adresu IP itd. 6.3.1.6. Posiada możliwość wysyłania powiadomienia np. e-mailem w przypadku zainstalowania programu lub jakiejkolwiek zmiany konfiguracji sprzętowej komputera. 6.3.1.7. Umożliwia odczytanie numeru seryjnego (klucze licencyjne). 6.3.1.8. Umożliwia automatyczne zarządzanie instalacjami i deinstalacjami oprogramowania poprzez określenie paczek aplikacji wymaganych oraz nieautoryzowanych. 6.3.1.9. Umożliwia przegląd informacji o konfiguracji systemu, np. komend startowych, zmiennych środowiskowych, kontach lokalnych użytkowników, harmonogramie zadań itp. 6.3.1.10. Umożliwia utworzenie listy plików użytkowników z określonym rozszerzeniem (np. filmy .AVI) znalezionych na stacjach roboczych oraz ich zdalne usuwanie wraz z wykrywaniem metadanych plików użytkownika: obrazów (wymiary obrazka), video (długość filmu), audio (długość nagrania), archiwów (liczba plików w środku, rozmiar po wypakowaniu). 6.3.1.11. Umożliwia wymianę plików do i ze stacją roboczą poprzez funkcję Menedżera plików. Działania administratorów wykonywane w tej funkcji są logowane.
6.3.2.	Moduł inwentaryzacji zasobów umożliwia prowadzenie bazy ewidencji majątku IT w zakresie sprzętu i programowania: 6.3.2.1. przechowywania wszystkich informacji dotyczących infrastruktury IT w jednym miejscu oraz automatycznego aktualizowania zgromadzonych informacji, 6.3.2.2. przydzielania dostępu administratorów do zasobów na podstawie praw do oddziałów, 6.3.2.3. tworzenia powiązań między zasobami a urządzeniami, 6.3.2.4. tworzenia powiązań między zasobami a kontami użytkowników (zarówno lokalnymi, jak i zsynchronizowanymi z Active Directory), wskazywanie osób odpowiedzialnych, 6.3.2.5. tworzenia relacji pomiędzy zasobami, 6.3.2.6. wskazania osób uprawnionych do użycia zasobów poprzez rozbudowane mechanizmy, 6.3.2.7. definiowania własnych typów zasobów (elementów wyposażenia), ich atrybutów oraz wartości - dla danego urządzenia lub oprogramowania istnieje możliwość dodawania dodatkowych informacji, np. numer inwentarzowy, osoba odpowiedzialna, numer dokumentu zakupu, wartość sprzętu lub oprogramowania, nazwa sprzedawcy, termin upływu gwarancji, termin kolejnego przeglądu (można podać datę, po której administrator otrzyma powiadomienie e-

	mail o zbliżającym się terminie przeglądu lub upływie gwarancji), nazwa firmy serwisującej, lub własny komentarz, 6.3.2.8. określenia atrybutów wymaganych, które są obowiązkowe dla wszystkich zasobów, 6.3.2.9. określenia atrybutów dodatkowych tylko dla wybranych typów zasobów, 6.3.2.10. masową edycję atrybutów zasobów, 6.3.2.11. definiowanie własnych list jednokrotnego wyboru jako dodatkowe informacje o zasobie, 6.3.2.12. importu danych z zewnętrznego źródła (.CSV), 6.3.2.13. przechowywania dowolnych dokumentów (np. pliki .DOCX, .XLSX, .PDF), np.: skan faktury zakupu, gwarancji, dowolnego dokumentu itp., 6.3.2.14. tworzenia powiązań między zasobami a dokumentami w relacji 1:N, 6.3.2.15. oznaczania statusów zasobów, np. w użyciu, w naprawie, zutylizowany itp., 6.3.2.16. ewidencji czynności wykonywanych na zasobach, np.: aktualizacja, naprawa w serwisie, konserwacja itp. wraz z możliwością określenia kosztu oraz czasu przeznaczonego na wykonanie czynności, 6.3.2.17. generowania zestawienia wszystkich zasobów, w tym urządzeń i zainstalowanego na nich oprogramowania, 6.3.2.18. przygotowanie wielu szablonów generowanych dokumentów i protokołów przekazania zasobów wraz z konfigurowalną sekcją zawierającą dane i logo organizacji, konfiguracji stylu automatycznego numerowania dodawanych zasobów wg zdefiniowanego wzorca, 6.3.2.19. konfiguracji stylu automatycznego numerowania dodawanych dokumentów i protokołów wg zdefiniowanego wzorca, 6.3.2.20. archiwizacji i porównywania audytów zasobów, 6.3.2.21. tworzenia kodów kreskowych dla zasobów, 6.3.2.22. drukowania kodów kreskowych oraz dwuwymiarowych kodów alfanumerycznych (QR Code) dla zasobów, które posiadają numer inwentarzowy, 6.3.2.23. inwentaryzacji zasobów posiadających kody kreskowe za pomocą aplikacji mobilnej dla systemu Android poprzez wyszukiwanie zasobów, skanowanie etykiet, dodawanie i edycję zasobów, dodawanie czynności serwisowych, drukowanie etykiet, 6.3.2.24. możliwość zmiany portu komunikacyjnego wykorzystywanego przez aplikację mobilną dla systemu Android, 6.3.2.25. inwentaryzacji stacji roboczych niepodłączonych do sieci (bez instalacji Agenta poprzez manualne wykonanie skanów inwentaryzacji offline), 6.3.2.26. definiowania alarmów z powiadomieniami e-mail dla dowolnych pól czasowych typu „data” z atrybutów zasobów lub licencji (np. „za 2 tygodnie wygaśnie licencja/gwarancja”).
6.3.3.	Inwentaryzacja oprogramowania zapewnia funkcjonalność w zakresie pozyskiwania informacji o oprogramowaniu i audycie licencji poprzez: 6.3.3.1. Skanowanie plików wykonywalnych i multimedialnych na stacjach roboczych, skanowanie archiwów ZIP. 6.3.3.2. Informacje o aplikacjach używanych w organizacji. 6.3.3.3. Tworzenie własnych wzorców aplikacji. 6.3.3.4. Tworzenie dowolnych kategorii aplikacji, np. nowe, zabronione, projektowe itp.

	6.3.3.5. Informacje o komputerach, na których aplikacja została wykryta. 6.3.3.6. Zarządzanie posiadanymi licencjami. 6.3.3.7. Wskazywanie osób odpowiedzialnych za licencję. 6.3.3.8. Wskazanie użytkowników licencji. 6.3.3.9. Tworzenia powiązań między licencjami a dokumentami w relacji 1:N. 6.3.3.10. Rozbudowane i konfigurowalne scenariusze zarządzania licencjami poprzez: przypisywanie do użytkownika, przypisywanie do wielu komputerów tego samego użytkownika, przypisywanie wg numerów seryjnych, przypisywanie wg różnych wersji aplikacji na jednym urządzeniu. 6.3.3.11. Łatwy audyt legalności oprogramowania oraz powiadamianie tylko w razie przekroczenia liczby posiadanych licencji - w każdej chwili istnieje możliwość wykonania aktualnych raportów audytowych. 6.3.3.12. Zarządzanie posiadanymi licencjami: raport zgodności licencji. 6.3.3.13. Możliwość przypisania do programów numerów seryjnych, wartości itp. Okna audytowe posiadają możliwość filtrowania elementów per oddział.

Wsparcie serwisowe

6.4.1. Przedmiotem zamówienia jest świadczenie usługi wsparcia serwisowego (Umowa Serwisowa) dla posiadanego oprogramowania umożliwiającego zarządzanie infrastrukturą IT Zamawiającego w najnowszej wersji, obejmującego 400 stacji roboczych z aktywnymi modułami:
- Network
- HelpDesk
- DataGuard
- Inventory

6.4.2. Zakres usług serwisowych

W ramach umowy serwisowej Wykonawca zobowiązany jest do zapewnienia:
- Aktualizacji oprogramowania – udostępnianie nowych wersji, poprawek bezpieczeństwa, łat systemowych oraz ulepszeń funkcjonalnych w całym okresie obowiązywania umowy.
- Wsparcia technicznego w formie:
  - kontaktu telefonicznego i e-mailowego,
  - pomocy zdalnej (np. poprzez narzędzia do zdalnego pulpitu),
  - konsultacji konfiguracyjnych i doradztwa w zakresie prawidłowego wykorzystania modułów.
- Diagnostyki i pomocy w przypadku awarii – analiza logów, weryfikacja błędów, wskazanie i wdrożenie rozwiązania problemu.
- Dostępu do dokumentacji i materiałów technicznych – instrukcji, podręczników użytkownika i rekomendacji producenta.
- Świadczenia usług w standardzie SLA – czas reakcji na zgłoszenie: następny dzień roboczy (NBD).

6.4.3. Czas trwania umowy: 36 miesięcy od dnia jej podpisania

6.4.4. Warunki dostępności i SLA
- Czas reakcji na zgłoszenie: do końca następnego dnia roboczego od chwili przyjęcia zgłoszenia.
- Godziny świadczenia usług: dni robocze od godziny 8:00 do 16:00.

- Zgłoszenia będą rejestrowane poprzez: e-mail, telefon lub portal serwisowy (jeśli dostępny).

6.4.5. Dokumenty i potwierdzenia

- Wykonawca zobowiązany jest dostarczyć Zamawiającemu dokument potwierdzający prawo do korzystania z usług wsparcia (np. certyfikat serwisowy, dokument od producenta oprogramowania).
- Każde zgłoszenie serwisowe musi być zamknięte poprzez raport zawierający opis podjętych działań.

6.4.6. Obowiązki wykonawcy

- Utrzymanie kompetentnego zespołu wsparcia technicznego posiadającego doświadczenie w pracy z systemem Zamawiającego.
- Zapewnienie ciągłości świadczenia usług przez cały okres umowy.
- Zachowanie poufności danych i konfiguracji systemu Zamawiającego.

6.4.7. Wymogi formalne

- Wykonawca musi być producentem oprogramowania lub jego autoryzowanym partnerem.
- Wykonawca zobowiązuje się do zapewnienia wsparcia w języku polskim.

Rozwiązanie równoważne

Zamawiający dopuszcza wymianę obecnie wykorzystywanego oprogramowania umożliwiającego zarządzanie infrastrukturą IT Zamawiającego na rozwiązanie równoważne, które zachowa wszystkie funkcjonalności obecnie wykorzystywanego systemu i funkcjonalności modułów, które są przedmiotem tego postępowania z okresem wsparcia serwisowego, które jest przedmiotem tego postępowania oraz nie mniejszą ilością licencji na poszczególne funkcjonalności.

Wymagania minimalne dla oprogramowania do zarządzania infrastrukturą IT Zamawiającego (stan przed realizacją tego zadania):

Lp.	Wymagania minimalne
Specyfikacja Techniczna Oprogramowania	
6.5.1.	Oprogramowanie posiada budowę modułową, składa się z: • serwera zarządzającego, • zdalnych konsoli • Agentów.
6.5.2.	Instalacje zdalnych konsoli zarządzania nie podlegają limitom i nie są objęte dodatkowym licencjonowaniem.
6.5.3.	Komunikacja pomiędzy Serwerem a Agentami i Konsolami nawiązywana jest przy użyciu szyfrowanego protokołu TLS 1.2.
6.5.4.	Program umożliwia zmianę portu komunikacyjnego wykorzystywanego przez konsolą zarządzającą
6.5.5.	Moduły umożliwiają kompleksowy monitoring sieci, monitoring sprzętu komputerowego na stanowiskach użytkowników pod kątem zmian sprzętowych i programowych oraz pomocy w formie interaktywnego połączenia sieciowego z obsługiwanym użytkownikiem.
6.5.6.	Program wykorzystuje darmowy, bezpieczny, stabilny i wysoce wydajny silnik bazy danych z kodem źródłowym dostępnym na licencji open-source tj. PostgreSQL, dzięki czemu nie jest

	objęty limitem ilości danych; baza danych jest rozwiązaniem darmowym niewymagającym dodatkowego licencjonowania.
6.5.7.	Agent programu korzysta z bazy danych z wydajnym i stabilnym silnikiem SQLite, która nie wymaga dodatkowego licencjonowania.
6.5.8.	Instalacja Serwera oraz Konsol zarządzających wymaga 64-bitowego systemu operacyjnego Windows.
6.5.9.	Oprogramowanie zawiera rozbudowany system raportowy zawierający ponad 130 raportów predefiniowanych oraz umożliwiający tworzenie własnych raportów wraz z możliwością pełnego dostosowania wyglądu.
6.5.10.	Główny Administrator ma możliwość zarządzania uprawnieniami konfiguracyjnymi programu dla innych kont z rolą administracyjną np. może wyłączyć możliwość zdalnej deinstalacji Agenta, ograniczyć dostęp do Opcji programu oraz logów działań innych administratorów.
6.5.11.	Działania administratorów są logowane oznacza to, że program posiada dziennik z listą czynności wykonanych przez administratorów, które zmodyfikowały obiekty znajdujące się w systemie w tym m.in. logowanie dostępu do Opcji programu, logowanie dostępu do informacji o aktywności użytkownika, logowanie poleceń deinstalacji Agenta.
6.5.12.	Działania administratorów mogą być automatycznie eksportowane do zewnętrznego kolektora Syslog.
6.5.13.	Lista kont użytkowników, w tym administratorów, może być synchronizowana z Active Directory wraz z awatarami, również przez szyfrowane połączenie LDAPS.
6.5.14.	Program umożliwia również tworzenie lokalnych kont użytkowników wraz z awatarami w środowiskach bez Active Directory.
6.5.15.	Liczba kont użytkowników w konsoli nie jest objęta limitem i nie podlega licencjonowaniu.
6.5.16.	Program umożliwia konfigurację polityki haseł do lokalnych kont użytkowników konsoli. Polityka pozawala na określenie: minimalnej długości hasła, liter, cyfr, znaków specjalnych oraz automatycznie wymusza dostosowanie bieżących haseł do obowiązujących zasad.
6.5.17.	Program zawiera mechanizmy uwierzytelniania logowań administratorów do konsoli z wykorzystaniem weryfikacji dwuskładnikowej (MFA).
6.5.18.	Kod autoryzacyjny może być wysyłany za pomocą e-mail i/lub SMS
6.5.19.	Ochrona przed usunięciem. Program jest zabezpieczony hasłem przed ingerencją użytkownika w jego działanie i próbą usunięcia, nawet jeśli użytkownik ma prawa administratora stacji roboczej, na której pracuje.
6.5.20.	Funkcjonalność Agenta. Możliwość automatycznego wyszukiwania serwera przez oprogramowanie monitorujące stacje robocze.
6.5.21.	Zabezpieczenia. Instalator programu jest zabezpieczony podpisem cyfrowym wystawionym i zweryfikowanym przez zaufany globalny urząd certyfikacji (CA).
6.5.22.	Globalna wyszukiwarka, zwracająca wyniki obiektów różnego typu na podstawie wyszukiwanych słów kluczowych, np.: urządzenia, użytkownicy, zasoby, elementy interfejsu konsoli zarządzającej, elementy opcji.
Moduł Network	
6.5.23.	Monitorowanie infrastruktury (bezagentowo) obejmuje serwery Windows, Linux, Unix, Mac; routery, przełączniki, urządzenia VoIP i firewalle w zakresie:

	6.5.23.1. wykrywania urządzeń w sieci poprzez skanowanie ping oraz arp-ping wykrywania urządzeń na podstawie informacji odczytanych z Active Directory (wraz z informacją o OU) 6.5.23.2. wizualizacji stanu urządzeń w postaci ikon urządzeń na graficznych mapach sieci 6.5.23.3. wizualizacji urządzeń na mapach z funkcją siatki umożliwiającej korygowanie pozycji ikon na mapie do najbliższej linii siatki 6.5.23.4. wizualizacji map urządzeń poprzez tworzenie spersonalizowanych map z dowolnym kolorem tła. 6.5.23.5. wizualizacji map urządzeń poprzez tworzenie spersonalizowanych map z wykorzystaniem jako tła zaimportowanych obrazków np. schematu rozmieszczenia pomieszczeń w budynku 6.5.23.6. wizualizacji map urządzeń poprzez grupowanie urządzeń na narysowanych czworokątach o dowolnym rozmiarze i kolorze 6.5.23.7. wizualizacji map urządzeń poprzez wstawianie dowolnego tekstu na mapie 6.5.23.8. wizualizacji połączeń pomiędzy urządzeniami a przełącznikami za pomocą linii i informacji, do którego portu przełącznika podłączone jest dane urządzenie w sposób manualny oraz automatyczny 6.5.23.9. zablokowania mapy urządzeń przed przypadkową edycją serwisów TCP/IP, HTTP, POP3, SMTP, FTP i innych wraz z możliwością definiowania własnych serwisów; program monitoruje czas ich odpowiedzi i procent utraconych pakietów 6.5.23.10. serwerów pocztowych: • program monitoruje czas logowania do serwisu odbierającego oraz czas wysyłania poczty • program ma możliwość monitorowania stanu systemów i wysyłania powiadomienia (e-mail, SMS i inne), w razie, gdyby przestały one odpowiadać lub funkcjonowały wadliwie (np. gdy ważne parametry znajdą się poza zakresem) • program ma możliwość wykonywania operacji testowych • program ma możliwość wysłania powiadomienia jeśli serwer pocztowy nie działa 6.5.23.11. monitorowania serwerów WWW i adresów URL 6.5.23.12. cyklicznego monitorowania czasu ładowania strony internetowej, zmiany treści na stronie internetowej i statusu protokołu HTTPS 6.5.23.13. obsługi szyfrowania SSL/TLS w powiadomieniach e-mail 6.5.23.14. obsługi urządzeń SNMP wspierających SNMP v1/2/3 z szyfrowaniem oraz autoryzacją, (np. przełączniki, routery, drukarki sieciowe, urządzenia VoIP itp.) – monitorowanie wartości za pomocą nazw zmiennych oraz OID 6.5.23.15. obsługi komunikatów syslog i pułapek SNMP i ewidencjonowanie odebranych z nich danych 6.5.23.16. monitoringu routerów i przełączników wg: • zmian stanu interfejsów sieciowych • ruchu sieciowego • podłączonych stacji roboczych – graficzna prezentacja panelu switcha • ruchu generowanego przez podłączone do portów stacje robocze

	6.5.23.17. serwisów Windows: monitor serwisów Windows alarmuje gdy serwis przestanie działać oraz pozwala na jego uruchomienie/zatrzymanie/zrestartowanie 6.5.23.18. wyświetlania statystyk przy każdym urządzeniu na mapie takich jak: czas odpowiedzi urządzenia, czas od ostatniej poprawnej odpowiedzi, nazwa DNS, adres IP, status zarządzalności SNMP, ostrzeżenie o zdarzeniu na urządzeniu 6.5.23.19. monitorowania stanu maszyn wirtualnych Vmware: działa, nie działa, wstrzymano 6.5.23.20. zarządzania stanem maszyn wirtualnych Vmware: wysyłanie poleceń włączenia, wstrzymania i wyłączenia zasilania do każdej maszyny 6.5.23.21. wydajności systemów Windows: • obciążenie CPU, pamięci, zajętość dysków, transfer sieciowy
6.5.24.	Program posiada Inteligentne Mapy i Oddziały, które służą do lepszego zarządzania logiczną strukturą urządzeń w przedsiębiorstwie (Oddziały) oraz tworzą dynamiczne mapy wg własnych filtrów (Mapy Inteligentne). Kryteria automatycznego filtrowania dotyczyć mogą m.in.: • statusu Agenta, • wygenerowanych alarmów, • zainstalowanych aplikacji, • przynależności do oddziału, serwisów sieciowych, danych z SNMP, danych z inwentaryzacji urządzenia itp.
6.5.25.	Program posiada funkcję kompilatora plików MIB, który umożliwia dodawanie definicji dla modułów SNMP.
6.5.26.	Program umożliwia nakładanie na urządzenia liczników wydajności WMI oraz SNMP wg szablonów definiowanie alarmów z wykorzystaniem akcji związanych ze zdarzeniami w systemie, m.in.: • wysłanie komunikatu pulpitowego, • wysłanie wiadomości e-mail, • wysłanie SMS, • wysłanie wiadomości SMS poprzez integrację z serwisem smsapi.pl, • wysłanie wiadomości przez Microsoft Teams (poprzez mechanizmy webhook i workflow) oraz Slack, • uruchomienie programu, • wysłanie pułapki SNMP, • wysłanie pakietu Wake-On-LAN, • zatrzymanie/restart usługi Windows, • wyłączenie/restart komputera.
6.5.27.	Alarmy budowane są przez administratora z wykorzystaniem ciągu przyczynowo skutkowego – oznacza to, że administrator samodzielnie może wskazać dowolne zdarzenie z listy, którego wykrycie wzbudzi alarm oraz dowolną liczbę akcji wybranych z listy, które zostaną wykonane jako reakcja na wykryte zdarzenie.
6.5.28.	Wykonywanie akcji alarmów można skonfigurować automatycznie po wykryciu zdarzenia, z opóźnieniem, na końcu zdarzenia oraz cyklicznie np. co 5 minut.
6.5.29.	Dla akcji można nałożyć ograniczenie czasowe np. nie wykonuj między 8:00-16:00.
6.5.30.	Alarmy pozwalają na priorytetyzację urządzeń, grupowanie wg. ważności i typu urządzenia.

6.5.31.	Oprogramowanie umożliwia wykorzystanie w alarmowaniu skrzynek email z wykorzystaniem autoryzacji OAuth 2.0
6.5.32.	Program ma możliwość integracji ze sprzętową bramką GSM HW-SMS-GW 3 w celu wysyłania powiadomień SMS z wykorzystaniem protokołu netGSM (SOAP) oraz poprzez integrację z bramkami SMSEagle.
Moduł HelpDesk	
6.5.33.	Program umożliwia realizację zdalnej pomocy użytkownikom
6.5.34.	W ramach kontroli stacji użytkownika dostępny jest podgląd pulpitu użytkownika i możliwość przejęcia nad nim kontroli wraz z możliwością zdefiniowania czy użytkownik powinien zostać zapytany o zgodę na połącznie i opcją odrzucenia takiego połącznia przez użytkownika (np. w przypadku pracowników wysokiego szczebla).
6.5.35.	Podczas dostępu zdalnego, zarówno użytkownik jak i administrator widzą ten sam ekran.
6.5.36.	Funkcja zdalnego dostępu oferuje również możliwość zasłonienia ekranu przed użytkownikiem w taki sposób, aby nie widział czynności wykonywanych przez administratora.
6.5.37.	Administrator w trakcie zdalnego dostępu ma możliwość wyboru dowolnego ekranu (monitora) oraz zablokowania działania myszy oraz klawiatury dla użytkownika.
6.5.38.	Zdalne połączenie jest możliwe również do komputerów, które nie posiadają ekranów (maszyny wirtualne, komputery bez podłączonego monitora lub laptopy z zamkniętym skrzydłem matrycy).
6.5.39.	Funkcja zdalnego dostępu umożliwia równoczesne podłączenie do tego samego komputera kilku administratorom.
6.5.40.	W module znajduje się baza zgłoszeń umożliwiająca użytkownikom zgłaszanie problemów technicznych poprzez dedykowany portal oraz przetwarzanie wiadomości e-mail, które są przetwarzane i przyporządkowywane odpowiednim administratorom, otrzymującym automatycznie powiadomienie o przypisanym im problemie.
6.5.41.	Oprogramowanie pozwala na integrację ze skrzynkami e-mail w oparciu o klasyczną autoryzację login/hasło oraz mechanizm OAuth 2.0.
6.5.42.	Moduł umożliwia również przetwarzanie zgłoszeń w trybie anonimowym (wsparcie w realizacji wymogów „Dyrektywy o sygnalistach") oraz zawiera dokumenty prawne dot. ochrony sygnalistów w tym szablon regulaminu zgłoszeń wewnętrznych wymagany przez Dyrektywę.
6.5.43.	Kolejną ważną funkcjonalnością jest umożliwienie użytkownikom monitorowania procesu rozwiązywania zgłoszonych przez nich problemów i ich aktualnych statusów, jak również możliwość wymiany informacji z administratorem poprzez komentarze, które są wpisywane i widoczne dla obu stron.
6.5.44.	System umożliwia użycie pośredniego statusu „zgłoszenie rozwiązane" przed ostatecznym zamknięciem zgłoszenia.
6.5.45.	Moduł ten zawiera komunikator (czat), który umożliwia prowadzenie rozmów w czasie rzeczywistym oraz archiwizację historii wiadomości pomiędzy zalogowanymi użytkownikami, pracownikami pomocy technicznej i administratorami (wraz z wyszukiwarką rozmów i wiadomości wg słów kluczowych oraz automatycznym oczyszczaniem historii rozmów).
6.5.46.	Ponadto czat pozwala na: • zarządzanie dostępem do czatu w 3 poziomach uprawnień: pełny dostęp, brak dostępu lub dostęp ograniczony wyłącznie do pomocy technicznej

	• rozmowy również między „zwykłymi” użytkownikami • osadzanie załączników w treści wiadomości, • osadzanie obrazków w treści wiadomości, • formatowanie tekstu, • tworzenie pokojów tematycznych, rozmów grupowych • oznaczanie kontaktów jako „ulubionych” na liście kontaktów • uruchomienie z poziomu ikony dostępowej Agenta oraz bezpośrednio w interfejsie WWW HelpDesku • może być wyświetlany w trybie jasnym lub ciemnym
6.5.47.	W module zawarta jest również baza wiedzy pomagająca użytkownikom samodzielnie rozwiązywać najprostsze, powtarzające się problemy wraz z możliwością nadawania artykułom 1 z 3 statusów (opublikowany, wewnętrzny, szkic).
6.5.48.	Program umożliwia informowanie pracowników o zdarzeniach, np. planowanych przestojach w dostępie do usług, przez komunikaty z graficznym formatowaniem treści oraz łączami do artykułów w bazie wiedzy.
6.5.49.	Użytkownik ma możliwość przeglądnięcia historii odczytanych komunikatów bezpośrednio z poziomu ikony Agenta. Administrator ma możliwość tworzenia szkiców i archiwizowania komunikatów.
6.5.50.	Dostęp do systemu zgłoszeń oraz bazy wiedzy realizowany jest przez dedykowany portal dostępny przez przeglądarkę internetową, który może być wyświetlany w trybie jasnym lub ciemnym.
6.5.51.	Funkcjonalność modułu umożliwia również uzyskanie dostępu z prywatnego komputera tylko do swojego komputera firmowego, który pozostał w organizacji, za pomocą funkcji zdalnego dostępu przez każdego pracownika.
6.5.52.	Moduł pomocy zdalnej umożliwia: • pobieranie listy użytkowników z Active Directory wraz z awatarami, • wyświetlanie w systemie zgłoszeń wizytówki użytkownika wraz z jego numerem telefonu, adresem e-mail oraz informacją o przełożonym, • zarządzanie lokalnymi kontami Windows w zakresie: tworzenia, usuwania, aktywacji, edycji uprawnień, resetu hasła, edycji kont, • zarządzanie dostępem pracowników HelpDesku do zgłoszeń poprzez rozbudowany system zarządzania regułami widoczności zgłoszeń, • zarządzanie dostępem zwykłych użytkowników końcowych do wybranych kategorii zgłoszeń, • zarządzanie dostępem zwykłych użytkowników końcowych do wybranych kategorii artykułów bazy wiedzy, • tworzenie własnego drzewa kategorii zgłoszeń wraz z możliwością grupowania kategorii w folderach (do 4 poziomów kategorii), opisami kategorii oraz klauzulą RODO, • automatyczne przypisywanie konkretnych pracowników helpdesk do zgłoszeń w określonych kategoriach lub pochodzących od określonych grup użytkowników, • definiowanie ścieżek akceptacji zgłoszeń – procesu, w którym użytkownik uzyskuje akceptację na realizację zgłoszenia od wyznaczonych osób w organizacji, • przypisywanie ścieżek akceptacji zgłoszeń do określonych kategorii, • procesowanie zgłoszeń użytkowników z wiadomości e-mail, • dostęp do plików źródłowych wiadomości e-mail przetworzonych na zgłoszenia,

	• obsługę wielu adresów e-mail jednego użytkownika w celu przetwarzania jako zgłoszeń pochodzących od tej samej osoby, • eksportowania listy zgłoszeń do plików CSV i XLSX, • integrację ze wieloma skrzynkami e-mail w celu obsługi różnych kanałów zgłoszeń wraz z automatyzacjami, • integrację ze skrzynkami e-mail w oparciu o klasyczną autoryzację login/hasło oraz mechanizm OAuth 2.0, • tworzenie formularzy z niestandardowymi polami opisowymi, dedykowanymi do wybranych kategorii zgłoszeń, • uwzględnianie wyników zgłoszeń na podstawie wyszukiwania informacji z pól niestandardowych, • współdzielenie pól dodatkowych pomiędzy wieloma kategoriami zgłoszeń, • dedykowane pola dodatkowe dostępne tylko dla pracowników HelpDesk, administratorów i operatorów, • informacje zawarte w polach dodatkowych widoczne w kolumnach widoku listy zgłoszeń, wykonywanie operacji na wielu zgłoszeniach równocześnie, • dołączanie załączników do zgłoszeń, • usuwanie zamkniętych zgłoszeń, • rozbudowane wyszukiwanie zgłoszeń i artykułów w bazie wiedzy, • szybki dostęp do ostatnich zgłoszeń, artykułów bazy wiedzy i załączników, • wprowadzenie komentarza oraz informacji o czasie poświęconym na rozwiązanie w kreatorze wyświetlanym przy zamykaniu zgłoszenia, • zrzuty ekranowe (podgląd pulpitu), • zdalną modyfikację rejestrów, • dystrybucję oprogramowania przez Agenty, • definiowanie aplikacji dozwolonych do samodzielnej instalacji przez użytkowników z pakietów MSI w postaci Kiosku z Aplikacjami, • przypisywanie dostępnych w Kiosku instalatorów do grup użytkowników, • dystrybucję oraz uruchamianie plików za pomocą Agentów (w tym plików MSI), • zadania dystrybucji plików, jeśli komputer jest wyłączony w trakcie zlecania operacji następuje kolejkowanie zadania dystrybucji pliku, • możliwość skonfigurowania automatyzacji procesowania zgłoszeń wraz z powiadomieniami e-mail wysyłanymi do określonych aktorów w zgłoszeniu, • możliwość skonfigurowania automatyzacji dodających komentarze publiczne wraz z załącznikami i odnośnikami do artykułów w Bazie Wiedzy, • planowanie nieobecności pracowników helpdesk, • obsługę umów o gwarantowanym poziomie świadczenia usług (SLA) wraz z raportami np. przekroczeń SLA wraz z podsumowaniem, • generowanie raportów obsługi helpdesk, • zdalne wykonywanie poleceń poprzez Agenty (np. utworzenie / edycja konta lokalnego użytkownika systemu), • zarządzania procesami systemu Windows (w zakresie: zakończ proces, zakończ drzewo procesu, uruchom nowy proces w sesji użytkownika wraz z parametrami), • wymiany plików do i ze stacji roboczej poprzez funkcję Menedżera plików bez blokowania interfejsu programu podczas przesyłania plików.

Moduł DataGuard	
6.5.53.	Ochrona danych przed wyciekiem poprzez blokowanie urządzeń. 6.5.53.1. Blokowanie urządzeń i nośników danych. Program ma możliwość zarządzania prawami dostępu do wszystkich urządzeń wejścia i wyjścia oraz urządzeń fizycznych, na które użytkownik może skopiować pliki z komputera firmowego lub uruchomić z nich program zewnętrzny. 6.5.53.2. Blokowanie urządzeń i interfejsów fizycznych: USB, FireWire, gniazda kart pamięci, SATA, dyski przenośne, napędy CD/DVD, stacje dyskietek. 6.5.53.3. Blokowanie interfejsów bezprzewodowych: Wi-Fi, Bluetooth, IrDA. 6.5.53.4. Blokownie dotyczy tylko urządzeń służących do przenoszenia danych - inne urządzenia (drukarka, klawiatura, mysz itp.) mogą być podłączane. 6.5.53.5. Alarmowanie o zdarzeniach podłączenia/odłączenia urządzeń zewnętrznych wraz z możliwością ograniczenia alarmów tylko do nośników niezaufanych. 6.5.53.6. Funkcje wspierające bezpieczeństwo systemu: integracja i zarządzanie ustawieniami Windows Defender. 6.5.53.7. Funkcje wspierające bezpieczeństwo systemu: monitorowanie stanu szyfrowania dysków BitLocker. 6.5.53.8. Funkcje wspierające bezpieczeństwo systemu: zdalne szyfrowanie dysków za pomocą BitLocker. 6.5.53.9. Tworzenie list (map) komputerów, które zostały już zaszyfrowane, lub jeszcze nie zostały zaszyfrowane. 6.5.53.10. Funkcje wspierające bezpieczeństwo systemu: zapisywanie klucza odzyskiwania do pliku oraz jako zasób w bazie danych programu. 6.5.53.11. Funkcje wspierające bezpieczeństwo systemu: integracja z Windows Defender w zakresie odczytu stanu ochrony, włączenia i wyłączenia ochrony, tworzenia reguł ruchu. 6.5.53.12. Funkcje wspierające bezpieczeństwo systemu: odczytanie informacji o aktywnym oprogramowaniu antywirusowym firm trzecich, innym niż Windows Defender. 6.5.53.13. Funkcje wspierające bezpieczeństwo systemu: monitorowanie stanu modułu TPM.
6.5.54.	Zarządzanie prawami dostępu do urządzeń: 6.5.54.1. Definiowanie praw użytkowników/grup do odczytu, zapisu czy wykonania plików. 6.5.54.2. Autoryzowanie urządzeń firmowych (przykładowo szyfrowanych): pendrive'ów, dysków itp. - urządzenia prywatne są blokowane. 6.5.54.3. Całkowite zablokowanie określonych typów urządzeń dla wybranych użytkowników. 6.5.54.4. Centralna konfiguracja poprzez ustawienie reguł (polityk) dla całej sieci. 6.5.54.5. Możliwość usuwania z listy znanych urządzeń tych nośników, które np. zostały zutylizowane.
6.5.55.	Audyt operacji na plikach na urządzeniach przenośnych: 6.5.55.1. Zapisywanie informacji o zmianach w systemie plików na urządzeniach przenośnych. 6.5.55.2. Podłączenie/odłączenie urządzenia przenośnego.
6.5.56.	Monitorowanie operacji na plikach w lokalnych folderach komputera użytkownika.

6.5.57.	Definiowanie reguł monitorowanych folderów w postaci list.
6.5.58.	Monitorowanie operacji na plikach na udostępnionych zasobach sieciowych (udziałach) na urządzeniach nieobsługiwanych przez Agenta (np. macierze, NAS itp.)
6.5.59.	Integracja z Active Directory - zarządzanie prawami dostępu przypisanymi do użytkowników oraz grup domenowych. Przydzielanie uprawnień również do kont użytkowników lokalnych.
6.5.60.	Program umożliwia prowadzenie rejestru naruszeń blokad podłączanych nośników.

II.7 Integracja z P1 - wsparcie digitalizacji dokumentacji medycznej

Cel zamówienia

Celem zamówienia jest zakup kompleksowego rozwiązania umożliwiającego digitalizację dokumentacji papierowej Zamawiającego oraz jej integrację z systemami centralnymi Centrum e-Zdrowia (CeZ).

Ogólny opis

Zamawiający posiada i użytkuje Szpitalny System Informatyczny firmy ASSECO POLSKA S.A. o nazwie AMMS, który posiada integrację z systemem e-zdrowia (P1) oraz powiązanymi systemami umożliwiającymi gromadzenie, przetwarzanie i udostępnianie zasobów cyfrowych o zdarzeniach medycznych pacjentów oraz indeksów elektronicznej dokumentacji medycznej (EDM).
Realizacja zadaniaumożliwi pełną integrację z zewnętrznym systemem służącym do digitalizacji dokumentacji papierowej. Produkt umożliwi zaindeksowanie w systemie P1 lub umieszczenie w centralnym repozytorium danych medycznych w Centrum e-Zdrowia zdigitalizowanych kart informacyjnych. Rozwiązanie wesprze Zamawiającego w monitorowaniu wartości wskaźnika (odsetka kart informacyjnych, które zostały zaindeksowane w P1 lub przekazane w postaci zdigitalizowanej) od 01 stycznia 2023 roku. Monitorowanie musi być dostępne również dla pozostałych typów dokumentów indeksowanych w P1.

Wymagania funkcjonalne

Lp.	Wymagania minimalne
7.3.1.	Możliwość monitorowania poziomu zaindeksowania dokumentów (karty informacyjne) - z uwzględnieniem kart przekazanych do centralnego repozytorium Centrum e-Zdrowia dla zdigitalizowanej papierowej dokumentacji medycznej z podziałem na jednostki organizacyjne (możliwość monitorowania wskaźnika na poziomie kierowników poszczególnych jednostek org.), z dokładnością do miesiąca.
7.3.2.	Możliwość ponownej wysyłki indeksów do P1 i przeglądu błędów indeksacji z poziomu GUI HIS (w tym możliwość wykonania reindeksacji w trybie synchronicznym bezpośrednio z ekranu dokumentacji medycznej w danych pobytu pacjenta w szpitalu.)
7.3.3.	Możliwość wymuszenia reindeksacji z poziomu GUI repozytorium EDM
7.3.4.	Funkcjonalność tworzenia dokumentów elektronicznych zgodnych z szablonem PIK HL7 CDA dla dokumentów zdigitalizowanych na bazie zarejestrowanych w systemie dokumentów zeskanowanych.
7.3.5.	Możliwość poświadczenia zgodności dokumentu zdigitalizowanego z oryginałem przez złożenie podpisu elektronicznego.

7.3.6.	Integracja z platformą P1 zgodnie z udostępnioną specyfikacją usług dla dokumentów zdigitalizowanych.
7.3.7.	Automatyczna reindeksacja dokumentów, dla których ustała przyczyna braku możliwości zaindeksowania (np. przekazano z opóźnieniem ZM) – proces działający w tle w oparciu o dostarczoną konfigurację.
7.3.8.	Możliwość przebudowy indeksu dokumentu i wysyłki do P1 bez konieczności tworzenia i podpisu nowej wersji dokumentu w przypadku braku ID ZM
7.3.9.	Prezentacja wskaźników indeksacji dokumentów oraz listy problemów związanych z indeksacją danych w systemie P1
7.3.10.	Wskazanie działań naprawczych dla problemów indeksacji dokumentów w P1 i dostęp do funkcjonalności je realizujących
7.3.11.	Przygotowanie listy dokumentów podlegających indeksowaniu w P1, ale niezaindeksowanych
7.3.12.	Zewnętrzne integracje: • Rozwiązanie obejmuje integrację z systemem P1 w zakresie związanym z obsługą dokumentów zdigitalizowanych.
7.3.13.	Zależności między modułami: • Funkcjonalność opiera się na systemie HIS zintegrowanym z repozytorium EDM oraz komponentem odpowiedzialnym za komunikację z P1.

Kryteria odbioru produktu

Lista mierzalnych i jednoznacznych kryteriów potwierdzających zakończenie prac i gotowość do odbioru:

Lp.	Zgodność funkcjonalna
7.4.1.	Umożliwia monitorowanie poziomu zaindeksowania dokumentów (karty informacyjne) z uwzględnieniem kart przekazanych do centralnego repozytorium Centrum e-Zdrowia dla zdigitalizowanej papierowej dokumentacji medycznej – prezentuje poprawne wartości statystyk zgodnie z liczbą przekazanych dokumentów lub indeksów.
7.4.2.	Umożliwia tworzenie dokumentów elektronicznych zgodnych z szablonem PIK HL7 CDA dla dokumentów zdigitalizowanych i ich utrwalenie w repozytorium EDM.
7.4.3.	Umożliwia przekazanie dokumentów zdigitalizowanych do platformy P1 zgodnie z udostępnioną specyfikacją usług.
7.4.4.	Umożliwia wymuszenie wysyłki indeksu dokumentu EDM do systemu P1 z poziomu GUI.

Wymagania do uruchomienia produktu

Lista zasobów, zależności i warunków koniecznych do uruchomienia modułu:

Lp.	Wymagania uruchomieniowe
7.5.1.	Warunki startowe: • Licencja: Licencja na funkcjonalność. • Działająca integracja z systemem P1 w zakresie wymiany EDM.
7.5.2.	Wymagania techniczne:

	• Rozwiązanie opiera się o istniejące komponenty. • Jako wsparcie/usprawnienie w digitalizacji mogą być wykorzystywane urządzenia skanujące dostawców zewnętrznych – zapewnienie zasobów zgodnie z ich wymaganiami.
7.5.3.	Wymagania organizacyjne: • Podmiot zintegrowany z platformą P1 (w szczególności aktywne konto podmiotu w P1 i aktualne certyfikaty dostępowe). • W przypadku wykorzystania systemów zewnętrznych, licencja na integrację.

Opis wdrożenia

Opis tego, co musi zostać uruchomione i skonfigurowane w ramach wdrożenia:

7.6.1. Uzupełnienie konfiguracji wykorzystywanego przez Zamawiającego szpitalnego systemu informatycznego (HIS) w celu realizacji zamówienia

7.6.2. Konfiguracja wykorzystywanego przez Zamawiającego szpitalnego systemu informatycznego (HIS) w zakresie integracji z urządzeniami skanującymi, które zostaną pozyskane w ramach realizacji zadaniu pn. „Zakup systemu służącego do digitalizacji dokumentacji papierowej” .

II.8 Zakup systemu służącego do digitalizacji dokumentacji papierowej

Ogólny opis

Przedmiotem zamówienia jest dostawa i wdrożenie systemu do automatycznej digitalizacji dokumentacji (dalej: System). System ma umożliwiać digitalizację pisma odręcznego, jak również zapewniać możliwość skanowania zewnętrznej dokumentacji medycznej z opcją opatrzenia jej podpisem cyfrowym.

Zakres prac

W ramach zamówienia Wykonawca zobowiązany jest do:

Lp.	Wymagania minimalne
8.2.1.	Dostawy sprzętu umożliwiającego wykonanie funkcjonalności Systemu – skanery typ 1 (5 sztuk), skanery typ 2 (1 sztuka).
8.2.2.	Dostawy licencji na system w liczbie sztuk 6.
8.2.3.	Instalacji i wdrożenia systemu automatycznej digitalizacji dokumentacji wraz z integracją z posiadanym środowiskiem systemu Medycznego HIS AMMS w jednostce Zamawiającego.
8.2.4.	Przeprowadzenia odpowiednich szkoleń w zakresie administrowania i użytkowania Systemu.
8.2.5.	Przygotowanie szablonów.
8.2.6.	Świadczenia opieki serwisowej wraz z nadzorem autorskim dla wszystkich przekazywanych licencji na System przez okres 36 miesięcy od daty zakończenia wdrożenia.

Wymagania dotyczące sprzętu

8.3.1. Skaner typ 1

Lp.	Wymagania minimalne
8.3.1.1.	Skaner powinien umożliwiać podłączenia za pomocą USB.
8.3.1.2.	Skaner powinien mieć prędkość skanowania 40ppm/80ipm
8.3.1.3.	Podajnik skanera powinien umożliwiać umieszczenie w nim do 80 arkuszy A4
8.3.1.4.	Skaner powinien umożliwiać skanowanie z optyczną rozdzielczością min. 300 DPI
8.3.1.5.	Skaner powinien umożliwiać obsługę polskiego OCR.
8.3.1.6.	Skaner powinien umożliwiać korzystanie ze sterownika TWAIN
8.3.1.7.	Skaner powinien wytrzymać obciążenie dzienne do 5000 stron
8.3.1.8.	Skaner nie może przekraczać wymiarów 330x290x250mm (szer x głęb x wys)
8.3.1.9.	Skaner nie może przekraczać wagi 3,5kg.
8.3.1.10.	Skaner powinien umożliwiać skanowanie długich dokumentów do 3m
8.3.1.11.	Zamawiający wymaga 24 miesięcznej gwarancji na skaner liczonej od momentu dostarczenia sprzętu. Wykonawca ponosi koszty napraw gwarancyjnych wraz z kosztami części i transportu.

8.3.2. Skaner typ 2

Lp	Wymagania minimalne
8.3.2.1.	Skaner powinien umożliwiać działanie w trybie sieciowym lub umożliwiać podłączenia za pomocą USB.
8.3.2.2.	Skaner powinien mieć prędkość skanowania 100ppm/200ipm
8.3.2.3.	Podajnik skanera powinien umożliwiać umieszczenie w nim do 300 arkuszy A3
8.3.2.4.	Skaner powinien umożliwiać skanowanie z optyczną rozdzielczością min. 300 DPI
8.3.2.5.	Skaner powinien umożliwiać obsługę polskiego OCR.
8.3.2.6.	Skaner powinien umożliwiać korzystanie ze sterownika TWAIN
8.3.2.7.	Skaner powinien wytrzymać obciążenie dzienne 45000 stron
8.3.2.8.	Skaner powinien umożliwiać skanowanie długich dokumentów do 4m
8.3.2.9.	Skaner powinien wykrywać podwójne pobrania dokumentów
8.3.2.10.	Zamawiający wymaga 24 miesięcznej gwarancji na skaner liczonej od momentu dostarczenia sprzętu. Wykonawca ponosi koszty napraw gwarancyjnych wraz z kosztami części i transportu.

Minimalne warunki licencji na system

Lp.	Wymagania minimalne
8.4.1.	Z chwilą dostarczenia danego rozwiązania lub jego części dla Zamawiającego, Wykonawca udzieli (z chwilą dostarczenia, bez konieczności składania dodatkowych oświadczeń woli) niewyłącznej licencji na takie rozwiązanie, na czas nieokreślony od daty podpisania przez

	Zamawiającego końcowego protokołu odbioru bez uwag i zastrzeżeń, na następujących polach eksploatacji: 8.4.1.1. wprowadzanie do pamięci komputera, 8.4.1.2. korzystanie, 8.4.1.3. sporządzanie kopii zapasowej, 8.4.1.4. przenoszenie pomiędzy stanowiskami.
8.4.2.	Zamawiający w ramach udzielonej licencji uprawniony będzie do korzystania z wygenerowanych za pomocą danego rozwiązania dokumentów (np. raportów, analiz) w szczególności poprzez: 8.4.2.1. opracowanie, w tym zmianę, adaptację, tłumaczenie, 8.4.2.2. utrwalanie lub zwielokrotnianie w całości lub w części jakimikolwiek środkami i w jakiejkolwiek formie, niezależnie od formatu, systemu lub standardu, w tym techniką drukarską, techniką reprograficzną, techniką cyfrową lub poprzez wprowadzanie do pamięci komputera, 8.4.2.3. publiczne rozpowszechnianie, w tym: wyświetlanie, odtwarzanie w dowolnym systemie lub stan-dardzie, a także publiczne udostępnianie w taki sposób, aby każdy mógł mieć do nich dostęp w miejscu i czasie przez siebie wybranym, 8.4.2.4. wprowadzanie do sieci multimedialnych oraz Internetu, 8.4.2.5. umieszczanie w publikacjach drukowanych (w tym m.in. ulotki, foldery, plakaty), 8.4.2.6. umieszczanie w publikacjach elektronicznych oraz aplikacjach elektronicznych, 8.4.2.7. umieszczanie w prezentacjach i materiałach prasowych, 8.4.2.8. umieszczania w spotach i filmach reklamowych.
8.4.3.	Licencja, o której mowa w ust. 1 i 2 uprawnia Zamawiającego do korzystania z rozwiązania na terytorium Rzeczypospolitej Polskiej.
8.4.4.	Zamawiający może wykonywać wszelkie prawa przyznane w ramach licencji również przy udziale, za pośrednictwem lub przy pomocy osób trzecich świadczących usługi na rzecz Zamawiającego, w tym w szczególności profesjonalnych doradców, konsultantów, zleceniobiorców oraz innych osób współpracujących z Zamawiającym.
8.4.5.	Zamawiający nie będzie mieć prawa przenosić licencji na inne osoby, przy czym wyjątkiem jest zmiana formy prawnej lub zmiany struktury właścicielskiej Zamawiającego, która wyłączona jest spod zapisów tego ustępu.
8.4.6.	Wykonawca składając ofertę oświadcza, iż: 8.4.6.1. przysługują mu wszelkie prawa do przedmiotów własności intelektualnej oferowanych w ramach postępowania oraz prawa te nie są w żaden sposób obciążone prawami osób trzecich; lub 8.4.6.2. przysługują mu prawa do sprzedaży sublicencji na przedmiot własności intelektualnej oferowanej w ramach postępowania oraz prawa te nie są w żaden sposób obciążone prawami osób trzecich; oraz 8.4.6.3. udzielenie licencji zgodnie z ofertą, jak również korzystanie przez Zamawiającego z przedmiotów własności intelektualnej zaoferowanych przez Wykonawcę nie będzie stanowić naruszenia praw osób trzecich.

8.4.7.	Zamawiający gwarantuje parametry ujęte w postępowaniu, a Wykonawca zobowiązany jest do dostarczenia pozostałych elementów niezbędnych do poprawnego wdrożenia rozwiązania.

Licencja integracyjna HIS

Lp.	Wymagania minimalne
8.5.1.	Wykonawca składając ofertę oświadcza, iż w zakresie integracji oferowanego Systemu z systemem HIS Zamawiającego: 8.5.1.1. przysługują mu wszelkie prawa do przedmiotów własności intelektualnej oferowanych w ramach postępowania oraz prawa te nie są w żaden sposób obciążone prawami osób trzecich; lub 8.5.1.2. przysługują mu prawa do sprzedaży sublicencji na przedmiot własności intelektualnej oferowanej w ramach postępowania oraz prawa te nie są w żaden sposób obciążone prawami osób trzecich; oraz 8.5.1.3. udzielenie licencji zgodnie z ofertą, jak również korzystanie przez Zamawiającego z przedmiotów własności intelektualnej zaoferowanych przez Wykonawcę nie będzie stanowić naruszenia praw osób trzecich.
8.5.2.	Oferta Wykonawcy nie przewiduje konieczności uiszczenia dodatkowych opłat za uruchomienie Systemu w integracji z HIS koniecznych do poniesienia przez Zamawiającego na rzecz dostawcy HIS.
8.5.3.	Po upływie 12 miesięcy od wdrożenia, tj. podpisana protokołu odbioru końcowego bez uwag, opłaty należne dostawcy systemu HIS Zamawiającego za wsparcie modułu integracyjnego między Systemem HIS Zamawiającego a dostarczanym przez Wykonawcę Systemem ponosi Zamawiający.
8.5.4.	Zamawiający podkreśla, iż nie dysponuje kodami źródłowymi do systemu HIS Zamawiającego. Wykonawca w ramach realizacji prac zobowiązywany będzie do samodzielnego kontaktu z dostawcą HIS Zamawiającego i zapewnienia wykonania wszelkich prac integracyjnych zarówno od strony dostarczanego Systemu, jak i dostawcy HIS.

Wdrożenie i szkolenia

Lp.	Wymagania minimalne
8.6.1.	W ramach realizacji przedmiotu zamówienie Wykonawca zobowiązany jest do przeprowadzenia wdrożenia systemu w następującym zakresie: 8.6.1.1. instalacja oprogramowania na maszynie wirtualnej w infrastrukturze sieciowej Zamawiającego; 8.6.1.2. rozmieszczenie dostarczanych sprzętów na stanowiskach roboczych wskazanych przez Zamawiającego; 8.6.1.3. instalacja na wskazanych stanowiskach, o których mowa w podpunkcie b, oprogramowania niezbędnego do poprawnej pracy systemu lub dostarczenie zestawu instalatorów wymaganych do przeprowadzenia instalacji domenowe

	8.6.1.4. konfiguracja i parametryzacja dostarczonego oprogramowania do współpracy z dostarczonym sprzętem; 8.6.1.5. w porozumieniu z dostawcą systemu dziedzinowego HIS uruchomienie integracji między systemem HIS a dostarczanym systemem; 8.6.1.6. przekazanie Zamawiającemu zestawu zmiennych i parametrów wymaganych do poprawnego działania integracji między systemem HIS a dostarczanym systemem; 8.6.1.7. przeprowadzenie szkoleń z zakresu działania systemu dla użytkowników systemu (personelu medycznego); 8.6.1.8. przeprowadzenie szkoleń z zakresu administrowania infrastrukturą i konfiguracją systemu dla administratorów szpitala; 8.6.1.9. dostarczenie dokumentacji powdrożeniowej.
8.6.2.	Zamawiający zastrzega sobie prawo do wskazania Wykonawcy w trakcie trwania wdrożenia mniejszej liczby stanowisk do instalacji i konfiguracji niż liczba dostarczonego przez Wykonawcę sprzętu i przeprowadzenia odbioru końcowego z uwzględnieniem powyższej zmiany. Wykonawca będzie zobowiązany do przeprowadzenia instalacji i konfiguracji pozostałych stanowisk w ramach świadczenia opieki serwisowej. Zamawiający uzgodni z Wykonawcą szczegółowy harmonogram instalacji i konfiguracji poza okresem wdrożenia, przy czym czas wykonania instalacji i konfiguracji nie może być dłuższy niż 20 dni roboczych od przekazania Wykonawcy informacji o zleceniu realizacji zadania.
8.6.3.	Szkolenia dla użytkowników systemu zostaną przeprowadzone w trybie: • szkoleń audytoryjnych przeprowadzonych w grupach; i/lub • szkoleń stanowiskowych - na każdym z zainstalowanych i skonfigurowanych stanowisk Wykonawca przeprowadzi szkolenie dla personelu szpitala obsługującego dane stanowisko w dwóch różnych terminach; • szkoleń dla administratorów szpitala z zakresu administrowania infrastrukturą i konfiguracją; • zamawiający przewiduje konieczność przeszkolenia około 27 osób; dokładna liczba osób do przeszkolenia zostanie przekazana Wykonawcy w terminie do 10 dni od zawarcia umowy. 8.6.3.1. Wykonawca jest zobowiązany do umożliwienia każdemu uczestnikowi szkolenia aktywnego uczestnictwa w szkoleniu polegającego na indywidualnym przejściu całego procesu związanego z wygenerowaniem dokumentu z systemu, podpisaniem dokumentu i zapisaniem dokumentu w systemie. 8.6.3.2. Wykonawca jest zobowiązany do uzyskania i udostępnienia Zamawiającemu potwierdzenia uczestnictwa od każdego z uczestników szkoleń. 8.6.3.3. Szkolenia mają być przeprowadzone w placówce Zamawiającego w dni robocze w godzinach od 8:00 do 15:00. Zamawiający zastrzega sobie prawo do zmiany trybu przeprowadzania szkoleń na formę zdalną za pośrednictwem telekonferencji w przypadku występowania w placówce sytuacji epidemiologicznej uniemożliwiającej przeprowadzenie szkoleń stacjonarnych. 8.6.3.4. Wykonawca przekaże Zamawiającemu materiały instruktażowe w postaci filmów instruktażowych lub instrukcji stanowiskowych, umożliwiających wykonanie samodzielnego szkolenia dla personelu szpitala. 8.6.3.5. Zamawiający zastrzega sobie prawo do zorganizowania szkoleń dla części personelu szpitala w terminie wykraczającym poza okres trwania prac wdrożeniowych i

	przeprowadzenia odbioru końcowego z uwzględnieniem powyższej zmiany. Wykonawca będzie zobowiązany do przeprowadzenia pozostałych szkoleń w ramach świadczenia opieki serwisowej. Zamawiający uzgodni z Wykonawcą szczegółowy harmonogram szkoleń poza okresem wdrożenia, przy czym czas przeprowadzenia szkoleń nie może być dłuższy niż 30 dni roboczych od przekazania Wykonawcy informacji o zleceniu realizacji zadania. 8.6.3.6. Wykonawca jest zobowiązany przedstawić Zamawiającemu propozycję szczegółowego harmonogramu szkoleń nie później niż na 3 dni robocze przed planowanym rozpoczęciem szkoleń. 8.6.3.7. Wykonawca jest zobowiązany do uwzględnienia uwag przekazanych przez Zamawiającego, a w przypadku braku takiej możliwości, do przedstawienia nowej propozycji harmonogramu szkoleń w terminie maksymalnie 2 dni roboczych od przekazania uwag.
8.6.4.	Wykonawca przekaże Zamawiającemu Dokumentację powdrożeniową po zakończeniu wszystkich prac wdrożeniowych aktualną na dzień odbioru końcowego. Dokumentacja powdrożeniowa ma obejmować: 8.6.4.1. raport z wykonanych prac wdrożeniowych 8.6.4.2. zestawienie personelu uczestniczącego w szkoleniach 8.6.4.3. instrukcję obsługi systemu 8.6.4.4. wykaz zmiennych i parametrów ustawionych dla systemu 8.6.4.5. informacje na temat dostępnego sposobu zgłaszania awarii i usterek w działaniu systemu 8.6.4.6. wykaz procedur wymaganych dla poprawnego działania systemu, które administrator systemu szpitalnego ma przeprowadzać na serwerze i dostarczonym systemie

Integracja systemu z działającym w placówce systemem HIS

W ramach realizacji przedmiotu zamówienia Wykonawca zobowiązany jest w porozumieniu z dostawcą systemu HIS AMMS do przeprowadzenia modyfikacji systemu w szczególności polegających na:

Lp.	Wymagania minimalne
8.7.1.	umożliwieniu dodawania szablonów dokumentów mających podlegać integracji za pomocą edytora będącego częścią dostarczanego systemu
8.7.2.	umożliwieniu umieszczania w polach aktywnych dokumentu powstałego z szablonu opisanego w pkt. 8.7.1. treści związanych z danymi pacjenta oraz danymi jednostki organizacyjnej szpitala pobieranych z systemu HIS Zamawiającego
8.7.3.	umożliwieniu powiązania dowolnej klasy dokumentacji z systemu HIS Zamawiającego z szablonem opisanym w pkt. 8.7.1.
8.7.4.	umożliwieniu dostosowania istniejących szablonów pism w systemie HIS Zamawiającego do obsługi w systemie digitalizacji poprzez: 8.7.4.1. umieszczenie w pliku szablonu pisma znaczników pól aktywnych takich jak pola podpisu, pola tekstowe, pola wyboru 8.7.4.2. dodanie możliwości przekazania dokumentu generowanego z szablonu pisma do obsługi w systemie digitalizacji

8.7.5.	w przypadku dokumentów opisanych w punkcie 8.7.4. umożliwieniu uzupełnienia dokumentu o dodatkowe dane wpisywane w formularzu systemu HIS Zamawiającego podczas generowania dokumentu
8.7.6.	umożliwieniu wygenerowania dokumentu z widoku Dokumentacji Medycznej w systemie HIS Zamawiającego dla konkretnego pacjenta
8.7.7.	wygenerowany dokument ma być jednoznacznie powiązany z pacjentem i kontekstem, w którym został utworzony
8.7.8.	umożliwieniu wskazania (rodzaju) urządzenia, na które dokument ma zostać przesłany celem podpisania przez pacjenta: 8.7.8.1. na stacji roboczej, z której generowany jest dokument w HIS Zamawiającego dla długopisów cyfrowych lub ekranów do podpisu, 8.7.8.2. na podstawie ręcznego wyboru urządzenia przez użytkownika z listy dla tabletów mobilnych. W tym celu System musi udostępnić HIS Zamawiającego interfejs sieciowy umożliwiający pobranie listy dostępnych w systemie urządzeń.
8.7.9.	Wskazanie urządzenia docelowego ma się odbywać za pośrednictwem słownika systemu HIS Zamawiającego
8.7.10.	wypełniony w systemie digitalizacji dokument ma zostać automatycznie udostępniony w widoku Dokumentacji Medycznej i powiązany z klasą dokumentu i szablonem pisma, z którego został wygenerowany
8.7.11.	umożliwieniu wskazania za pośrednictwem parametrów systemu HIS Zamawiającego, czy dokumenty tego samego typu generowane dla tego samego pacjenta mają być zapisywane jako nowy dokument czy kolejna wersja wcześniejszego dokumentu
8.7.12.	umożliwieniu uwierzytelnienia się w Systemie za pośrednictwem danych autoryzacyjnych użytkownika systemu HIS Zamawiającego, a w przypadku uruchomienia w jednostce Zamawiającego logowania domenowego, umożliwieniu uwierzytelnienia za pomocą danych autoryzacyjnych użytkownika domenowego
8.7.13.	umożliwieniu załączenia dokumentacji dostarczonej przez pacjenta w postaci papierowej i zeskanowanej za pomocą systemu digitalizacji do widoku Dokumentacja Medyczna z możliwością wskazania pacjenta i klasy dokumentu, do których zeskanowany dokument ma być powiązany, bezpośrednio w aplikacji stanowiącej część systemu digitalizacji

Wymagania w zakresie przygotowania szablonów wykorzystywanych do rozpoznawania treści na skanowanej dokumentacji pacjenta

Lp.	Wymagania minimalne
8.8.1.	W celu realizacji zamówienia Wykonawca zobowiązany będzie do przeprowadzenia analizy i przygotowania szablonów dla dokumentacji papierowej posiadanej obecnie przez Zamawiającego, w celu wprowadzenia ich do systemu digitalizacji, w pakiecie zawierającym maksymalnie 5 sztuk.
8.8.2.	Po przekazaniu przez Zamawiającego dokumentacji papierowej, dla której mają powstać szablony, Wykonawca ma obowiązek podjąć się jej analizy. W przypadku napotkania problemów z prawidłowym przygotowaniem szablonów dla przesłanej dokumentacji

	papierowej, Wykonawca zobowiązany jest do zgłoszenia uwag w tym zakresie do Zamawiającego. W przypadku dokumentów niemożliwych do oszablonowania wg uwag Wykonawcy, Zamawiający przewiduje możliwość wymiany dostarczonego dokumentu na inny lub akceptację wykonania przez Wykonawcę mniejszej liczby sztuk szablonów.
8.8.3.	W przypadku wymiany dokumentu niemożliwego do oszablonowania na inny, po dostarczeniu nowego dokumentu przez Zamawiającego, Wykonawca ma 5 dni roboczych na podjęcie się jego analizy.
8.8.4.	W przypadku braku zgłoszenia uwag przez Wykonawcę do dostarczonej przez Zamawiającego dokumentacji w ciągu 10 dni roboczych od ich dostarczenia Zamawiający przyjmuje, iż dostarczone dokumenty są możliwe do oszablonowania i wprowadzenia do systemu.
8.8.5.	Zamawiający zastrzega sobie prawo do dostarczenia w trakcie trwania wdrożenia mniejszej liczby dokumentów do oszablonowania niż wskazana w niniejszym opisie, w takiej sytuacji Wykonawca zobowiązany będzie do prawidłowego wprowadzenia dokumentacji formularzowej do systemu w trakcie trwania opieki serwisowej.

Wsparcie serwisowe Systemu

W ramach wsparcia serwisowego Systemu Wykonawca w okresie 36 miesięcy świadczyć będzie następujące usługi/ wykonywać będzie następujące prace:

Lp	Wymagania minimalne
8.9.1.	udostępnianie nowych wersji oprogramowania ,
8.9.2.	udostępnianie łatek i hotfixów zapewniających bezpieczeństwo działania Systemu,
8.9.3.	wykonywanie wymaganych prac programistycznych oraz konfiguracyjnych w przypadku awarii lub nieprawidłowego działania Systemu,
8.9.4.	świadczenie wsparcia technicznego w godzinach pracy serwisu,
8.9.5.	naprawa awarii, wad i usterek oprogramowania opisanych w tabeli Warunki brzegowe realizacji usług serwisowych,
8.9.6.	obsługa konsultacji opisanych w tabeli Warunki brzegowe realizacji usług serwisowych.

Warunki brzegowe realizacji usług serwisowych:
Wsparcie serwisowe musi być świadczone w dni robocze (od poniedziałku do piątku – oprócz dni ustawowo wolnych od pracy) w godzinach 08:00 – 16:00

Lp.	Minimalne warunki serwisu		Uwagi
8.9.7.	Reakcja serwisu	do 2h roboczych	Czas w godzinach liczony od chwili zaewidencjonowania w serwisie Zgłoszenia Serwisowego do momentu przyjęcia zgłoszenia tj. nadania mu statusu „przyjęte/ zarejestrowane” w godzinach pracy serwisu.
8.9.8.	Usunięcie awarii (błędu krytycznego) [1]	do 8h	Czas liczony w godzinach roboczych od upłynięcia czasu reakcji. Możliwe jest zaproponowanie tymczasowego obejścia błędu w wymaganym czasie 8h, pod warunkiem kontynuowania prac nad usunięciem awarii.
8.9.9.	Usunięcie wady aplikacji [2]	5 dni	Czas liczony w dniach roboczych od upłynięcia czasu reakcji

8.9.10.	Usunięcie wady programistycznej [3]	10 dni	Czas liczony w dniach roboczych od upłynięcia czasu reakcji
8.9.11.	Obsługa konsultacji [4]	10 dni	Czas liczony w dniach roboczych od upłynięcia czasu reakcji.

Objaśnienia oznaczeń w powyższej tabeli:

[1] przez awarię (błąd krytyczny) rozumiany jest błąd natury technicznej uniemożliwiający korzystanie z aplikacji i realizację procesu dla niej przewidzianego w pierwotnych założeniach aplikacji, wynikający z nieprawidłowego działania Wykonawcy w zakresie tworzenia lub konfiguracji i występujący w odosobnieniu od okoliczności, na które Wykonawca nie ma wpływu.

[2] przez wadę rozumiana jest niezgodność z pierwotnymi założeniami aplikacji, która nie mogła zostać wykryta w trakcie testów akceptacyjnych.

[3] przez usterkę rozumiany jest błąd w aplikacji wynikający z nieprawidłowego stworzenia kodu programistycznego w odniesieniu do pierwotnych założeń aplikacji, ale nie powodujący przerwania pracy, a stanowiący utrudnienie korzystania z aplikacji.

[4] dotyczy zgłoszeń i zapytań nie związanych z wystąpieniem błędu, a dotyczących zastosowania dodatkowych lub alternatywnych możliwości wykorzystania istniejących funkcji.

Wymagania dla oprogramowania

8.10.1. Wymagania ogólne – System do digitalizacji (dalej: System)

Lp.	Wymagania minimalne
8.10.1.1.	System musi umożliwiać pracę w odizolowanym środowisku na infrastrukturze Zamawiającego, bez dostępu do Internetu lub jakichkolwiek połączeń sieciowych poza infrastrukturę teleinformatyczną Zamawiającego
8.10.1.2.	System ma umożliwiać implementację nowych szablonów do Systemu poprzez import do aplikacji webowej uprzednio przygotowanego pliku, posiadającego informacje o polach (nazwy, współrzędne) opisujących dokument (np. skan). Szablon musi umożliwiać pozyskiwanie treści z dokumentów na podstawie zdefiniowanych współrzędnych lub opierając się na relacjach do treści zawartych w dokumencie (np. rozpoznanie PESELu pacjenta na podstawie odniesienia się/przesunięcia od wyszukanego słowa „PESEL").
8.10.1.3.	System musi posiadać Aplikację Centralną, dostępną z poziomu przeglądarki Internetowej, wymagającą logowania na konto użytkownika.
8.10.1.4.	System musi umożliwiać zarządzanie wersjami formularzy i szablonów w celu umożliwienia modyfikacji szablonu bez zmian konfiguracji powiązanych systemów lub narzędzi. System musi umożliwiać tworzenie dowolnej liczby wersji danego szablonu z oznaczeniem aktualnie obowiązującej wersji.
8.10.1.5.	Repozytorium dokumentów: 8.10.1.5.1. System musi posiadać wbudowane mechanizmy zapisywania, przechowywania i katalogowania dokumentów w ramach Systemu, 8.10.1.5.2. System musi umożliwiać samodzielne tworzenie, usuwanie i zmianę nazwy katalogów i podkatalogów możliwych do przeglądania z poziomu Aplikacji Centralnej.

	8.10.1.5.3. System musi umożliwiać przenoszenie dokumentów pomiędzy katalogami oraz definiowanie domyślnych katalogów zapisu dokumentów. 8.10.1.5.4. System musi umożliwiać samodzielną konfigurację struktury danych, która prezentuje dokumenty w postaci rekordów zbudowanych na podstawie danych zawartych w dokumentach. To znaczy, że jeżeli w określonych polach dokumentów znajdują się określone wartości, to System automatycznie utworzy nowy rekord i zapisze w nim dokumenty lub przypisze dokumenty do istniejącego rekordu zawierającego te dane.
8.10.1.6.	System musi umożliwiać zarządzanie podłączonymi do Systemu stanowiskami, w podziale na typ urządzenia, aktualny status komunikacji. Aplikacja Centralna musi ponadto umożliwiać przegląd ostatnich zdarzeń na stanowisku oraz możliwość zdalnej zmiany konfiguracji w celu zarządzania stanowiskami.
8.10.1.7.	System musi udostępniać panel administracyjny dostępny z poziomu Aplikacji Centralnej.
8.10.1.8.	System musi umożliwiać tworzenie kont użytkowników i zarządzanie nimi z poziomu panelu administracyjnego.
8.10.1.9.	Integracje: 8.10.1.9.1. System musi umożliwiać otwartą integrację z systemami zewnętrznymi za pomocą API w technologii REST. 8.10.1.9.2. System umożliwia wysłanie do podpisu dokumentu za pośrednictwem funkcjonalności wirtualnej drukarki. W przypadku braku dostosowania dokumentów do pracy z systemem, aplikacja obsługująca wirtualną drukarkę powinna umożliwiać ręczne wskazanie lokalizacji pól podpisu. 8.10.1.9.3. System musi pozwalać na przesłanie do podpisu dowolnego dokumentu w formacie PDF oraz ukrycie niezbędnych informacji o dokumencie, w szczególności o polach podpisu, w samej treści dokumentu – bez konieczności obsługi tych informacji w zapytaniu integracyjnym. 8.10.1.9.4. System musi umożliwiać cofnięcie autoryzacji dla danej integracji w celu zabezpieczenia przed wyciekiem. 8.10.1.9.5. System musi posiadać funkcjonalność ustawiania automatycznych powiadomień o podpisaniu dokumentu na wskazany webservice w celu umożliwienia integracji bez konieczności wykonania prac po stronie Wykonawcy.

8.10.2. Wymagania związane z urządzeniami

Skaner:

Lp	Wymagania minimalne
8.10.2.1.	Możliwość uruchomienia aplikacji Systemu na dowolnym komputerze z systemem operacyjnym Windows 10/11, wersja 64-bitowa
8.10.2.2.	System musi umożliwiać automatyczne skanowanie dokumentów z możliwością opatrzenia tych skanów podpisem cyfrowym - kwalifikowanym, niekwalifikowanym i osobistym (e-Dowód).

8.10.2.3.	System musi umożliwiać lokalne zapisywanie dokumentów zeskanowanych, a w przypadku automatycznego rozpoznania danych, automatyczne nadanie plikom nazwy i hasła dostępu do nich na podstawie szablonu nazewnictwa.
8.10.2.4.	System musi umożliwiać pobieranie bezpośrednio z dokumentu danych opisujących dokument
8.10.2.5.	System musi umożliwiać regulację stopnia kompresji plików.
8.10.2.6.	System musi umożliwiać przed rozpoczęciem skanowania ustawienie dzielenia skanowanych dokumentów co wybraną liczbę stron.
8.10.2.7.	System musi posiadać funkcjonalność optycznego rozpoznawania znaków (OCR) bez limitów rozpoznawanych dokumentów.
8.10.2.8.	System musi umożliwiać automatyczne uzupełnianie kolejnych danych w polach dokumentu na podstawie takich samych danych wcześniej poprawnie wprowadzonych w szablonie.
8.10.2.9.	System musi mieć funkcje dzielenia kompletów dokumentów skanowanych seryjnie z automatycznego podajnika dokumentów urządzenia skanującego.
8.10.2.10.	System musi posiadać wbudowaną wyszukiwarkę dokumentów.
8.10.2.11.	System musi umożliwiać weryfikację poprawności rozpoznanych lub wprowadzonych danych przed ich zatwierdzeniem.
8.10.2.12.	System musi wymagać uwierzytelnienia (zalogowania) użytkownika.
8.10.2.13.	System musi umożliwiać zapisywanie wersji roboczych nieprzetworzonych dokumentów zeskanowanych w celu powrotu do pracy nad nimi po uruchomieniu kolejnej sesji.
8.10.2.14.	System musi umożliwiać rozpoznawanie danych bezpośrednio ze skanowanego dokumentu na podstawie informacji zawartych w szablonach zaimplementowanych uprzednio do Systemu. W szczególności należy umieścić współrzędne pól takich jak tytuł dokumentu oraz pól niezbędnych do identyfikacji osoby, której dokument dotyczy, celem przesłania go do systemu.
8.10.2.15.	System musi posiadać funkcjonalność dzielenia dokumentów według szablonów i automatycznego dołączania do nich dowolnej ilości stron niebędących szablonami.
8.10.2.16.	System musi umożliwiać ustawienie domyślnego szablonu skanowania, który będzie automatycznie wskazywany w sytuacji, gdy nie będzie możliwe rozpoznanie szablonu dla skanowanego dokumentu.
8.10.2.17.	System musi umożliwiać współpracę z urządzeniami skanującymi działającymi za pośrednictwem protokołu TWAIN.
8.10.2.18.	Skanowanie i zarządzanie dokumentami zeskanowanymi przed wysłaniem ich do systemu HIS, musi odbywać się w aplikacji będącej częścią systemu zainstalowanej na stacji roboczej podłączonej do skanera

Prawo weryfikacji oferowanego rozwiązania

Zamawiający zastrzega sobie prawo do wezwania Wykonawcy, którego oferta została najwyżej oceniona, do przedstawienia i zaprezentowania oferowanego rozwiązania (w całości lub w części), celem przeprowadzenia weryfikacji zgodności z wymaganiami określonymi w Opisie Przedmiotu Zamówienia (OPZ).

Weryfikacja ta może obejmować m.in. demonstrację funkcjonalności, dostęp do środowiska testowego, dokumentację techniczną lub inne środki pozwalające na rzetelną ocenę zgodności rozwiązania z wymaganiami Zamawiającego. Brak możliwości wykazania zgodności może skutkować odrzuceniem oferty jako niezgodnej z OPZ.

Wymagane oświadczenia

Zamawiający żąda złożenia przez Wykonawcę wraz z ofertą oświadczenia producenta systemu HIS posiadanego przez Zamawiającego, w celu potwierdzenia, że integracja między systemem Wykonawcy, a systemem HIS posiadanym przez Zamawiającego spełnia zakres funkcji zgodny z punktem 7 niniejszego dokumentu.

II.9 Rozbudowa i integracja systemu szpitalnego o możliwość elektronicznego podpisu dokumentów za pomocą urządzeń do zbierania podpisu oraz czytników e-Dowodów wraz z wymaganymi licencjami i sprzętem.

Ogólny opis

Przedmiotem zamówienia jest dostawa i wdrożenie systemu do automatycznej digitalizacji dokumentacji (dalej: System). System ma umożliwiać digitalizację pisma odręcznego.

Zakres prac

W ramach zamówienia Wykonawca zobowiązany jest do:

Lp	Wymagania minimalne
9.2.1.	Przeprowadzenia analizy przedwdrożeniowej.
9.2.2.	Dostawy sprzętu umożliwiającego wykonanie funkcjonalności Systemu – długopisy cyfrowe (22 sztuki), ekrany (10 sztuk), uchwyty do ekranów montowane do ściany (5 sztuk), uchwyty typu „Z” (5 sztuk), czytnik e-dowodu (3 sztuki)
9.2.3.	Dostawy licencji na system w liczbie sztuk 32.
9.2.4.	Instalacji i wdrożenia systemu automatycznej digitalizacji dokumentacji wraz z integracją z posiadanym środowiskiem systemu Medycznego HIS AMMS w jednostce Zamawiającego.
9.2.5.	Przeprowadzenia odpowiednich szkoleń w zakresie administrowania i użytkowania Systemu.
9.2.6.	Przygotowanie dokumentacji formularzowej.
9.2.7.	Świadczenia opieki serwisowej wraz z nadzorem autorskim dla wszystkich przekazywanych licencji na System przez okres 36 miesięcy od daty zakończenia wdrożenia

Analiza przedwdrożeniowa

Na potrzebę realizacji zamówienia Wykonawca, przeprowadzi analizę przedwdrożeniową w placówce Zamawiającego. Wykonawca wraz z Zamawiającym dokonają wizji lokalnej stanowisk, które zostaną zaproponowane przez Zamawiającego w ramach wdrożenia.

Wynikiem analizy ma być raport przekazany Zamawiającemu przez Wykonawcę w terminie 3 dni roboczych od zakończenia analizy. Raport powinien wskazywać niezbędne do wykonania przez Zamawiającego zmiany w infrastrukturze placówki celem sprawnego wdrożenia zamawianego rozwiązania.

Zamawiający zastrzega, że Wykonawca nie ma prawa do samodzielnej ingerencji w infrastrukturę placówki.

Zamawiający zastrzega, że w przypadku zasugerowania zmian niemających krytycznego wpływu na proces wdrożenia i uruchomienia Systemu, Zamawiający nie ma obowiązku ich wprowadzenia. Jednocześnie nie może przełożyć się to na opóźnienia w realizacji prac zleconych dla Wykonawcy. W zakresie zmian krytycznych dla wdrożenia Wykonawca zobowiązany jest do ich wyraźnego wskazania w raporcie.

Wymagania dotyczące sprzętu

Lp.	Typ sprzętu	Charakterystyka (wymagania minimalne)
9.4.1.	**Długopis cyfrowy**	9.4.1.1. Pamięć długopisu powinna wystarczyć na co najmniej 1000 wypełnionych stron A4 zanim będzie potrzeba jego synchronizacji i przesłania danych do Systemu. 9.4.1.2. Długopis cyfrowy musi posiadać czułość co najmniej 250 poziomów nacisku. 9.4.1.3. Długopis powinien mieć wbudowany akumulator litowo-jonowy lub litowo-polimerowy i umożliwiać ładowanie przez port USB. 9.4.1.4. Maksymalny czas pełnego ładowania nie może przekraczać 2,5 godziny. 9.4.1.5. Minimalny czas ciągłego pisania nie może być krótszy niż 5 godzin. 9.4.1.6. Waga długopisu cyfrowego nie może przekroczyć 35g. 9.4.1.7. Długopis powinien wytrzymać upadek na dowolną powierzchnię z wysokości maksimum 1,5m. 9.4.1.8. Długopis cyfrowy powinien zostać dostarczony ze stacją dokującą umożliwiającą ładowanie oraz komunikację ze stacją roboczą. 9.4.1.9. Przesłanie danych do Systemu powinno być możliwe za pomocą portu USB 2.0. 9.4.1.10. Zamawiający wymaga 24 miesięcznej gwarancji na długopis liczonej od momentu dostarczenia sprzętu. Wykonawca ponosi koszty napraw gwarancyjnych wraz z kosztami części i transportu. 9.4.1.11. Serwis obejmuje wymianę sprzętu na nowy w razie zaistnienia takiej konieczności
9.4.2.	**Ekran do podpisu - dotykowy**	9.4.2.1. Ekran powinien posiadać rozdzielczość min. Full HD (1920x1080) i przekątną co najmniej 13 cali. 9.4.2.2. Ekran powinien być podłączany do komputera za pomocą portów USB-C. 9.4.2.3. Ekran nie powinien przekraczać wymiarów 34cmx23cmx1,5cm 9.4.2.4. Ekran nie powinien przekraczać wagi 950g.

		9.4.2.5. Rysik dołączony do ekranu powinien posiadać czułość co najmniej 4000 poziomów nacisku 9.4.2.6. Dedykowany rysik do ekranu powinien mieć możliwość przymocowania go na stałe, jednocześnie, w razie awarii samego rysika, umożliwiając jego wymianę. 9.4.2.7. Zamawiający wymaga 36 miesięcznej gwarancji na ekran liczonej od momentu dostarczenia sprzętu. Wykonawca ponosi koszty napraw gwarancyjnych wraz z kosztami części i transportu.

Minimalne warunki licencji na system

Lp	Wymagania minimalne
9.5.1.	Z chwilą dostarczenia danego rozwiązania lub jego części dla Zamawiającego, Wykonawca udzieli (z chwilą dostarczenia, bez konieczności składania dodatkowych oświadczeń woli) niewyłącznej licencji na takie rozwiązanie, na czas nieokreślony od daty podpisania przez Zamawiającego końcowego protokołu odbioru bez uwag i zastrzeżeń, na następujących polach eksploatacji: 9.5.1.1.wprowadzanie do pamięci komputera, 9.5.1.2.korzystanie, 9.5.1.3.sporządzanie kopii zapasowej, 9.5.1.4. przenoszenie pomiędzy stanowiskami.
9.5.2.	Zamawiający w ramach udzielonej licencji uprawniony będzie do korzystania z wygenerowanych za pomocą danego rozwiązania dokumentów (np. raportów, analiz) w szczególności poprzez: 9.5.2.1. opracowanie, w tym zmianę, adaptację, tłumaczenie, 9.5.2.2. utrwalanie lub zwielokrotnianie w całości lub w części jakimikolwiek środkami i w jakiejkolwiek formie, niezależnie od formatu, systemu lub standardu, w tym techniką drukarską, techniką reprograficzną, techniką cyfrową lub poprzez wprowadzanie do pamięci komputera, 9.5.2.3. publiczne rozpowszechnianie, w tym: wyświetlanie, odtwarzanie w dowolnym systemie lub stan-dardzie, a także publiczne udostępnianie w taki sposób, aby każdy mógł mieć do nich dostęp w miejscu i czasie przez siebie wybranym, 9.5.2.4. wprowadzanie do sieci multimedialnych oraz Internetu, 9.5.2.5. umieszczanie w publikacjach drukowanych (w tym m.in. ulotki, foldery, plakaty), 9.5.2.6. umieszczanie w publikacjach elektronicznych oraz aplikacjach elektronicznych, 9.5.2.7. umieszczanie w prezentacjach i materiałach prasowych, 9.5.2.8. umieszczania w spotach i filmach reklamowych.
9.5.3.	Licencja, o której mowa w ust. 1 i 2 uprawnia Zamawiającego do korzystania z rozwiązania na terytorium Rzeczypospolitej Polskiej.
9.5.4.	Zamawiający może wykonywać wszelkie prawa przyznane w ramach licencji również przy udziale, za pośrednictwem lub przy pomocy osób trzecich świadczących usługi na rzecz Zamawiającego, w tym w szczególności profesjonalnych doradców, konsultantów, zleceniobiorców oraz innych osób współpracujących z Zamawiającym.

9.5.5.	Zamawiający nie będzie mieć prawa przenosić licencji na inne osoby, przy czym wyjątkiem jest zmiana formy prawnej lub zmiany struktury właścicielskiej Zamawiającego, która wyłączona jest spod zapisów tego ustępu.
9.5.6.	Wykonawca składając ofertę oświadcza, iż: 9.5.6.1. przysługują mu wszelkie prawa do przedmiotów własności intelektualnej oferowanych w ramach postępowania oraz prawa te nie są w żaden sposób obciążone prawami osób trzecich; lub 9.5.6.2. przysługują mu prawa do sprzedaży sublicencji na przedmiot własności intelektualnej oferowanej w ramach postępowania oraz prawa te nie są w żaden sposób obciążone prawami osób trzecich; oraz 9.5.6.3. udzielenie licencji zgodnie z ofertą, jak również korzystanie przez Zamawiającego z przedmiotów własności intelektualnej zaoferowanych przez Wykonawcę nie będzie stanowić naruszenia praw osób trzecich.
9.5.7.	Zamawiający gwarantuje parametry ujęte w postępowaniu, a Wykonawca zobowiązany jest do dostarczenia pozostałych elementów niezbędnych do poprawnego wdrożenia rozwiązania.

Licencja integracyjna HIS

Lp	Wymagania minimalne
9.6.1.	Wykonawca składając ofertę oświadcza, iż w zakresie integracji oferowanego Systemu z systemem HIS Zamawiającego: 9.6.1.1. przysługują mu wszelkie prawa do przedmiotów własności intelektualnej oferowanych w ramach postępowania oraz prawa te nie są w żaden sposób obciążone prawami osób trzecich; 9.6.1.2. lub przysługują mu prawa do sprzedaży sublicencji na przedmiot własności intelektualnej oferowanej w ramach postępowania oraz prawa te nie są w żaden sposób obciążone prawami osób trzecich; 9.6.1.3. oraz udzielenie licencji zgodnie z ofertą, jak również korzystanie przez Zamawiającego z przedmiotów własności intelektualnej zaoferowanych przez Wykonawcę nie będzie stanowić naruszenia praw osób trzecich.
9.6.2.	Oferta Wykonawcy nie przewiduje konieczności uiszczenia dodatkowych opłat za uruchomienie Systemu w integracji z HIS koniecznych do poniesienia przez Zamawiającego na rzecz dostawcy HIS.
9.6.3.	Po upływie 12 miesięcy od wdrożenia, tj. podpisana protokołu odbioru końcowego bez uwag, opłaty należne dostawcy systemu HIS Zamawiającego za wsparcie modułu integracyjnego między Systemem HIS Zamawiającego a dostarczanym przez Wykonawcę Systemem ponosi Zamawiający.
9.6.4.	Zamawiający podkreśla, iż nie dysponuje kodami źródłowymi do systemu HIS Zamawiającego. Wykonawca w ramach realizacji prac zobowiązywany będzie do samodzielnego kontaktu z dostawcą HIS Zamawiającego i zapewnienia wykonania wszelkich prac integracyjnych zarówno od strony dostarczanego Systemu, jak i dostawcy HIS.

Opcjonalny

Lp	Wymagania minimalne
9.7.1.	W ramach realizacji przedmiotu zamówienie Wykonawca zobowiązany jest do przeprowadzenia wdrożenia systemu w następującym zakresie: 9.7.1.1. przysługują a) instalacja oprogramowania na maszynie wirtualnej w infrastrukturze sieciowej Zamawiającego; 9.7.1.2. rozmieszczenie dostarczanych sprzętów na stanowiskach roboczych wskazanych przez Zamawiającego; 9.7.1.3. instalacja na wskazanych stanowiskach, o których mowa w podpunkcie b, oprogramowania niezbędnego do poprawnej pracy systemu lub dostarczenie zestawu instalatorów wymaganych do przeprowadzenia instalacji domenowej; 9.7.1.4. konfiguracja i parametryzacja dostarczonego oprogramowania do współpracy z dostarczonym sprzętem; 9.7.1.5. w porozumieniu z dostawcą systemu dziedzinowego HIS uruchomienie integracji między systemem HIS a dostarczanym systemem; 9.7.1.6. przekazanie Zamawiającemu zestawu zmiennych i parametrów wymaganych do poprawnego działania integracji między systemem HIS a dostarczanym systemem; 9.7.1.7. przeprowadzenie szkoleń z zakresu działania systemu dla użytkowników systemu (personelu medycznego); 9.7.1.8. przeprowadzenie szkoleń z zakresu administrowania infrastrukturą i konfiguracją systemu dla administratorów szpitala; 9.7.1.9. dostarczenie dokumentacji powdrożeniowej.
9.7.2.	Zamawiający zastrzega sobie prawo do wskazania Wykonawcy w trakcie trwania wdrożenia mniejszej liczby stanowisk do instalacji i konfiguracji niż liczba dostarczonego przez Wykonawcę sprzętu i przeprowadzenia odbioru końcowego z uwzględnieniem powyższej zmiany. Wykonawca będzie zobowiązany do przeprowadzenia instalacji i konfiguracji pozostałych stanowisk w ramach świadczenia opieki serwisowej. Zamawiający uzgodni z Wykonawcą szczegółowy harmonogram instalacji i konfiguracji poza okresem wdrożenia, przy czym czas wykonania instalacji i konfiguracji nie może być dłuższy niż 20 dni roboczych od przekazania Wykonawcy informacji o zleceniu realizacji zadania.
9.7.3.	Szkolenia dla użytkowników systemu zostaną przeprowadzone w trybie: • szkoleń audytoryjnych przeprowadzonych w grupach; i/lub • szkoleń stanowiskowych - na każdym z zainstalowanych i skonfigurowanych stanowisk Wykonawca przeprowadzi szkolenie dla personelu szpitala obsługującego dane stanowisko w dwóch różnych terminach; • szkoleń dla administratorów szpitala z zakresu administrowania infrastrukturą i konfiguracją; • zamawiający przewiduje konieczność przeszkolenia około 95 osób; dokładna liczba osób do przeszkolenia zostanie przekazana Wykonawcy w terminie do 10 dni od zawarcia umowy. 9.7.3.1. Wykonawca jest zobowiązany do umożliwienia każdemu uczestnikowi szkolenia aktywnego uczestnictwa w szkoleniu polegającego na indywidualnym przejściu całego procesu związanego z wygenerowaniem dokumentu z systemu, podpisaniem dokumentu i zapisaniem dokumentu w systemie.

	9.7.3.2. Wykonawca jest zobowiązany do uzyskania i udostępnienia Zamawiającemu potwierdzenia uczestnictwa od każdego z uczestników szkoleń. 9.7.3.3. Szkolenia mają być przeprowadzone w placówce Zamawiającego w dni robocze w godzinach od 8:00 do 15:00. Zamawiający zastrzega sobie prawo do zmiany trybu przeprowadzania szkoleń na formę zdalną za pośrednictwem telekonferencji w przypadku występowania w placówce sytuacji epidemiologicznej uniemożliwiającej przeprowadzenie szkoleń stacjonarnych. 9.7.3.4. Wykonawca przekaże Zamawiającemu materiały instruktażowe w postaci filmów instruktażowych lub instrukcji stanowiskowych, umożliwiających wykonanie samodzielnego szkolenia dla personelu szpitala. 9.7.3.5. Zamawiający zastrzega sobie prawo do zorganizowania szkoleń dla części personelu szpitala w terminie wykraczającym poza okres trwania prac wdrożeniowych i przeprowadzenia odbioru końcowego z uwzględnieniem powyższej zmiany. Wykonawca będzie zobowiązany do przeprowadzenia pozostałych szkoleń w ramach świadczenia opieki serwisowej. Zamawiający uzgodni z Wykonawcą szczegółowy harmonogram szkoleń poza okresem wdrożenia, przy czym czas przeprowadzenia szkoleń nie może być dłuższy niż 30 dni roboczych od przekazania Wykonawcy informacji o zleceniu realizacji zadania. 9.7.3.6. Wykonawca jest zobowiązany przedstawić Zamawiającemu propozycję szczegółowego harmonogramu szkoleń nie później niż na 3 dni robocze przed planowanym rozpoczęciem szkoleń. 9.7.3.7. Wykonawca jest zobowiązany do uwzględnienia uwag przekazanych przez Zamawiającego, a w przypadku braku takiej możliwości, do przedstawienia nowej propozycji harmonogramu szkoleń w terminie maksymalnie 2 dni roboczych od przekazania uwag.
9.7.4.	Wykonawca przekaże Zamawiającemu Dokumentację powdrożeniową po zakończeniu wszystkich prac wdrożeniowych aktualną na dzień odbioru końcowego. Dokumentacja powdrożeniowa ma obejmować: 9.7.4.1. raport z wykonanych prac wdrożeniowych 9.7.4.2. zestawienie personelu uczestniczącego w szkoleniach 9.7.4.3. instrukcję obsługi systemu 9.7.4.4. wykaz zmiennych i parametrów ustawionych dla systemu 9.7.4.5. informacje na temat dostępnego sposobu zgłaszania awarii i usterek w działaniu systemu 9.7.4.6. wykaz procedur wymaganych dla poprawnego działania systemu, które administrator systemu szpitalnego ma przeprowadzać na serwerze i dostarczonym systemie

Integracja systemu z działającym w placówce systemem HIS

W ramach realizacji przedmiotu zamówienia Wykonawca zobowiązany jest w porozumieniu z dostawcą systemu HIS AMMS do przeprowadzenia modyfikacji systemu w szczególności polegających na:

Lp	Wymagania minimalne

9.8.1.	umożliwieniu dodawania szablonów dokumentów mających podlegać integracji za pomocą edytora będącego częścią dostarczanego systemu
9.8.2.	umożliwieniu umieszczania w polach aktywnych dokumentu powstałego z szablonu opisanego w pkt. a) treści związanych z danymi pacjenta oraz danymi jednostki organizacyjnej szpitala pobieranych z systemu AMMS
9.8.3.	umożliwieniu powiązania dowolnej klasy dokumentacji z systemu AMMS z szablonem opisanym w pkt. a)
9.8.4.	umożliwieniu dostosowania istniejących szablonów pism w systemie AMMS do obsługi w systemie digitalizacji poprzez: 9.8.4.1. umieszczenie w pliku szablonu pisma znaczników pól aktywnych takich jak pola podpisu, pola tekstowe, pola wyboru 9.8.4.2. dodanie możliwości przekazania dokumentu generowanego z szablonu pisma do obsługi w systemie digitalizacji
9.8.5.	w przypadku dokumentów opisanych w punkcie d) umożliwieniu uzupełnienia dokumentu o dodatkowe dane wpisywane w formularzu systemu AMMS podczas generowania dokumentu
9.8.6.	umożliwieniu wygenerowania dokumentu z widoku Dokumentacji Medycznej w systemie HIS AMMS dla konkretnego pacjenta
9.8.7.	wygenerowany dokument ma być jednoznacznie powiązany z pacjentem i kontekstem, w którym został utworzony
9.8.8.	umożliwieniu wskazania (rodzaju) urządzenia, na które dokument ma zostać przesłany celem podpisania przez pacjenta: 9.8.8.1. na stacji roboczej, z której generowany jest dokument w HIS AMMS dla długopisów cyfrowych lub ekranów do podpisu, 9.8.8.2. na podstawie ręcznego wyboru urządzenia przez użytkownika z listy dla tabletów mobilnych. W tym celu System musi udostępnić HIS AMMS interfejs sieciowy umożliwiający pobranie listy dostępnych w systemie urządzeń.
9.8.9.	Wskazanie urządzenia docelowego ma się odbywać za pośrednictwem słownika systemu AMMS
9.8.10.	wypełniony w systemie digitalizacji dokument ma zostać automatycznie udostępniony w widoku Dokumentacji Medycznej i powiązany z klasą dokumentu i szablonem pisma, z którego został wygenerowany
9.8.11.	umożliwieniu wskazania za pośrednictwem parametrów systemu AMMS, czy dokumenty tego samego typu generowane dla tego samego pacjenta mają być zapisywane jako nowy dokument czy kolejna wersja wcześniejszego dokumentu
9.8.12.	umożliwieniu uwierzytelnienia się w Systemie za pośrednictwem danych autoryzacyjnych użytkownika systemu HIS – AMMS, a w przypadku uruchomienia w jednostce Zamawiającego logowania domenowego, umożliwieniu uwierzytelnienia za pomocą danych autoryzacyjnych użytkownika domenowego

Wymagania w zakresie przygotowania dokumentacji formularzowej podpisywanej odręcznie przez pacjenta

Lp	Wymagania minimalne
9.9.1.	W celu realizacji zamówienia Wykonawca zobowiązany będzie do przeprowadzenia analizy i przygotowania dokumentacji formularzowej podpisywanej odręcznie przez pacjenta, wykorzystywanej obecnie przez Zamawiającego, w celu wprowadzenia jej do systemu digitalizacji, w pakiecie zawierającym maksymalnie 150 sztuk.

9.9.2.	Po przekazaniu przez Zamawiającego dokumentacji formularzowej, Wykonawca ma obowiązek podjąć się jej analizy i przygotowania. W przypadku napotkania problemów z prawidłowym wprowadzeniem dokumentacji formularzowej do systemu wynikającej z typów dokumentów dostarczonych przez Zamawiającego, Wykonawca zobowiązany jest do zgłoszenia uwag w tym zakresie do Zamawiającego. W przypadku dokumentów niemożliwych do przerobienia wg uwag Wykonawcy, Zamawiający przewiduje możliwość wymiany dostarczonego formularza na inny lub akceptację wykonania przez Wykonawcę mniejszej liczby sztuk dokumentacji formularzowej.
9.9.3.	W przypadku wymiany dokumentu niemożliwego do wprowadzenia do systemu na inny, po dostarczeniu nowego typu formularza przez Zamawiającego, Wykonawca ma 5 dni roboczych na podjęcie się analizy nowego formularza.
9.9.4.	W przypadku braku zgłoszenia uwag przez Wykonawcę do dokumentacji formularzowej dostarczonej przez Zamawiającego w ciągu 10 dni roboczych od ich dostarczenia Zamawiający przyjmuje, iż dostarczone formularze możliwe są do wprowadzenia do systemu.
9.9.5.	Zamawiający zastrzega sobie prawo do dostarczenia w trakcie trwania wdrożenia mniejszej liczby formularzy niż wskazana w niniejszym opisie, w takiej sytuacji Wykonawca zobowiązany będzie do prawidłowego wprowadzenia dokumentacji formularzowej do systemu w trakcie trwania opieki serwisowej.

Wsparcie serwisowe systemu

W ramach wsparcia serwisowego Systemu Wykonawca w okresie 36 miesięcy świadczyć będzie następujące usługi/ wykonywać będzie następujące prace:

Lp	Wymagania minimalne
9.10.1.	udostępnianie nowych wersji oprogramowania ,
9.10.2.	udostępnianie łatek i hotfixów zapewniających bezpieczeństwo działania Systemu,
9.10.3.	wykonywanie wymaganych prac programistycznych oraz konfiguracyjnych w przypadku awarii lub nieprawidłowego działania Systemu,
9.10.4.	świadczenie wsparcia technicznego w godzinach pracy serwisu,
9.10.5.	naprawa awarii, wad i usterek oprogramowania opisanych w tabeli Warunki brzegowe realizacji usług serwisowych,
9.10.6.	obsługa konsultacji opisanych w tabeli Warunki brzegowe realizacji usług serwisowych.

Warunki brzegowe realizacji usług serwisowych:
Wsparcie serwisowe musi być świadczone w dni robocze (od poniedziałku do piątku – oprócz dni ustawowo wolnych od pracy) w godzinach 08:00 – 16:00

Lp.	Minimalne warunki serwisu		Uwagi
9.10.7.	Reakcja serwisu	do 2h roboczych	Czas w godzinach liczony od chwili zaewidencjonowania w serwisie Zgłoszenia Serwisowego do momentu przyjęcia zgłoszenia tj. nadania mu statusu „przyjęte/ zarejestrowane” w godzinach pracy serwisu.

9.10.8.	Usunięcie awarii (błędu krytycznego) [1]	do 8h	Czas liczony w godzinach roboczych od upłynięcia czasu reakcji. Możliwe jest zaproponowanie tymczasowego obejścia błędu w wymaganym czasie 8h, pod warunkiem kontynuowania prac nad usunięciem awarii.
9.10.9.	Usunięcie wady aplikacji [2]	5 dni	Czas liczony w dniach roboczych od upłynięcia czasu reakcji
9.10.10.	Usunięcie wady programistycznej [3]	10 dni	Czas liczony w dniach roboczych od upłynięcia czasu reakcji
9.10.11.	Obsługa konsultacji [4]	10 dni	Czas liczony w dniach roboczych od upłynięcia czasu reakcji.

Objaśnienia oznaczeń w powyższej tabeli:

[1] przez awarię (błąd krytyczny) rozumiany jest błąd natury technicznej uniemożliwiający korzystanie z aplikacji i realizację procesu dla niej przewidzianego w pierwotnych założeniach aplikacji, wynikający z nieprawidłowego działania Wykonawcy w zakresie tworzenia lub konfiguracji i występujący w odosobnieniu od okoliczności, na które Wykonawca nie ma wpływu.

[2] przez wadę rozumiana jest niezgodność z pierwotnymi założeniami aplikacji, która nie mogła zostać wykryta w trakcie testów akceptacyjnych.

[3] przez usterkę rozumiany jest błąd w aplikacji wynikający z nieprawidłowego stworzenia kodu programistycznego w odniesieniu do pierwotnych założeń aplikacji, ale nie powodujący przerwania pracy, a stanowiący utrudnienie korzystania z aplikacji.

[4] dotyczy zgłoszeń i zapytań nie związanych z wystąpieniem błędu, a dotyczących zastosowania dodatkowych lub alternatywnych możliwości wykorzystania istniejących funkcji.

Wynagania dla oprogramowania

9.11.1. Wymagania ogólne – System do digitalizacji (dalej: System)

Lp	Wymagania minimalne
9.11.1.1.	System musi umożliwiać pracę w odizolowanym środowisku na infrastrukturze Zamawiającego, bez dostępu do Internetu lub jakichkolwiek połączeń sieciowych poza infrastrukturę teleinformatyczną Zamawiającego
9.11.1.2.	System musi umożliwiać współpracę z różnymi urządzeniami do digitalizacji dokumentów dostępnymi na rynku – ekranami piórkowymi dedykowanymi do składania podpisów kontekstowych, tabletami mobilnymi, długopisami cyfrowymi, skanerami dokumentacji. W ramach Systemu, Zamawiający ma mieć możliwość doboru kompatybilnych urządzeń dobranych do aktualnych potrzeb, bez wprowadzania przez Wykonawcę zmian w oprogramowaniu (z wyłączeniem niezbędnych aktualizacji).
9.11.1.3.	System musi posiadać Aplikację Centralną, dostępną z poziomu przeglądarki Internetowej, wymagającą logowania na konto użytkownika.
9.11.1.4.	System ma umożliwiać implementację nowych formularzy do Systemu poprzez import do aplikacji edytora (będącej elementem Systemu) tła dokumentu w postaci PDF (tzn. obrazu niezmiennej części dokumentu), a następnie naniesienie na tło regionów aktywnych, które mogą być edytowalne w celu personalizacji powstających dokumentów. Utworzone w ten sposób regiony powinny znaleźć się w wynikowym pliku PDF i być zgodne ze specyfikacją

	formatu PDF (w szczególności umożliwiać kompatybilność z popularnymi przeglądarkami plików PDF, np. Adobe Reader).
9.11.1.5.	System musi umożliwiać obsługę innych plików PDF niezdefiniowanych wcześniej w Systemie.
9.11.1.6.	System musi umożliwiać zarządzanie wersjami formularzy w celu umożliwienia modyfikacji szablonu bez zmian konfiguracji powiązanych systemów lub narzędzi. System musi umożliwiać tworzenie dowolnej liczby wersji danego formularza z oznaczeniem aktualnie obowiązującej wersji.
9.11.1.7.	Repozytorium dokumentów: 9.11.1.7.1. System musi posiadać wbudowane mechanizmy zapisywania, przechowywania i katalogowania dokumentów w ramach Systemu, 9.11.1.7.2. System musi umożliwiać samodzielne tworzenie, usuwanie i zmianę nazwy katalogów i podkatalogów możliwych do przeglądania z poziomu Aplikacji Centralnej. 9.11.1.7.3. System musi umożliwiać przenoszenie dokumentów pomiędzy katalogami oraz definiowanie domyślnych katalogów zapisu dokumentów. 9.11.1.7.4. System musi umożliwiać samodzielną konfigurację struktury danych, która prezentuje dokumenty w postaci rekordów zbudowanych na podstawie danych zawartych w dokumentach. To znaczy, że jeżeli w określonych polach dokumentów znajdują się określone wartości, to System automatycznie utworzy nowy rekord i zapisze w nim dokumenty lub przypisze dokumenty do istniejącego rekordu zawierającego te dane.
9.11.1.8.	System musi umożliwiać zarządzanie podłączonymi do Systemu stanowiskami, w podziale na typ urządzenia, aktualny status komunikacji. Aplikacja Centralna musi ponadto umożliwiać przegląd ostatnich zdarzeń na stanowisku oraz możliwość zdalnej zmiany konfiguracji w celu zarządzania stanowiskami.
9.11.1.9.	System musi umożliwiać śledzenie statusu podpisywania poszczególnych dokumentów.
9.11.1.10.	System musi umożliwiać nakładanie w polach podpisu pieczątek konfigurowalnych w Systemie.
9.11.1.11.	System musi udostępniać panel administracyjny dostępny z poziomu Aplikacji Centralnej.
9.11.1.12.	System musi umożliwiać tworzenie kont użytkowników i zarządzanie nimi z poziomu panelu administracyjnego.
9.11.1.13.	Integracje: 9.11.1.13.1. System musi umożliwiać otwartą integrację z systemami zewnętrznymi za pomocą API w technologii REST. 9.11.1.13.2. System umożliwia wysłanie do podpisu dokumentu za pośrednictwem funkcjonalności wirtualnej drukarki. W przypadku braku dostosowania dokumentów do pracy z systemem, aplikacja obsługująca wirtualną drukarkę powinna umożliwiać ręczne wskazanie lokalizacji pól podpisu. 9.11.1.13.3. System musi pozwalać na przesłanie do podpisu dowolnego dokumentu w formacie PDF oraz ukrycie niezbędnych informacji o dokumencie, w szczególności o polach podpisu, w samej treści dokumentu – bez konieczności obsługi tych informacji w zapytaniu integracyjnym. 9.11.1.13.4. System musi umożliwiać cofnięcie autoryzacji dla danej integracji w celu zabezpieczenia przed wyciekiem.

	9.11.1.13.5. System musi posiadać funkcjonalność ustawiania automatycznych powiadomień o podpisaniu dokumentu na wskazany webservice w celu umożliwienia integracji bez konieczności wykonania prac po stronie Wykonawcy.
9.11.1.14.	Podpisy: 9.11.1.14.1. System zapewnia użytkownikowi zrozumiały proces składania podpisu odręcznego, tzn. podpis składany jest zawsze w kontekście dokumentu „tak jak na papierze". Podpis odręczny nie może być składany na odrębnym urządzeniu, które nie wyświetla jednocześnie dokumentu, ani w odrębnym wyskakującym oknie aplikacji. 9.11.1.14.2. System umożliwia składanie pisma odręcznego na dokumentach również poza polami podpisu, w celu umożliwienia digitalizacji dowolnej treści, również takiej, która nie została wcześniej zdefiniowana na poziomie wzoru formularza. 9.11.1.14.3. System powinien umożliwiać opatrzenie dokumentów elektronicznym podpisem odręcznym (biometrycznym). System powinien gromadzić informacje takie jak siła nacisku czy znaczniki czasowe umożliwiające weryfikację autentyczności podpisu. 9.11.1.14.4. System niezależnie powinien umożliwiać opatrzenie dokumentów podpisem osobistym z e-Dowodu.

9.11.2. Wymagania związane z urządzeniami

9.11.2.1. Ekran do podpisu

Lp	Wymagania minimalne
9.11.2.1.1.	Możliwość uruchomienia aplikacji Systemu na dowolnym komputerze z systemem operacyjnym Windows 10/11, wersja 64-bitowa
9.11.2.1.2.	Dedykowany ekran powinien być na stałe połączony z komputerem, aby umożliwiać digitalizację dokumentu w czasie rzeczywistym.
9.11.2.1.3.	System umożliwia prezentację na ekranie treści multimedialnych, gdy ten nie jest wykorzystywany do wyświetlania i podpisywania dokumentu. Konfiguracja wyświetlanych treści powinna odbywać się z poziomu panelu administracyjnego w Aplikacji Centralnej.
9.11.2.1.4.	System umożliwia uzupełnianie, zaznaczanie, wypełnianie i edycję pól aktywnych (tekstowych, zaznaczalnych, wyboru) w trakcie podpisywania dokumentu.
9.11.2.1.5.	System umożliwia utrzymywanie aktywnego połączenia aplikacji obsługującej ekran z serwerem, tak aby wywołanie dokumentu do podpisu nie wymagało aktywności użytkownika w aplikacji.
9.11.2.1.6.	System powinien mieć funkcję powiększania, zmniejszania i przesuwania wyświetlanego formularza, gdyby ten był nieczytelny.
9.11.2.1.7.	System powinien zapewniać operatorowi Systemu możliwość podglądu i kontroli przebiegu podpisywania na własnym monitorze (synchronizacja widoków).
9.11.2.1.8.	System musi umożliwiać zalogowanie wielu użytkowników do jednej aplikacji z możliwością przełączania się pomiędzy ich kontami.

9.11.2.2. Długopis cyfrowy

Lp	Wymagania minimalne
9.11.2.2.1.	System powinien umożliwiać uruchomienie aplikacji do obsługi długopisu cyfrowego na dowolnym komputerze z systemem operacyjnym Windows 10/11, wersja 64-bitowa
9.11.2.2.2.	System powinien umożliwiać odwzorowanie formularza papierowego w wersji elektronicznej w wersji 1:1.
9.11.2.2.3.	System powinien umożliwiać wygenerowanie formularza w taki sposób, aby każdy wydrukowany formularz był unikatowy. Oznacza to, że wypełnienie papierowego formularza długopisem cyfrowym, tworzy wzajemnie jednoznacznie przyporządkowaną do niego wersję elektroniczną dokumentu.
9.11.2.2.4.	System powinien umożliwiać podgląd danych pochodzących bezpośrednio z urządzeń przez wysłaniem dokumentu do repozytorium.
9.11.2.2.5.	System powinien umożliwiać automatyczny wydruk dokumentów przeznaczonych do obsługi długopisem cyfrowym, bez konieczności ingerencji ze strony użytkownika Systemu.
9.11.2.2.6.	System powinien umożliwiać zbieranie danych na formularzach papierowych niezależnie od infrastruktury informatycznej (zbieranie danych off-line)
9.11.2.2.7.	System nie może pozwalać na odtworzenie danych z długopisu cyfrowego bez zgrania danych i zalogowania się do systemu.
9.11.2.2.8.	Odręczny podpis wykonany długopisem cyfrowym powinien być przechowywany w Systemie jako grafika oraz informacje zawierające cechy biometryczne.
9.11.2.2.9.	Wydruk formularza dopasowanego do długopisu cyfrowego musi umożliwiać standardowa drukarka laserowa o parametrach minimalnych:

Prawo weryfikacji oferowanego rozwiązania

Zamawiający zastrzega sobie prawo do wezwania Wykonawcy, którego oferta została najwyżej oceniona, do przedstawienia i zaprezentowania oferowanego rozwiązania (w całości lub w części), celem przeprowadzenia weryfikacji zgodności z wymaganiami określonymi w Opisie Przedmiotu Zamówienia (OPZ).

Weryfikacja ta może obejmować m.in. demonstrację funkcjonalności, dostęp do środowiska testowego, dokumentację techniczną lub inne środki pozwalające na rzetelną ocenę zgodności rozwiązania z wymaganiami Zamawiającego. Brak możliwości wykazania zgodności może skutkować odrzuceniem oferty jako niezgodnej z OPZ.

Wymagane oświadczenia

Zamawiający żąda złożenia przez Wykonawcę wraz z ofertą oświadczenia producenta systemu HIS posiadanego przez Zamawiającego, w celu potwierdzenia, że integracja między systemem Wykonawcy, a systemem HIS posiadanym przez Zamawiającego spełnia zakres funkcji zgodny z punktem 8 niniejszego dokumentu.

II.10 Zakup systemu EDR (Endpoint Detection and Response)

Stan obecny

Zamawiający posiada i użytkuje oprogramowanie Bitdefender GravityZone Business Security, które jest rozwiązaniem bezpieczeństwa klasy korporacyjnej (endpoint protection) dla firm chroniącym komputery, serwery i inne urządzenia przed złośliwym oprogramowaniem, ransomware, atakami sieciowymi itd.

Ogólny opis

Przedmiotem zamówienia jest rozbudowa posiadanego oprogramowania lub zakup nowego systemu klasy EDR (Endpoint Detection and Response) do ochrony stacji roboczych i serwerów + urządzenia mobilne + serwer Exchange + środowisko wirtualne + konsola do zarządzania dla 400 aktywnych użytkowników oraz zapewnienie okresu wsparcia przez okres 36 miesięcy od dnia dostarczenia systemu.

Wymagania dotyczące systemu

Lp.	Wymagania minimalne
Wymagania systemowe	
10.3.1.	Systemy operacyjne komputerów: • Windows 11 October 2024 Update (24H2) • Windows 11 October 2023 Update (23h2) • Windows 10 November 2022 Update (22H2) • Windows 11 September 2022 Update (22H2) • Windows 11 (initial release) • Windows 10 November 2021 Update (21H2) • Windows 10 May 2021 Update (21H1) • Windows 10 October 2020 Update (20H2) • Windows 10 May 2020 Update (20H1) • Windows 10 May 2019 Update (19H1) • Windows 10 October 2018 Update (Redstone 5) • Windows 10 April 2018 Update (Redstone 4) • Windows 10 Fall Creators Update (Redstone 3) • Windows 10 Creators Update (Redstone 2) • Windows 10 Anniversary Update (Redstone 1) • Windows 10 November Update (Threshold 2) • Windows 10 (initial release)
10.3.2.	Windows Tablet oraz systemy wbudowane: • Windows 10 IoT Enterprise • Windows Embedded 8.1 Industry • Windows Embedded 8 Standard
10.3.3.	Systemy operacyjne serwera: • Windows Server 2025 64x • Windows Server 2022 Core

	• Windows Server 2022 • Windows Server 2019 Core • Windows Server 2019 • Windows Server 2016 • Windows Server 2016 Core • Windows Server 2012 R2 • Windows Server 2012 • Windows Small Business Server (SBS) 2011 • Windows Server 2008 R2
10.3.4.	Systemy operacyjne Linux i wersja kernel: 10.3.4.1. Oparte o RPM • RHEL 7.x - 3.10.0 (build 957) 64-bit • RHEL 8.x - 4.18.0 64-bit • RHEL 9.x - 5.14.0 64-bit • Oracle Linux 7.x (UEK) - 4.18.0 64-bit • Oracle Linux 7.x (RHCK) - 3.10.0 build 957 64-bit • Oracle Linux 8.x (UEK) - 5.4.17 / 5.15.0 64-bit • Oracle Linux 8.x (RHCK) – 4.18.0 64-bit • Oracle Linux 9.x (UEK) – 5.15.0 64-bit • Oracle Linux 9.x (RHCK) – 5.14.0 64-bit • CentOS 7.x - 3.10.0 (build 957) 32-bit/64-bit • CentOS 8 Stream - 4.18.0 64-bit • CentOS 9 Stream - 5.14.0 64-bit • Fedora 37 – 40 – wsparcie do wygaśnięcia. 64-bit • AlmaLinux 8.x - 4.18.0 64-bit • AlmaLinux 9.x - 5.14.0 64-bit • Rocky Linux 8.x - 4.18.0 64-bit • Rocky Linux 9.x - 5.14.0 64-bit • CloudLinux 7.x - 3.10 (build 957) 64-bit • CloudLinux 8.x - 4.18.0 64-bit • Miracle Linux 8.x - 4.18.0 64-bit • Kylinv10 RHEL - 4.19.90 64-bit 10.3.4.2. Oparte o Debian • Debian 9 - 4.9.0 32-bit/64-bit • Debian 10 - 4.19 32-bit/64-bit • Debian 11 - 5.10 32-bit/64-bit • Debian 12 – 6.1.0 64-bit • Ubuntu 16.04.x - 4.8 / 4.10 / 4.13 / 4.15 32-bit/64-bit • Ubuntu 18.04.x - 5.0 / 5.3 / 5.4 64-bit • Ubuntu 20.04.x - 5.4 / 5.8 / 5.11 / 5.13 / 5.15 64-bit • Ubuntu 22.04.x - 5.15 / 5.19 64-bit • Ubuntu 23.04.x – 6.2.0 64-bit • Ubuntu 24.04.x – 6.8.0 64- bit • PopOS 22.04.x – 6.2.6 64-bit

	• Pardus 21 – 5.10.0 64-bit • Mint 20.x – 5.4.0 64-bit • Mint 21.x – 5.15.0 64-bit • Mint 22.x – 6.8.0.x 64-bit • Zorin OS – 6.5.x 64-bit • Linux Mint Debian Edition 6 – 6.1.x 64-bit 10.3.4.3. Oparte o SUSE • SLES 12 SP4 - 4.12.14-x 64-bit • SLES 12 SP5 - 4.12.14-x 64-bit • SLES 15 SP1 - 4.12.14-x 64-bit • SLES 15 SP2 - 5.3.18-x 64-bit • SLES 15 SP3 - 5.3.18-x 64-bit • SLES 15 SP4 – 5.14.21 64-bit • SLES 15 SP5 – 5.14.21 64-bit • SLES 15 SP6 – 6.4.x 64-bit • SLED 15 SP4 – 5.14.21 64-bit • openSUSE Leap 15.4 - 15.5 - 5.14.21 64-bit
10.3.5.	Obsługiwane środowiska Microsoft Exchange: • Exchange Server 2019 z rolą Edge Transport lub Mailbox • Exchange Server 2016 z rolą Edge Transport lub Mailbox
10.3.6.	Ochrona środowisk wirtualnych (SVE): 10.3.6.1. Możliwość zastosowania zewnętrznego silnika skanującego w postaci maszyny wirtualnej. 10.3.6.2. Maszyna wirtualna pełniąca rolę silnika skanującego może być pobrana w formacie: • OVA • XVA • VHD • VHDX • VMDK 10.3.6.3. Środowiska wspierane: • VMware vSphere and vCenter Server: ➢ version 7.0, including update 1, update 2, update 2b, update 2c and update 2d ➢ version 8.0, including update 1, update 2 • VMware Horizon/View 7.8, 7.7, 7.6, 7.5, 7.1, 6.x, 5.x • VMware Workstation 11.x, 10.x, 9.x, 8.0.6 • VMware Player 7.x, 6.x, 5.x • Citrix Xen Hypervisor: 8.4. • Citrix Virtual Apps and Desktops 7 1808, 7 1811, 7 1903, 7 1906 • Citrix XenApp and XenDesktop 7.18, 7.17, 7.16, 7.15 LTSR, 7.6 LTSR • Citrix VDI-in-a-Box 5.x • Microsoft Hyper-V Server 2008 R2, 2012, 2012 R2, 2016, 2019 or Windows Server 2008 R2, 2012, 2012 R2, 2016, 2019 (including Hyper-V Hypervisor), 2022, 2025 • Red Hat Enterprise Virtualization 3.0 (including KVM Hypervisor) • Oracle VM 3.0

	• Oracle VM VirtualBox 5.2, 5.1 • Nutanix Prism with AOS 5.6, 5.5, 5.20 LTS, 5.18 STS, 5.15 LTS, 5.11, 5.10 (Enterprise Edition) • Nutanix Prism with AHV 20170830.115, 20170830.301, 20170830.395 and 20190916.294 (Community Edition)
Ochrona antywirusowa i antyspyware	
10.3.7.	Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
10.3.8.	Interfejs oraz pomoc techniczna świadczona w języku polskim.
10.3.9.	Wykrywanie zagrożeń i analiza procesów technikami heurystycznymi.
10.3.10.	Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.
10.3.11.	Wbudowana technologia do ochrony przed rootkitami.
10.3.12.	Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
10.3.13.	Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie".
10.3.14.	Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
10.3.15.	Możliwość ustawienia zadania skanowania z niskim priorytetem zmniejszając obciążenie systemu w trakcie wykonywania tego procesu.
10.3.16.	Możliwość skanowania dysków sieciowych i dysków przenośnych.
10.3.17.	Skanowanie plików spakowanych i skompresowanych.
10.3.18.	Ochrona krytycznych kluczy rejestru przed ich wykorzystaniem lub nieautoryzowanym dostępem do nich.
10.3.19.	Możliwość dodawania wykluczeń na podstawie: • Plik • Folder • Rozszerzenie • Proces • Hash pliku • Hash certyfikatu • Nazwa zagrożenia • Wiersz poleceń • IP/maska
10.3.20.	Skanowanie poczty opartej o protokoły IMAP, MAPI, POP3 i SMTP w czasie rzeczywistym.
10.3.21.	Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany, a użytkownikowi wyświetlane jest stosowne powiadomienie w przeglądarce.
10.3.22.	Blokowanie możliwości przeglądania wybranych stron internetowych. Listę blokowanych stron internetowych określa administrator. Dodatkowo zdefiniowane są grupy stron przez producenta.
10.3.23.	Wsparcie przeglądarek Internet Explorer 8+, Mozilla Firefox 30+, Google Chrome 34+, Safari 4+, Microsoft Edge 20+ i Opera 21+ bez konieczności zmian w konfiguracji.

10.3.24.	Program powinien umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, RDP, FTPS, SCP/SSH, IMAPS, MAPI, POP3S, SMTPS.
10.3.25.	Program powinien skanować ruch HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe.
10.3.26.	W GUI programu na punkcie końcowym z systemem Windows oraz macOS możliwość wyświetlenia aktualnej wersji produktu i aktualnej wersji silników.
10.3.27.	W GUI programu na punkcie końcowym z systemem Windows oraz macOS możliwość wyświetlenia, kiedy była przeprowadzana ostatnia aktualizacja z dokładnością co do dnia i godziny.
10.3.28.	Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń.
10.3.29.	Obsługa pobierania aktualizacji za pośrednictwem serwera proxy.
10.3.30.	Administrator musi mieć możliwość ukrycia ikony oprogramowania w obszarze powiadomień systemu Windows.
10.3.31.	Dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji baz wirusów i samego oprogramowania bezpośrednio na punkcie końcowym Windows i macOS.
10.3.32.	Stacje robocze mogą łączyć się do serwera administracyjnego za pośrednictwem sieci Internet.
10.3.33.	Oprogramowanie klienckie posiada wbudowaną funkcję do komunikacji z serwerem administracyjnym, ale nie dopuszcza się osobnego agenta instalowanego na stacji roboczej.
10.3.34.	System musi umożliwiać kontrolę dostępu do urządzeń na podstawie interfejsów, do których zostały one podłączone.
10.3.35.	Możliwość dodania zaufanych urządzeń bezpośrednio z konsoli administracyjnej na podstawie ich wykrycia lub wpisanych ręcznie ID urządzenia lub ID produktu.
10.3.36.	Funkcja blokowania informacji wysyłanych przez HTTP lub SMTP jak: (adresy e-mail, Piny, Konta bankowe, hasła itp.).
10.3.37.	Funkcja blokowania wysyłanych informacji konfigurowana zdalnie przez administratora.
10.3.38.	Wbudowana zapora osobista, umożliwiająca tworzenie reguł na podstawie aplikacji oraz ruchu sieciowego.
10.3.39.	Wbudowany IDS.
10.3.40.	Możliwość wykorzystania funkcji skanowania lokalnego lub hybrydowego ze sprawdzaniem reputacji plików w chmurze.
10.3.41.	Możliwość tworzenia list sieci zaufanych.
10.3.42.	Możliwość dezaktywacji funkcji zapory sieciowej.
10.3.43.	Dodatkowa funkcja ochrony przeciwko znanym zagrożeniom typu ransomware.
10.3.44.	Użytkownik na punkcie końcowym ma możliwość opóźnienia restartu potrzebnego do zakończenia jednego lub wielu zadań (konfigurowalne w politykach bezpieczeństwa).
10.3.45.	Komunikacja między konsolą zarządzającą, a punktami końcowymi jest szyfrowana.
10.3.46.	Wbudowana ochrona przed exploitami wyposażona w minimum 15 różnych technik wykrycia exploitów z możliwością włączenia lub wyłączenia każdej z nich oraz dająca możliwość dodania własnych procesów. Funkcja umożliwia również:
10.3.47.	Możliwość wymuszenia funkcji DEP systemu Windows.

10.3.48.	Możliwość wymuszenia relokacji modułów (ASLR) dla Windows.
10.3.49.	Ochrona przed atakami sieciowymi – Mechanizm obronny przed atakującymi próbującymi uzyskać dostęp do systemu poprzez wykorzystanie luk w sieci. Funkcja ta musi obejmować ochronę przed technikami takimi jak: • Pierwszy dostęp. • Dostęp do poświadczeń. • Wykrycie. • Crimeware. • Ruch boczny.
10.3.50.	Ochrona przed ransomware - możliwość wykrywania i blokowania ataków typu ransomware niezależnie od tego czy atak został przeprowadzony lokalnie lub zdalnie na punkcie końcowym oraz utworzenie kopii zapasowej plików w momencie szyfrowania, a w przypadku ataku odzyskanie i przywrócenie ich do pierwotnej lokalizacji. Oprogramowanie musi dać możliwość odzyskania plików na żądanie lub automatycznie, o następujących rozszerzeniach: 3fr, ai, arw, bay, cdr, cer, cr2, crt, crw, dcr, der, dll, dng, doc, docm, docx, dwg, dxf, dxg, eps, erf, exe, indd, jpe, jpeg, jpg, mdf, mef, mrw, nef, nrw, odb, odc, odm, odp, ods, odt, orf, p12, p7b, p7c, pdd, pdf, pef, pem, pfx, ppt, pptm, pptx, psd, pst, ptx, png, r3d, raf, rtf, rw2, rwl, sr2, srf, srw, wb2, wpd, wps, x3f, xlk, xls, xlsb, xlsm, xlsx, msg, py, ini, xml, msi, cab, tsf, dgn, log, gif, csv, avi, mov, mp4
10.3.51.	System musi wykrywać podatne sterowniki zainstalowane na punkcie końcowym z Windows i Linux.
10.3.52.	Agent i usługi oprogramowania antywirusowego zainstalowanego na punkcie końcowym muszą być chronione przed próbami manipulacji i naruszenia ich integralności w systemie Windows.
10.3.53.	Oprogramowanie musi skanować nośniki USB zanim użytkownik zaloguje się do systemu Windows.
10.3.54.	System musi umożliwiać skanowanie oprogramowania układowego UEFI.
10.3.55.	System umożliwia przechwytywanie TLS handshake pozwalając na skanowanie ruchu sieciowego bez konieczności deszyfracji.
10.3.56.	Telemetria - Możliwość przesyłania nieprzetworzonych danych bezpieczeństwa z punktów końcowych z systemem operacyjnym Windows i macOS do SIEM Splunk (wymaga TLS 1.2 lub wyższy) lub z systemem Windows i Linux do serwera Syslog (JSON).
10.3.57.	Oprogramowanie pozwala na skanowanie punktów końcowych pod kątem wyszukiwania wskaźników naruszeń bezpieczeństwa (IOC).
Stacje robocze i serwery	
10.3.58.	Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
10.3.59.	Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.
10.3.60.	Jedna wersja instalacyjna na stacje robocze i serwery plików Windows.
10.3.61.	Oprogramowanie zawiera monitor antywirusowy uruchamiany automatycznie w momencie startu systemu operacyjnego komputera, który działa nieprzerwanie do momentu zamknięcia systemu operacyjnego.

10.3.62.	Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet gdy posiada ona prawa lokalnego lub domenowego administratora, przy próbie deinstalacji program powinien pytać o hasło.
10.3.63.	Produkt i zawartość zabezpieczeń powinny być aktualizowane nie rzadziej niż raz na godzinę.
10.3.64.	Oprogramowanie posiada możliwość raportowania zdarzeń informacyjnych.
10.3.65.	Oprogramowanie musi posiadać możliwość włączenia/wyłączenia powiadomień określonego rodzaju.
10.3.66.	Oprogramowanie musi posiadać możliwość skanowania jedynie nowych i zmienionych plików.
10.3.67.	Oprogramowanie posiada możliwość odblokowania ustawień lokalnych konfiguracji na systemach Windows po doinstalowaniu odpowiedniego modułu. Zmiana ustawień zabezpieczona jest hasłem.
10.3.68.	Po kliknięciu prawym klawiszem myszy na ikonie programu i wybraniu opcji „O programie”, możliwość wyświetlenia danych do pomocy technicznej tj: adres strony pomocy, adres e-mail do administratora ochrony, numer telefonu do administratora ochrony z wyłączeniem systemów Linux.
10.3.69.	Dla maszyn z systemem Linux możliwość wskazania katalogów, które mogą być chronione w czasie rzeczywistym.
Ochrona Exchange	
10.3.70.	Rozwiązanie musi zapewniać filtrowanie antymalware dla przychodzącego, wewnętrznego i wychodzącego ruchu mailowego.
10.3.71.	Rozwiązanie musi wspierać skanowanie "na życzenie" oraz skanowanie według harmonogramu dla skrzynek pocztowych i folderów publicznych, w tym możliwość zarówno wykluczenia konkretnych skrzynek bądź folderów publicznych, jak i skanowania tylko emaili z załącznikami bądź emaili otrzymanych w ciągu określonego czasu.
10.3.72.	Zdolność konfigurowania różnych akcji wykonywanych na plikach zainfekowanych, podejrzanych oraz niemożliwych do przeskanowania.
10.3.73.	Możliwość skanowania w poszukiwaniu potencjalnie niechcianych aplikacji (PUA).
10.3.74.	Możliwość skanowania malware wewnątrz archiwów.
10.3.75.	Rozwiązanie musi zapewniać filtr antyspamowy dla ruchu mailowego, z możliwością dodania do białej listy konkretnych adresów email i domen.
10.3.76.	Możliwość odpytania serwerów Realtime Blackhole List (RBL) zdefiniowanych przez administratorów i odfiltrowania wiadomości zaklasyfikowanych jako spam bazując na reputacji wysyłającego serwera.
10.3.77.	Zdolność automatycznego oznaczenia jako spam wiadomości mailowych napisanych przy użyciu alfabetów azjatyckich bądź cyrylicy.
10.3.78.	Zdolność do wykonania zapytań bazujących na chmurze dla udoskonalonej ochrony przeciw nowemu spamowi.
10.3.79.	Zdolność do podjęcia różnych akcji na wykrytych mailach ze spamem, takich jak poprzedzanie tematu maila konkretną etykietą, usunięcie, przeniesienie do kwarantanny bądź przekierowanie maila do konkretnej skrzynki pocztowej.

10.3.80.	Rozwiązanie musi zapewniać funkcjonalności filtrowania zawartości dla przychodzącego, wewnętrznego i wychodzącego ruchu mailowego, bazujące na konkretnym tekście bądź wyrażeniach regularnych zgodnych z tematem maila i/lub jego zawartością.
10.3.81.	Zdolność do podejmowania różnych akcji na emailach, pasujących do reguł filtrowania treści, takich jak dodawanie prefiksu w postaci taga do tematu maila, usuwanie, wysyłanie do kwarantanny bądź przekierowywanie emaila do konkretnej skrzynki.
Konsola zdalnej administracji	
10.3.82.	System musi umożliwiać centralne zarządzanie i konfigurację ochrony wspieranych stacji roboczych i serwerów.
10.3.83.	Możliwość integracji wielu domen Active Directory.
10.3.84.	Możliwość uruchomienia zdalnego skanowania wybranych punktów końcowych.
10.3.85.	Możliwość sprawdzenia z centralnej konsoli zarządzającej stanu ochrony punktu końcowego (aktualnych ustawień programu, wersji programu i bazy wirusów, wyników skanowania na żądanie, zainstalowanych modułów, ostatniej aktualizacji oraz przypisanej polityki).
10.3.86.	Możliwość utworzenia konta użytkownika z rolą administrator firmy, administrator sieci, analityk bezpieczeństwa lub z ustawieniami niestandardowymi.
10.3.87.	Możliwość sprawdzenia z centralnej konsoli zarządzającej podstawowych informacji dotyczących stacji roboczej: adresów IP, systemu operacyjnego.
10.3.88.	Możliwość centralnej aktualizacji punktów końcowych z serwera w sieci lokalnej lub z Internetu.
10.3.89.	Możliwość wysłania linku instalacyjnego bezpośrednio z poziomu konsoli administracyjnej.
10.3.90.	Możliwość uruchomienia centralnej konsoli jedynie z poziomu przeglądarki internetowej.
10.3.91.	Możliwość ręcznego (na żądanie) i automatycznego generowania raportów (według ustalonego harmonogramu) oraz wyeksportowanie ich do formatu: pdf i csv. Również zbiorczo w formie archiwum zip.
10.3.92.	Raport generowany według harmonogramu z możliwością automatycznego wysłania go do osób zdefiniowanych w tym raporcie.
10.3.93.	Możliwość generowania raportu co godzinę.
10.3.94.	Pierwsza aktywacja modułu kontroli urządzeń nie wymaga restartu stacji docelowej.
10.3.95.	Możliwość dodania etykiety do stacji roboczej.
10.3.96.	Możliwość dezinstalacji oprogramowania antywirusowego innych firm w trakcie instalacji zdalnej.
10.3.97.	Możliwość przechowywania kwarantanny maksymalnie 180 dni.
10.3.98.	Możliwość definiowania, czy pliki z kwarantanny mają być przesyłane do producenta i co ile godzin ma się ta czynność odbywać.
10.3.99.	Po aktualizacji zawartości bezpieczeństwa opcja automatycznego przeskanowania kwarantanny.
10.3.100.	Wsparcie techniczne mailowe i telefoniczne w j. polskim od poniedziałku do piątku w godzinach 8:00-16:00. W pozostałych godzinach możliwość bezpośredniego kontaktu z producentem (24/7) w j. angielskim.
10.3.101.	Po integracji z lokalnym Active Directory możliwość przypisywania polityk automatycznie po zalogowaniu do systemu operacyjnego w zależności od tego jaki użytkownik domenowy się zalogował lub do jakiej grupy domenowej on należy.

10.3.102.	Możliwość automatycznego przypisywania polityk na podstawie reguły lokalizacji. Określenie lokalizacji na podstawie: • Zakres adresów IP/IP. • Adres bramy. • Adres serwera WINS. • Adres serwera DNS. • Połączenie DHCP sufiksów DNS. • Punkt końcowy może rozwiązać hosta. • Typ sieci. • Nazwa hosta.
10.3.103.	Uwierzytelnienie dwuskładnikowe realizowane przy pomocy aplikacji kompatybilnej ze standardem RFC6238.
10.3.104.	Możliwość naprawy instalacji agenta z poziomu konsoli.
10.3.105.	Możliwość utworzenia reguły, która będzie usuwała punkty końcowe z konsoli zarządzającej, jeżeli punkt końcowy nie połączył się z konsolą przez określoną liczbę dni. Funkcja ta pozwala również na określenie wzoru nazw maszyn, które automatycznie będą usuwane oraz na określenie godziny, o której te maszyny będą usuwane.
10.3.106.	Możliwość wyświetlania adresu MAC dołączonego do nazwy hosta.
10.3.107.	Możliwość wyświetlenia czy punkt końcowy jest serwerem czy stacją roboczą.
10.3.108.	Możliwość wyświetlenia informacji czy zainstalowany na punkcie końcowym system operacyjny to Windows, Linux lub MacOS.
10.3.109.	Możliwość filtrowania punktów końcowych, które były online w ciągu ostatnich 24 godzin, 7 lub 30 dni.
10.3.110.	Menu tworzenia paczek instalacyjnych musi określać czy dany moduł jest dostępny dla stacji roboczych Windows, Serwerów Windows, Linux, MacOS.
10.3.111.	Oprogramowanie umożliwia pobranie oddzielnego pakietu instalacyjnego dla systemów MacOS z Intel x86 oraz oddzielnego dla Apple M oraz osobnego pakietu dla systemów Windows z Intel x86 oraz oddzielnego dla architektury ARM.
10.3.112.	System umożliwia pobieranie plików poddanych kwarantannie z poziomu centralnej konsoli administracyjnej.
10.3.113.	Możliwość wygenerowania i zapisania logów na stacji roboczej z poziomu konsoli zarządzającej.
10.3.114.	Możliwość zarządzania ochroną na serwerach Exchange, tworzenie polityk i konfiguracji zdalnej ochrony.
10.3.115.	Znaczniki punktów końcowych – oprogramowanie musi umożliwiać przypisywanie znaczników (tagów) do punktów końcowych. Przypisywanie musi odbywać się ręcznie lub automatycznie. Musi istnieć możliwość filtrowania punktów końcowych na podstawie kilku wybranych znaczników w jednym czasie.
10.3.116.	Ochrona proaktywna oparta o maszynowe uczenie, która działa w fazie poprzedzającej wykonanie. Ochrona ta musi wykrywać zagrożenia takie jak: • Ukierunkowane ataki. • Podejrzane pliki i ruch w sieci. • Exploity. • Ransomware.

	• Grayware.
10.3.117.	Moduł ochrony proaktywnej musi posiadać oddzielne działania jakie będzie podejmował dla plików i oddzielne dla ruchu sieciowego.
10.3.118.	Moduł ochrony proaktywnej musi działać w trybach, które administrator może dowolnie zmieniać na: • Tolerancyjny. • Normalny. • Agresywny.
10.3.119.	Zintegrowany sandbox po stronie producenta, który pozwala na analizę pliku: • Plik może zostać wysłany automatycznie ze stacji roboczej, jeżeli oprogramowanie uzna go za podejrzany lub ręcznie z poziomu konsoli przez administratora. • Możliwość ręcznego przesłania archiwum zabezpieczonego hasłem. • Możliwość ręcznego przesłania adresu URL. • W przypadku ręcznego przesłania wielu plików jednorazowo, możliwość detonacji próbek pojedynczo.
10.3.120.	Wbudowany sandbox musi działać w trybie monitorowania i blokowania.
10.3.121.	Wbudowany sandbox musi oferować działania naprawcze takie jak dezynfekcja, przeniesienie do kwarantanny lub tylko raportowanie.
10.3.122.	Wbudowany sandbox musi oferować opcję wstępnego filtrowania plików z kategorii aplikacje, dokumenty, skrypty, archiwa, maile zapisane do pliku, pod kątem podejrzanego zachowania.
10.3.123.	Wbudowany sandbox musi posiadać opcję, która pozwala na dodanie określonych rozszerzeń do wyjątków, pliki z tym rozszerzeniem nie zostaną przesłane do sandboxa.
10.3.124.	Minimalny rozmiar pliku jaki może zostać automatycznie przesłany do sandboxa to 1KB.
10.3.125.	Maksymalny rozmiar pliku jaki może zostać automatycznie przesłany do sandboxa to 50MB.
10.3.126.	System zarządzania ryzykiem – Zintegrowany z konsolą zarządzającą system, który pozwala oszacować podatność środowiska na atak na podstawie punktów ryzyka. Punkty ryzyka powinny być przydzielane od 0 do 100, gdzie liczba mniejsza stanowi mniejsze ryzyko, a liczba większa większe ryzyko. System ponadto musi posiadać: • Funkcję, która pozwala wyszukiwać podatności ustawień punktów końcowych oraz naprawiać je lub ignorować z podziałem na typ wykrytej konfiguracji: ➢ Przeglądarka ➢ Sieć ➢ System operacyjny ➢ Luki System ponadto musi określać nasilenie zagrożenia wynikłego z wykrytej podatności w oparciu o punkty procentowe oraz posiadać funkcję cofnięcia wprowadzonych zmian w ustawieniach systemów. • System zarządzania ryzykiem powinien określać luki w wykrytym zainstalowanym oprogramowaniu podając przy tym numer CVE tych luk. • System pozwala na śledzenie i wykrywanie ryzykownych działań jakie podejmuje użytkownik na punkcie końcowym wraz z poinformowaniem o liczbie użytkowników, których takie działanie dotyczy oraz jaka jest jego szkodliwość.

	• System pozwala na skanowanie punktów końcowych pod kątem wykrywania ryzyka na podstawie harmonogramu lub pojedynczo utworzonego zadania. • System pozwala na raportowanie na ilu urządzeniach wykryto błędną konfigurację i luki w aplikacjach oraz jaka jest ilość takich podatności i ich szkodliwość wyrażona w procentach. • System pozwala na wykrywanie podatności w oparciu o standardy bezpieczeństwa zgodne z: CISv8, SOC 2, ISO/IEC 27001:2022, GDPR (EU), NIS2 (EU) oraz DORA (EU). • System musi mieć możliwość określenia, które konkretnie zapisy standardów bezpieczeństwa: CISv8, SOC 2, ISO/IEC 27001:2022, GDPR (EU), NIS2 (EU) oraz DORA (EU) nie są spełnione w wyniku wykrytej błędnej konfiguracji.
10.3.127.	Możliwość scentralizowanego podglądu wykrytych zagrożeń z wszystkich modułów ochrony w jednym miejscu i odfiltrowania ich według daty, kategorii, typu zagrożenia, działań naprawczych i innych.
10.3.128.	Możliwość ustawienia wymagania zmiany hasła logowania do konsoli co 90 dni.
10.3.129.	Możliwość zablokowania konta w konsoli, jeżeli użytkownik tego konta podejmował pięć kolejnych prób logowania nieprawidłowym hasłem.
10.3.130.	Funkcja pojedynczego logowania – Single Sign-on (SSO) przy integracji z Microsoft Azure.
10.3.131.	Raport podsumowujący - Możliwość podglądu raportu, który streszcza stan środowiska firmowego w ciągu ostatnich 24h, 7 dni lub 30 dni. Z rozróżnieniem na takie sekcje jak: • Zarządzane punkty końcowe. • Ilość zajętych miejsc w licencji z rozróżnieniem na stacje robocze Windows, serwery Windows, macOS, Linux oraz fizyczne punkty końcowe i maszyny wirtualne. • Pięć rodzajów najczęściej blokowanych zagrożeń. • Podział zagrożeń na urządzenia takie jak stacje robocze i serwery. • Status incydentów bezpieczeństwa, które wystąpiły. • Stan modułów punktów końcowych. • Ocena ryzyka firmy. • Zablokowane strony WWW w oparciu o wykryte tam szkodliwe oprogramowanie, phishing, oszustwa. • Zablokowane techniki ataku sieciowego z podziałem na takie jak wczesny dostęp, dostęp do poświadczeń, wykrycie, ruch boczny, crimeware.
10.3.132.	Możliwość integracji z innymi systemami poprzez API takich elementów bądź sekcji jak: Firmy • Raporty • Licencjonowanie • Konta • Pakiety • Incydenty • Sieć • Kwarantanna • Integracje • Event Push Service • Polityki

10.3.133.	Early access – Oprogramowanie musi umożliwiać dobrowolne przystąpienie do darmowych testowych programów wczesnego dostępu. Programy wczesnego dostępu powinny umożliwiać testowanie najnowszych funkcji oprogramowania, których nie ma jeszcze w wersji końcowej produktu. Uzyskanie dostępu do programu testowego musi być natychmiastowe.
10.3.134.	Możliwość utworzenia konsoli typu Partner, która pozwala na zarządzanie wieloma firmami z poziomu jednej scentralizowanej konsoli zarządzającej, konsola partnerska musi umożliwiać: • Pobieranie przez partnera plików z kwarantanny podległych firm. • Zarządzanie systemem ochrony firm podrzędnych przez Partnera z jednej konsoli lub tworzenie bezpośrednich dostępów użytkowników dla tych firm. • Odseparowanie przez administratora konsoli podrzędnej od konsoli partnera nadrzędnego.
10.3.135.	Profil firmy - Możliwość określenia profilu przedsiębiorstwa w konsoli webowej. Dostępne są kategorie m.in: Lotnictwo, Budownictwo, Edukacja, Służba zdrowia, Handel i inne.
10.3.136.	System musi umożliwiać wybór trzech poziomów obciążenia procesora dla zadań określonych w harmonogramie skanowania na systemach Linux i macOS.
10.3.137.	System musi posiadać funkcję wstrzymywania skanowania podczas pracy na baterii.
10.3.138.	Konsola administracyjna umożliwia zmianę motywu dla interfejsu spośród jasnego, ciemnego lub wybranego automatycznie w oparciu o ustawienia systemowe.
10.3.139.	System umożliwia tymczasowe wyłączenie wszystkich lub wybranych modułów ochrony na określony czas, który wynosi 15 minut, 30 minut, 1 godzina, 2 godziny, 4 godziny. Po ponownym uruchomieniu ochrony możliwość przeprowadzenia pełnego skanowania.
10.3.140.	Centrum integracji – Panel umożliwiający zarządzanie integracjami z rozwiązaniami zewnętrznymi tj. Vmware vCenter, Veeam Backup & Replication, Microsoft Active Directory, Vmware Tanzu, Microsoft Exchange (on-premises), SecurityCoach (KnowBe4).
10.3.141.	Wbudowany sandbox musi posiadać możliwość przesyłania pliku do analizy z komputera zdalnego za pomocą podanej ścieżki. Wielkość pliku nie może przekraczać 100MB.
10.3.142.	Filtrowanie wykrytych incydentów bezpieczeństwa m.in. na podstawie: • ID. • Ostatnia aktualizacja. • Status. • Osoba przydzielająca. • Data utworzenia. • Priorytet. • Ocena szkodliwości w skali 0-100. • Podmioty. • Zasoby. • Ostatnia faza killchain. • Wykonane czynności. • Skorelowane incydenty. • Typ incydentu.

10.3.143.	System umożliwia wygenerowanie i pobranie zestawu informacji z chronionych punktów końcowych w formie archiwum. Funkcja powinna być dostępna dla systemów Windows, Linux oraz macOS. Archiwum musi zawierać co najmniej informacje: • Windows ➢ Logi zainstalowanego agenta. ➢ Dziennik zdarzeń Windows. ➢ Informacje o systemie. ➢ DnsCache. ➢ Webcache. ➢ Informacje z głównych katalogów rejestru (SYSTEM, SOFTWARE, DEFAULT, DRIVERS, SAM, SECURITY). ➢ Harmonogram zadań. ➢ Historia Powershell (jeśli włączono). • Linux ➢ Podstawowy log pomocy technicznej zainstalowanego agenta. ➢ Certyfikaty. ➢ Autorun i usługi. ➢ Informacje sieciowe. ➢ Informacje systemowe. ➢ Zainstalowane pakiety. • macOS ➢ Podstawowy log pomocy technicznej zainstalowanego agenta. ➢ Autorun. ➢ Lista procesów. ➢ Informacje sieciowe. ➢ Informacje o systemie.
10.3.144.	Oprogramowanie musi umożliwiać przegląd konfiguracji punktów końcowych w czasie rzeczywistym poprzez tworzenie zapytań pod kątem wykrywania: • historia powłoki. • wczytywanie bibliotek .dll z podejrzanej lokalizacji. • Sesje logowania z użyciem jawnych danych uwierzytelniających. • Arp cache. • Ip forwarding. • Lista zamontowanych nośników. • Konfiguracja ip tables. • Połączenia TLS które używają certyfikatów self-signed. • Używane rozszerzenia w przeglądarce Chrome. • Używane rozszerzenia w przeglądarce Firefox. • Używane rozszerzenia w przeglądarce Safari. • Źródła apt w systemach Linux. • Wyświetlanie zainstalowanych pakietów DEB. • Wyświetlanie zainstalowanych pakietów RPM. • Pakiety Python zainstalowane w systemie. • Lista użytkowników, którzy zostali utworzeni w ciągu ostatnich 30 dni (Linux). • Wykrywanie czy aplikacje zdalnego dostępu są zainstalowane w systemie MacOS.

	• Wykrywanie czy Kontrola Kont Użytkowników (UAC) jest wyłączona. • Wykrywanie czy SecureBoot jest włączony. • Lista zapamiętanych sieci bezprzewodowych. • Wykrywa, czy zmienił się domyślny folder startowy użytkownika. • Wykrywa, czy zmienił się domyślny folder startowy maszyny.
10.3.145.	Oprogramowanie musi umożliwiać tworzenie konfigurowalnych reguł, po spełnieniu których może zostać wygenerowany incydent bezpieczeństwa. Funkcja ta powinna: • Oferować opcję podjęcia automatycznych działań po spełnieniu warunków tj.: izolacja punktu końcowego, wygenerowanie archiwum diagnostycznego, przesłanie pliku do analizy sandbox, zakończenie procesu i innych. • Automatyczne działania zapobiegawcze są zależne od wyboru kategorii. • Tworzenie reguł musi być określone poprzez wybór operatora np. „to”, „zawiera”, „jest jednym z” itp. • Dotyczyć określonych kryteriów tj. proces, plik, rejestr, połączenia. • Zapewniać możliwość tworzenia zapytań YARA. • Umożliwiać określenie priorytetu kolejności automatyzacji. • Administrator powinien mieć możliwość wyboru poziomu szkodliwości potencjalnie wygenerowanych incydentów (wysokie, średnie i niskie).
Lp.	**EDR - Endpoint Detection and Response**
10.3.146.	Produkt musi zapewniać szczegółowe informacje o wykrytych incydentach, interaktywną mapę incydentów i działania naprawcze.
Wspierane systemy operacyjne	
10.3.147.	Systemy desktopowe: • Windows 11 October 2024 Update (24H2) • Windows 11 October 2023 Update (23h2) • Windows 10 November 2022 Update (22H2) • Windows 11 September 2022 Update (22H2) • Windows 11 (initial release) • Windows 10 November 2021 Update (21H2) • Windows 10 May 2021 Update (21H1) • Windows 10 October 2020 Update (20H2) • Windows 10 May 2020 Update (20H1) • Windows 10 May 2019 Update (19H1) • Windows 10 October 2018 Update (Redstone 5) • Windows 10 April 2018 Update (Redstone 4) • Windows 10 Fall Creators Update (Redstone 3) • Windows 10 Creators Update (Redstone 2) • Windows 10 Anniversary Update (Redstone 1) • Windows 10 November Update (Threshold 2) • Windows 10 (initial release)
10.3.148.	Systemy operacyjne serwera: • Windows Server 2025 64x • Windows Server 2022 Core • Windows Server 2022

	• Windows Server 2019 Core • Windows Server 2019 • Windows Server 2016 • Windows Server 2016 Core • Windows Server 2012 R2 • Windows Server 2012 • Windows Small Business Server (SBS) 2011 • Windows Server 2008 R2
10.3.149.	Systemy operacyjne Linux i wersja kernel: 10.3.149.1. Oparte o RPM • RHEL 7.x - 3.10.0 (build 957) 64-bit • RHEL 8.x - 4.18.0 64-bit • RHEL 9.x - 5.14.0 64-bit • Oracle Linux 7.x (UEK) - 4.18.0 64-bit • Oracle Linux 7.x (RHCK) - 3.10.0 build 957 64-bit • Oracle Linux 8.x (UEK) - 5.4.17 / 5.15.0 64-bit • Oracle Linux 8.x (RHCK) – 4.18.0 64-bit • Oracle Linux 9.x (UEK) – 5.15.0 64-bit • Oracle Linux 9.x (RHCK) – 5.14.0 64-bit • CentOS 7.x - 3.10.0 (build 957) 32-bit/64-bit • CentOS 8 Stream - 4.18.0 64-bit • CentOS 9 Stream - 5.14.0 64-bit • Fedora 37 – 40 – wsparcie do wygaśnięcia. 64-bit • AlmaLinux 8.x - 4.18.0 64-bit • AlmaLinux 9.x - 5.14.0 64-bit • Rocky Linux 8.x - 4.18.0 64-bit • Rocky Linux 9.x - 5.14.0 64-bit • CloudLinux 7.x - 3.10 (build 957) 64-bit • CloudLinux 8.x - 4.18.0 64-bit • Miracle Linux 8.x - 4.18.0 64-bit • Kylinv10 RHEL - 4.19.90 64-bit 10.3.149.2. Oparte o Debian • Debian 9 - 4.9.0 32-bit/64-bit • Debian 10 - 4.19 32-bit/64-bit • Debian 11 - 5.10 32-bit/64-bit • Debian 12 – 6.1.0 64-bit • Ubuntu 16.04.x - 4.8 / 4.10 / 4.13 / 4.15 32-bit/64-bit • Ubuntu 18.04.x - 5.0 / 5.3 / 5.4 64-bit • Ubuntu 20.04.x - 5.4 / 5.8 / 5.11 / 5.13 / 5.15 64-bit • Ubuntu 22.04.x - 5.15 / 5.19 64-bit • Ubuntu 23.04.x – 6.2.0 64-bit • Ubuntu 24.04.x – 6.8.0 64- bit • PopOS 22.04.x – 6.2.6 64-bit • Pardus 21 – 5.10.0 64-bit

	• Mint 20.x – 5.4.0 64-bit • Mint 21.x – 5.15.0 64-bit • Mint 22.x – 6.8.0.x 64-bit • Zorin OS – 6.5.x 64-bit • Linux Mint Debian Edition 6 – 6.1.x 64-bit 10.3.149.3. Oparte o SUSE • SLES 12 SP4 - 4.12.14-x 64-bit • SLES 12 SP5 - 4.12.14-x 64-bit • SLES 15 SP1 - 4.12.14-x 64-bit • SLES 15 SP2 - 5.3.18-x 64-bit • SLES 15 SP3 - 5.3.18-x 64-bit • SLES 15 SP4 – 5.14.21 64-bit • SLES 15 SP5 – 5.14.21 64-bit • SLES 15 SP6 – 6.4.x 64-bit • SLED 15 SP4 – 5.14.21 64-bit • openSUSE Leap 15.4 - 15.5 - 5.14.21 64-bit
Komponenty EDR	
10.3.150.	Sensor EDR, który gromadzi i przetwarza dane dotyczące punktu końcowego i zachowania aplikacji w celu ich raportowania.
10.3.151.	Analityka Bezpieczeństwa, komponent służący do interpretacji metadanych gromadzonych przez sensor EDR.
10.3.152.	Możliwość instalacji dodatkowego, dedykowanego agenta z sensorem EDR dla urządzeń z systemem Windows, aby rozszerzyć już zainstalowaną równolegle ochronę świadczoną przez innego producenta oprogramowania antywirusowego.
Wykrywanie podejrzanej aktywności	
10.3.153.	Monitorowanie zdarzeń na punktach końcowych w poszukiwaniu oznak ataku i wywoływanie incydentów po wykryciu takiej aktywności. 10.3.153.1. Bazowanie na systemach opartych o techniki MITRE ATT&CK i własnej inteligencji. 10.3.153.2. Zgłaszanie naruszeń jako incydent w module EDR.
Badanie incydentów i wizualizacja	
10.3.154.	Produkt zapewnia wsparcie analizy incydentów poprzez dostarczenie narzędzi, które pomagają filtrować, badać i podejmować działania dotyczące wszystkich zdarzeń bezpieczeństwa wykrytych przez czujnik EDR w określonym czasie.
10.3.155.	Produkt integruje się z bazą wiedzy MITRE ATT&CK i odpowiednio oznacza zdarzenia bezpieczeństwa.
10.3.156.	Produkt zapewnia zaawansowaną wizualizację zdarzeń bezpieczeństwa z określonymi danymi lub działaniami z następującymi informacjami: • Karta podsumowująca zawiera przegląd wpływu zdarzenia i szczegółowe informacje o każdym węźle zdarzenia. • Funkcja osi czasu zbiera informacje o rozwoju zdarzenia bezpieczeństwa w kolejności chronologicznej. • System gromadzi informacje o działaniach podejmowanych przez produkt w związku ze zdarzeniem bezpieczeństwa.
Incydenty	

10.3.157.	Oprogramowanie musi informować o zagrożeniach wykrytych i zablokowanych w formie grafu i chronologicznej linii zdarzeń oraz daje możliwość: • Filtrowania zdarzeń. • Zakończenia procesów. • Dodania procesów do czarnej listy. • Dodania procesów do białej listy. • Izolacji hosta. • Przesłania pliku do Sandbox. • Sprawdzenia informacji o pliku w Google. • Sprawdzenia informacji o pliku w VirusTotal.
10.3.158.	Możliwość szybkiego podglądu incydentów za pomocą spersonalizowanych widoków list lub widoku domyślnego.
10.3.159.	Możliwość wyświetlenia 10,20,30,50,100 zdarzeń na jednej stronie.
10.3.160.	System musi umożliwiać blokowanie na podstawie utworzonych reguł czarnej listy przy pomocy kategorii: • Hash MD5 lub SHA256. • Pełna ścieżka do aplikacji. • Reguła połączenia.
10.3.161.	Możliwość importu reguł czarnej listy dla hash, ścieżek do aplikacji oraz reguł połączeń z pliku CSV.
10.3.162.	System musi oferować szeroki zakres filtrowania dodanych reguł blokowania minimum po nazwie pliku, hash pliku, typu hash, ścieżce, protokole porcie/zakresie portów, daty dodania.
10.3.163.	Możliwość wygenerowania i wyeksportowania listy incydentów do pliku .csv.
10.3.164.	Możliwość importu reguł czarnej listy dla hash, ścieżek do aplikacji oraz reguł połączeń z pliku CSV.

II.11 Rozszerzenie EDM o nowe dokumenty ustawowe

Stan obecny

Zamawiający posiada i użytkuje Szpitalny System Informatyczny (HIS) firmy ASSECO POLSKA S.A. o nazwie AMMS.

Opis ogólny

Przedmiotem zamówienia jest rozbudowa Szpitalnego Systemu Informatycznego (HIS) używanego przez Zamawiającego, polegająca na wdrożeniu i pełnym udostępnieniu obsługi nowych wzorów elektronicznej dokumentacji medycznej (EDM), zgodnych z wymaganiami Centrum e-Zdrowia wraz z zapewnianiem 36 miesięcznej usługi gwarancyjnej.

Wymagania minimalne

Przedmiotem

Lp.	Typ sprzętu	Charakterystyka (wymagania minimalne)
11.3.1.	**Zakres merytoryczny**	Szpitalny System Informatycznego (HIS) wykorzystywany przez Zamawiającego musi obsługiwać następujące dokumenty EDM: • e-wyniki i opisy badań histopatologicznych, • e-wyniki i opisy badań cytologicznych, • karta diagnostyki i leczenia onkologicznego (e-DILO), • plan leczenia onkologicznego, • Patient Summary (Karta zdrowia pacjenta), • karta opieki kardiologicznej (e-KOK), • karta medycznych czynności ratunkowych, • karta medyczna lotniczego zespołu ratownictwa medycznego, • dokumenty medycyny pracy: ➢ orzeczenie lekarskie, ➢ zalecenia wynikające z warunków pracy lub stanowiska pracy. Każdy z dokumentów musi być tworzony, walidowany, podpisywany i przechowywany zgodnie z wymaganiami CEZ, a tam gdzie to wymagane – przekazywany do systemu P1.
11.3.2.	**Wymagania techniczne**	11.3.2.1. Uwierzytelnienie i autoryzacja • W przypadku standardu uwierzytelnienia użytkowników i systemów muszą być stosowane dwie metody: ➢ OAuth 2.0 (Client Credentials Grant) – zgodnie z mechanizmami używanymi przy obsłudze zdarzeń medycznych. ➢ Certyfikaty TLS i WSS wydane przez Centrum Certyfikacji P1. • Uwierzytelnienie systemu wykonawcy wywołującego usługi P1 musi następować w warstwie transportowej połączenia TLS z obustronnym uwierzytelnieniem (mutual TLS). • System wykonawcy musi używać certyfikatu uwierzytelniającego system, wydanego przez Centrum Certyfikacji P1, także do pobierania informacji pomocniczych (np. przykłady komunikatów). • Komunikaty SOAP muszą być podpisane cyfrowo przy użyciu certyfikatu do uwierzytelniania danych. • Po weryfikacji podpisu następuje identyfikacja i uwierzytelnienie systemu wykonawcy. • Po uwierzytelnieniu musi nastąpić autoryzacja obejmująca: ➢ sprawdzenie przydzielenia uprawnienia do wywoływanej usługi w P1, ➢ autoryzację dostępu do danych na podstawie parametrów wywołania. • W komunikacji z systemem P1 wymagane jest użycie: ➢ rozszerzenia Web Services Security, ➢ profilu Web Services Security X.509 Certificate Token Profile. 11.3.2.2. Standardy komunikacji i formaty dokumentów

		• e-DILO, plan leczenia onkologicznego – standard HL7 FHIR, zasoby przekazywane usługami REST. • Karta opieki kardiologicznej (e-KOK) – standard HL7, interfejs SOAP. • Wyniki i opisy badań histopatologicznych, cytologicznych, Patient Summary, dokumenty medycyny pracy – standard HL7 CDA, interfejs SOAP. • Karty ratownictwa medycznego (ZRM, LPR) – standard HL7 CDA, dokumenty przechowywane w repozytorium podmiotu, przekazywany indeks EDM do P1. 11.3.2.3. Szczegółowe wymagania techniczne dla implementacji poszczególnych wzorów dokumentów EDM Wykonawca jest zobowiązany każdorazowo pozyskiwać z Centrum e-Zdrowia (CEZ), które publikuje specyfikacje integracyjne, profile komunikacyjne, schematy XML/JSON oraz przykłady komunikatów. 11.3.2.4. Wykonawca musi zapewnić, że wdrożenie w systemie AMMS będzie w pełni zgodne z najnowszymi wersjami specyfikacji i wytycznymi CEZ, a w przypadku ich aktualizacji – dostosować rozwiązanie w ramach realizacji umowy, bez dodatkowych kosztów dla Zamawiającego.
11.3.3.	**Zapewnienie interoperacyj-ności**	Wykonawca musi zapewnić pełną interoperacyjność w ramach oferowanej ceny, zgodnie z: • ustawą z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. z 2024 r. poz. 1557 z późn. zm.), • Rozporządzeniem Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności (Dz.U. 2024 poz. 773), • ustawą z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia (Dz.U. z 2023 r. poz. 2465 z późn. zm.), • minimalnymi wymaganiami dla systemów określonymi w art. 8a ww. ustawy.

II.12 Zakup i wdrożenie oprogramowania do uwierzytelniania wieloskładnikowego i zarządzania tożsamością w domenie Active Directory

Opis ogólny

Przedmiotem zamówienia jest zakup i wdrożenie oprogramowania do uwierzytelniania wieloskładnikowego i zarządzania tożsamością w domenie Active Directory Zamawiającego.

Wymagania dotyczące licencji

Lp.	Wymagania minimalne
12.2.1.	Długość obowiązywania licencji:

	• licencja wieczysta
12.2.2.	Liczba użytkowników: • 750 użytkowników domenowych
12.2.3.	Liczba administratorów obsługujących aplikację: 3
12.2.4.	Dostęp do wsparcia i aktualizacji: • 36 miesięcy

Wymagania dotyczące oprogramowania

Lp.	Wymagania minimalne
12.3.1.	System pozwala na zmianę portu HTTP/HTTPs z poziomu interfejsu graficznego
12.3.2.	System działa w formie aplikacji Internetowej
12.3.3.	System działa na systemach z rodziny Windows.
12.3.4.	System pozwala na wdrożenie aplikacji na platformy mobilne iOS.
12.3.5.	System pozwala na podłączenie certyfikatu, w formacie .PFX(PKCS12) oraz Java Keystore
12.3.6.	System obsługuje bazy danych PostgreSQL oraz MSSQL, jako instancje do przechowywania danych
12.3.7.	System działa na pojedynczej bazie danych
12.3.8.	System posiada wbudowane skryptu, które pozwalają na: • backup bazy danych, • odtworzenie bazy danych, • zmianę bazy danych.
12.3.9.	System posiada wbudowany program, z interfejsem graficznym, który pozwala na aktualizację aplikacji.
12.3.10.	System używa jednego konta do połączenia z domeną.
12.3.11.	System posiada wbudowany program, z interfejsem graficznym, który pozwala na aktualizację aplikacji.
12.3.12.	System pozwala na zmianę portu HTTP/HTTPs z poziomu interfejsu graficznego.
12.3.13.	System pozwala na wygenerowanie CSR, do własnego certyfikatu, z poziomu interfejsu graficznego.
12.3.14.	System umożliwia podłączenie innych aplikacji, w celu autentykacji SSO, poprzez protokół SAML, w tym wszystkie aplikacje będą wyświetlane w interfejsie graficznym aplikacji
12.3.15.	System umożliwia na konfigurację uwierzytelniania wieloskładnikowego (MFA) za pomocą dowolnej z 14 obsługiwanych metod uwierzytelniania, w tym YubiKey, uwierzytelniania odcisków palców, RSA SecurID i DUO Security
12.3.16.	System umożliwia integrację z usługą 'Have I Been Pwned?' I zablokowanie użycia znanych haseł podczas procesu zmiany hasła lub resetu hasła przez użytkownika
12.3.17.	System umożliwia obsługę usługi Azure AD MFA, dzięki czemu można teraz używać Azure AD MFA do weryfikacji tożsamości podczas: samodzielnego resetowania/odblokowywania; samoobsługowe logowanie do portalu; logowanie do aplikacji w chmurze, maszyny oraz OWA. Metoda autentykacji jest dostępna zarówno w aplikacjach internetowych oraz mobilnych.
12.3.18.	Aplikacja daje użytkownikom możliwość resetowania hasła, odblokowania konta, aktualizacji danych, zapisywania do grup mailowych i security w środowisku Active Directory. Wszystkie wymienione funkcje powinny być dostępne z poziomu przeglądarki internetowej, a resetowanie hasła i odblokowanie konta z poziomu modułu GINA/Credential Provider Windows

12.3.19.	System umożliwia konfigurowanie polityk dla poszczególnych jednostek organizacyjnych OU, a w szczególności: • Konfigurowanie ustawień dla pytań zabezpieczających i odpowiedzi kontrolnych • Konfigurowanie ustawień dla uwierzytelniania za pomocą wiadomości SMS 1.20.3. Konfigurowanie ustawień dla uwierzytelniania za pomocą jednorazowej wiadomości e-mail • Zablokowanie użytkowników, którzy nie uwierzytelnią się odpowiedziami na pytania kontrolne, kod SMS, jednorazowe hasło wysyłane jako e-mail • Po udanej autoryzacji następuje automatyczne resetowanie i odblokowywanie kont
12.3.20.	Metody uwierzytelniania z punktów 1.34.1-1.34.12 powinny dawać możliwość ustawienia pojedynczej metody lub powiązania ich ze sobą w celu wprowadzenia uwierzytelniania wieloskładnikowego
12.3.21.	System umożliwia podłączenie innych aplikacji, w celu autentykacji SSO, poprzez protokół SAML, w tym wszystkie aplikacje będą wyświetlane w interfejsie graficznym aplikacji
12.3.22.	System nie posiada ograniczenia ilości dodawanych aplikacji, odnosząc się do punktu 1.17
12.3.23.	System umożliwia notyfikowanie użytkowników o: • O fakcie, że hasło wygaśnie za x dni – gdzie istnieje możliwość konfiguracji powiadomień, co cykliczny okres czasu – w tym o niestandardową ilość powiadomień • Dokonaniu restartu hasła • Dokonania odblokowania konta • Dokonania zmiany hasła • Dokonania rejestracji w programie • Dokonania samodzielnej aktualizacji danych
12.3.24.	System pozwala na konfigurację notyfikacji, w zależności od OU/Grupy
12.3.25.	System współpracuje z bazą danych MSSQL
12.3.26.	System pozwala na wysyłanie notyfikacji za pomocą e-mail'a, jak i SMS'a.
12.3.27.	System umożliwia konfigurację widoku edycji danych dla użytkownika w portalu samoobsługi, a w szczególności ma mieć możliwość: • Modyfikacji ekranu do aktualizacji danych przez użytkowników za pomocą funkcji „przeciągnij i upuść" • Dodawania własnych atrybutów
12.3.28.	System umożliwia rejestrowanie pytań i odpowiedzi, a w szczególności: • Wysyłać powiadomienia do użytkowników z prośbą o zdefiniowanie pytań kontrolnych w systemie • Wysyłać przypomnienia o rejestracji pytań poprzez wyszukiwanie niezarejestrowanych użytkowników i kojarzenie ich konta ze skryptem logowania, który przypomina o rejestracji przy każdym logowaniu do sieci • Rejestrowanie pytań i odpowiedzi dla wielu użytkowników z wykorzystaniem pliku csv
12.3.29.	System umożliwia skonfigurowanie modułu GINA/Credential Provider dla stacji roboczych użytkowników w celu resetowania hasła i odblokowania konta za pomocą ekranu logowania, a w szczególności: • Pozwalać na instalację modułu GINA/CP bezpośrednio z aplikacji • Pozwalać tworzenie harmonogramu instalacji
12.3.30.	System umożliwia dodawanie serwisanta systemu i przypisywanie mu odpowiedniej roli
12.3.31.	System umożliwia tworzenie zaplanowanych raportów i posiada wbudowane raporty dotyczące: 12.3.32.1. Ogólne raporty w czasie rzeczywistym:

	• Zablokowani użytkownicy • Użytkownicy, których hasła wygasły • Hasła użytkowników, które wkrótce wygasną 12.3.32.2. Raporty audytowe: • Raport z audytu zresetowanych haseł • Raport z audytu odblokowanych kont • Raport z audytu samodzielnych uaktualnień • Raport z audytu zmian hasła 12.3.32.3. Nieudane próby odpowiedzi na pytania zabezpieczające • Raporty z rejestracji: • Raport o zarejestrowanych użytkownikach • Raport o niezarejestrowanych użytkownikach • Raport o licencjonowanych użytkownikach • Raport o pytaniach i odpowiedziach zabezpieczających
12.3.33.	System umożliwia wyszukiwanie pracowników w katalogu
12.3.34.	System umożliwia automatyczne wysyłanie powiadomień o wygasających hasłach i kontach
12.3.35.	System umożliwia wymuszenie własnych zasad haseł, przy zmianie hasła, w tym ustawiania: • Minimalnej długości • Maksymalnej długości • Ilości znaków specjalnych • Ilości znaków numerycznych • Wymuszania, by pierwszym znakiem w haśle była litera • Wymuszania, by hasło posiadało duże i mały litery • Niezezwalania, by hasło posiadało dwie te same litery z rzędu • Niezezwalania, by było używane 5 znaków z loginu • Niezezwalania, by było używane 5 znaków z poprzedniego hasła
12.3.36.	12.3.36.1. Niezezwalania, na użycie określonej liczby kolejnych znaków z nazw użytkowników i starych haseł 12.3.36.2. Niezezwalania, na użycie danego znaku (specjalnego, cyfry, litery) określoną ilość razy z rzędu 12.3.36.3. Określanie czy hasło ma się zaczynać od dużej litery, małej litery, cyfry lub znaku specjalnego 12.3.36.4. Niezezwalanie, na zakończenie hasła cyfrą 12.3.36.5. Określenie ilości wykluczonych starych haseł
12.3.37.	System pozwala na synchronizację haseł pomiędzy AD, a: • Microsoft 365 • G-Suite • IBM AS400 • HP UX
12.3.38.	System umożliwia personalizacje portalu dla użytkowników
12.3.39.	System umożliwia włączenie workflow (akceptacji) dla: • Zrestartowania hasła • Odblokowania konta • Samodzielnej aktualizacji danych w AD
12.3.40.	System obsługuje autoryzację użytkownika końcowego poprzez: • Pytania zabezpieczające • Microsoft Authenticator (TOTP) • Google Authenticator

	• Odcisk palca • YubiKey • Notyfikacje push na wcześniej zarejestrowanej aplikacji • E-mail • SMS • Duo Security • Autentykację RADIUS'ową • QR Code • SAML • Pytania zabezpieczające z AD • Azure AD MFA • RSA SecurID • Zoho OneAuth TOTP • Smart Card Authentication • Custom TOTP Authenticator
12.3.41.	System posiada aplikację na platformy mobilne, celem weryfikacji użytkownika.
12.3.42.	System pozwala na wdrożenie aplikacji na platformy mobilne iOS.
12.3.43.	System pozwala na zmianę portu HTTP/HTTPs z poziomu interfejsu graficznego.
12.3.44.	System działa w formie aplikacji Internetowej.
12.3.45.	System działa na systemach z rodziny Windows.
12.3.46.	System pozwala na podłączenie certyfikatu, w formacie .PFX(PKCS12) oraz Java Keystore.
12.3.47.	System obsługuje bazy danych PostgreSQL oraz MSSQL, jako instancje do przechowywania danych.
12.3.48.	System działa na pojedynczej bazie danych.
12.3.49.	System posiada wbudowane skryptu, które pozwalają na: • backup bazy danych, • odtworzenie bazy danych, • zmianę bazy danych.
12.3.50.	System posiada wbudowany program, z interfejsem graficznym, który pozwala na aktualizację aplikacji.
12.3.51.	System używa jednego konta do połączenia z domeną
12.3.52.	System posiada wbudowany program, z interfejsem graficznym, który pozwala na aktualizację aplikacji
12.3.53.	System pozwala na zmianę portu HTTP/HTTPs z poziomu interfejsu graficznego.
12.3.54.	System pozwala na wygenerowanie CSR, do własnego certyfikatu, z poziomu interfejsu graficznego.
12.3.55.	System posiada integrację z usługą "Have I Been Pwnded?", co uniemożliwia korzystanie z naruszonych haseł podczas zmiany lub resetowania hasła przez użytkownika
12.3.56.	Administrator posiada możliwość określenia skryptu do rejestracji, widoku tytułu oraz tekstu.
12.3.57.	System posiada możliwość wykluczenia adresów IP.
12.3.58.	System pozwala na modyfikację strony logowania do aplikacji, w tym: • Ma możliwość modyfikacji strony logowania z podstrony administracyjnej • Ma możliwość graficznej edycji strony logowania, za pomocą przeciągania odpowiednich elementów
12.3.59.	System posiada możliwość zarządzania dostępem na podstawie geolokalizacji.
12.3.60.	System obsługuje trzy różne metody instalacji agenta logowania Windows:

	• Remcom • PAExec • WMI
12.3.61.	System i inne aplikacje SSO są dostępne za pomocą zaawansowanych metod uwierzytelniania, takich jak biometria, YubiKey, Google Authenticator itp.
12.3.62.	System umożliwia wymuszoną rejestrację dla usługi MFA logowania do komputera.
12.3.63.	System pozwala na konfigurację usługi MFA dla aplikacji w chmurze w oparciu o SAML/OAuth2.
12.3.64.	System obsługuje jednokrotne logowanie oparte na OAuth i OpenID Connect dla dowolnej aplikacji korporacyjnej obsługującej te protokoły, oprócz już istniejącej obsługi SAML.
12.3.65.	System pozwala na silne zabezpieczenie środowiska Exchange dzięki dedykowanej konfiguracji uwierzytelniania wieloskładniowego (MFA) z ponad 17 zaawansowanymi metodami uwierzytelniania dla Outlooka w sieci Web i logowania do centrum administracyjnego Exchange.
12.3.66.	System obsługuje agenta Mac dla macOS Big Sur.
12.3.67.	System posiada możliwość blokady określonych mailów domenowych oraz formatów numeru telefonu podczas rejestracji przy użyciu aplikacji mobilnej.
12.3.68.	System posiada obsługę logowania jednokrotnego (SSO) do lokalnej wersji ManageEngine ServiceDesk Plus.
12.3.69.	System posiada obsługę wyzwań RADIUS dla uwierzytelniania wieloskładnikowego RADIUS.
12.3.70.	System posiada obsługę aktualizacji informacji z kontrolerów domeny opartych na lokacji – umożliwia to przypisanie określonego zestawu kontrolerów domeny do jednostki organizacyjnej.
12.3.71.	System pozwala na wybranie poszczególnych połączonych kont dla zadania Password Sync w celu zresetowania hasła, odblokowania konta czy zmiany hasła
12.3.72.	System posiada możliwość ograniczenia dostępu do portalu oparty na protokole IP.
12.3.73.	System obsługuje agenta Mac dla macOS Monterey.
12.3.74.	System obsługuje sprzętowy token TOTP Protectimus i Deepnet Security.
12.3.75.	System posiada możliwość wygenerowania zapasowych kodów (Backup codes) dla kont technicznych
12.3.76.	System pozwala na wymuszenie metod MFA jeżeli użytkownik nie jest podłączony do żadnej sieci (Offline MFA) dla systemów Windows oraz MacOS
12.3.77.	System obsługuje agenta Mac dla macOS Ventura.
12.3.78.	System pozwala na rejestracje do rozwiązania po prawidłowym zalogowaniu się do aplikacji chmurowych
12.3.79.	System pozwala na skonfigurowanie urządzeń FIDO jako jedną z metod MFA
12.3.80.	Dla uwierzytelniania RSA zapewniono obsługę integracji opartą na interfejsie REST API
12.3.81.	System pozwala na tworzenie użytkowników za pomocą funkcji Just-In-Time. Pozwala ona na zakładanie konto do aplikacji Assetsonar, Monday.com, Peakon, Slack i innych
12.3.82.	Aplikacja wspiera DUO SDK w wersji 4, do zarządzania urządzeniami DUO zarejestrowanych użytkowników
12.3.83.	Aplikacja pozwala na dodanie dwóch metod biometrycznej autentykacji na Android, może być to jednocześnie odcisk palca i skan twarzy, w przypadku wspieranych urządzeń
12.3.84.	Aplikacja pozwala na zaktualizowanie poświadczeń na urządzeniu Windows, które jest z dala od sieci firmowej. Aktualizację poświadczeń poprzedza restart hasła wykonany z ekranu logowania, a następnie hasło jest aktualizowane na stacji roboczej/serwerze. Mechanizm może działać bez VPN'a lub z VPN'em

12.3.85.	Aplikacja obsługuje autentykacje OAUTH w przypadku synchronizacji haseł użytkowników, dla Microsoft Entra ID(Azure) jak i Microsoft Dynamics CRM
12.3.86.	MFA i zmiana hasła przez użytkownika oraz odblokowywanie konta z poziomu logowania do maszyn, dla macOS. (Wpierane wyłącznie dla Apple Silicon, czyli M1 w górę).
12.3.87.	ADSelfService Plus teraz wspiera logowanie SSO i MFA przez Kosmos, co daje klientom więcej swobody w wyborze dostawców tożsamości
12.3.88.	Smart Card i YubiKey do logowania – Możliwość logowania do VPN, OWA, i Windows za pomocą fizycznych tokenów (np. YubiKey)
12.3.89.	Teraz MFA działa także na maszynach z Red Hat i Rocky Linux (wersje 8.x i 9.x).
12.3.90.	Nawet jeśli klient ma przestarzałego klienta VPN, może skorzystać z MFA przez bezpiecznylink w przeglądarce.
12.3.91.	Funkcja blokady konta działa teraz nie tylko w portalu, ale też w aplikacjach firmowych
12.3.92.	Admin może automatycznie odblokować konta
12.3.93.	Silniejsze hasła dzięki regexom(wyrażenia regularne) – Admin może wymusić tworzenie silniejszych haseł zgodnych z polityką firmy (np. co najmniej 1 znak specjalny, bez sekwencji itp.)

Wdrożenie i szkolenia

Lp.	Wymagania minimalne
12.4.1.	Instalacja aplikacji i konfiguracja usługi.
12.4.2.	Konfiguracja zabezpieczeń (HTTPs i folderu aplikacji).
12.4.3.	Integracja z domeną ActiveDirectory Zamawiającego.
12.4.4.	Konfiguracja 2 administratorów,
12.4.5.	Podłączenie skrzynki pocztowej,
12.4.6.	Konfiguracja 1 polityki restartu haseł,
12.4.7.	Konfiguracja 1 profilu notyfikacji o wygasającym haśle,
12.4.8.	Konfiguracja 1 układu zmiany danych w ActiveDirectory.
12.4.9.	Wdrożenie agenta GINA (Graphical Identification and Authentication) na 1 stacji Zamawiającego
12.4.10.	Weryfikacja działania skonfigurowanych elementów.
12.4.11.	Omówienie utrzymania aplikacji,
12.4.12.	Omówienie funkcjonalności systemu.
12.4.13.	Omówienie działania aplikacji na najwyższej możliwej wersji (zostaną omówione dodatkowe funkcje oprogramowania w przypadku braku posiadania licencji na dany moduł).
12.4.14.	Wszystkie prace będą realizowane przy udziale lub w konsultacji z pracownikami Zamawiającego.
12.4.15.	W celu realizacji przedmiotu umowy Zamawiający udostępni Wykonawcy środowisko serwerowe oparte na systemie wirtualizacyjnym VMware w konfiguracji zaproponowanej przez Wykonawcę. W razie konieczności zwiększenie zasobów maszyny wirtualnej, może to nastąpić po uprzednim uzgodnieniu z Zamawiającym.

Warunki świadczenia gwarancji i serwisu

Lp.	Wymagania minimalne
12.5.1.	Dostarczane oprogramowanie musi być objęte co najmniej 36 miesięczną asystą techniczną umożliwiającą: • nielimitowane wsparcie techniczne drogą mailową i systemem zdalnej pomocy w dni robocze w godzinach od 8:00 do 16:00 – bez dodatkowych opłat, • darmowy dostęp do podstawowych uaktualnień i poprawek w Oprogramowaniu, • możliwość aktualizacji głównej wersji oprogramowania bez dodatkowych opłat, • dostęp do portalu pomocy technicznej i bazy rozwiązań.
12.5.2.	W okresie ważności asysty technicznej Wykonawca zobowiązuje się usuwać, wszelkie Awarie, Usterki i Wady w działaniu ww. oprogramowania, bez dodatkowych opłat, • Awaria – błąd uniemożliwiający eksploatację Systemu i niepozwalający na znalezienie takiego sposobu używania Systemu, aby skutecznie obejść jego przyczyny, • Usterka – błąd, nie uniemożliwiający eksploatacji Systemu lub pozwalający na skuteczne obejście jego przyczyny, • Wada – błąd powodujący niewykonywanie lub nieprawidłowe wykonywanie funkcji określonych w specyfikacji technicznej Producenta.
12.5.3.	Zgłoszenia Awarii, Usterek i Wad przyjmowane będą w godzinach od 8:00 do 16:00, w dni robocze przez serwis Wykonawcy drogą telefoniczną, pocztą elektroniczną lub poprzez dedykowany portal Wykonawcy. Wykonawca zobowiązany jest w ciągu 2 godzin potwierdzić drogą elektroniczną otrzymanie od Zamawiającego zgłoszenia dokonanego drogą telefoniczną. Adres poczty elektronicznej, numer telefonu i adres dedykowanego portalu Wykonawca wskaże w umowie.
12.5.4.	Przewidywane czasy rozwiązania: • zgłoszonej Awarii to 2 dni robocze od momentu jej zgłoszenia przez Zamawiającego, • zgłoszonej Usterki to 10 dni roboczych od momentu jej zgłoszenia przez Zamawiającego, • Wady to 20 dni roboczych od momentu jej zgłoszenia przez Zamawiającego.
12.5.5.	W przypadku braku możliwości usunięcia Awarii, Usterki lub Wady przez Wykonawcę i konieczności przekazania zgłoszenia Zamawiającego do realizacji przez Producenta oprogramowania, jest ono przekazywane niezwłocznie i realizowane zgodnie z warunkami licencji oprogramowania oraz warunkami wsparcia technicznego Producenta oprogramowania. Czas usunięcia Awarii, Usterki lub Wady zostaje w takim przypadku wydłużony i wynosi: • dla Awarii nie później niż w terminie 4 dni roboczych od momentu otrzymania zgłoszenia od Zamawiającego, • dla Usterki nie później niż w terminie 20 dni roboczych od momentu otrzymania zgłoszenia od Zamawiającego, • dla Wady nie później niż w terminie 40 dni roboczych od momentu otrzymania zgłoszenia od Zamawiającego.
12.5.6.	Wykonawca zobowiązuje się, na żądanie Zamawiającego, udokumentować w ciągu 3 dni od zgłoszenia żądania fakt przesłania zgłoszenia do realizacji przez Producenta,
12.5.7.	Do biegu terminów określonych w ust. 4, nie wlicza się dni ustawowo wolnych od pracy oraz godzin od 16:00 do 8:00,
12.5.8.	Wykonawca zapewni dostęp do najnowszych wersji Oprogramowania.

II.13 Zakup systemu do zarządzania lukami w zabezpieczeniach

Opis ogólny

Przedmiotem zamówienia jest zakup i wdrożenie oprogramowania, które umożliwia kompleksowe i centralne zarządzanie podatnościami w infrastrukturze Zamawiającego, w tym automatyczne wykrywanie, ocenę i eliminację zagrożeń bezpieczeństwa IT.

Wymagania dotyczące licencji

Lp.	Wymagania minimalne
13.2.1.	Długość obowiązywania licencji: • licencja wieczysta
13.2.2.	Licencja obejmująca zarządzanie co najmniej: • 400 stacji roboczych • 20 serwerów • 1 Secure Gateway Server
13.2.3.	Liczba administratorów obsługujących aplikację: 3
13.2.4.	Dostęp do wsparcia i aktualizacji: • 36 miesięcy

Wymagania dotyczące oprogramowania

Lp.	Wymagania minimalne
13.3.1.	Oprogramowanie umożliwia jego instalację na systemie operacyjnym Windows i Windows Server
13.3.2.	Interfejs oprogramowania oraz konfiguracji jest w całości dostępny z poziomu przeglądarki internetowej (Microsoft Edge, Mozilla Firefox, Google Chrome) bez potrzeby instalacji tzw. grubego klienta.
13.3.3.	Aplikacja posiada wsparcie dla wielu języków w tym także dla języka polskiego.
13.3.4.	Architektura systemu jest agentowa
13.3.5.	Architektura systemu daje możliwość instalacji serwerów dystrybucyjnych w lokalizacjach zdalnych
13.3.6.	System powinien wspiera bazy danych: PostgreSQL 10.23 oraz MSSQL Server wersja2008 i późniejsze
13.3.7.	System posiada dwustopniową autoryzację
13.3.8.	System ma możliwość tworzenia Statycznych i Dynamicznych grup dla komputerów w wielu domenach
13.3.9.	System ma możliwość zarządzania systemami operacyjnymi: • Linux: ➢ Ubuntu 10.04 i nowsze, ➢ Debian 7 i nowsze, ➢ Red Hat Enterprise Linux 8 i nowsze, ➢ CentOS 8 i nowsze, ➢ Fedora 19 i nowsze, ➢ Mandriva 2010 i nowsze, ➢ Linux Mint 13 i nowsze, ➢ OpenSuSE 11 i nowsze,

	➢ SuSE Enterprise Linux 11 i nowsze • Mac OS: ➢ Snow Leopard, ➢ 10.7 – Lion, ➢ 10.8 - Mountain Lion, ➢ 10.9 – Mavericks, ➢ 10.10 – Yosemite, ➢ 10.11 - El Capitan, ➢ 10.12 – Sierra, ➢ 10.13 - High Sierra, ➢ 10.14 – Mojave, ➢ 11 Big Sur, ➢ 12 Monteray I nowsze • Windows OS: od 10 do 11
13.3.10.	System rozpoznaje stacje robocze w ramach sieci Active Directory oraz Workgroup
13.3.11.	System umożliwia instalację i deinstalację aktualizacji aplikacji
13.3.12.	System posiada możliwość aktualizacji zainstalowanych na stacjach roboczych i serwerach sterowników
13.3.13.	System ma wbudowane funkcje zarządzania i wdrażania łat systemowych i ServicePack na stacjach roboczych oraz serwerach Funkcje wdrażania obejmuje: • Systemy operacyjne Windows OS (10,11, Server 2016, 2019, 2022, 2025). • Microsoft Office • Google Chrome • Opera • Skype • Mozilla Firefox • Adobe Reader • Adobe Acrobat • Adobe Shockwave Player • Adobe Flash Player • Java • WinRar
13.3.14.	System ma możliwość włączenia opcji testowania i zatwierdzania poprawek na wybranej grupie komputerów testowych przed instalacją poprawek w całym środowisku produkcyjnym
13.3.15.	System ma wbudowane narzędzia rozpoznawania podatności stacji roboczych na zagrożenia w oparciu o brakujące łaty systemowe
13.3.16.	Architektura systemu umożliwia zarządzanie stacjami roboczymi w sieci LAN, WAN bezpośrednio z poziomu serwera centralnego
13.3.17.	System ma rozbudowany system zarządzania użytkownikami z podziałem na administratora, audytora, gościa, menadżera łat, z możliwością dodawania nowych ról z określonymi uprawnieniami
13.3.18.	System ma możliwość dodania nowego użytkownika systemu z uwierzytelnianiem lokalnym lub Active Directory
13.3.19.	System umożliwia generowanie następujących raportów: • Raportów dotyczących zagrożeń. • Raportów dotyczących wszystkich paczek • Raportów dotyczących zarządzanych zasobów

13.3.20.	System umożliwia planowanie raportów i przesyłanie ich w formie pliku PDF, XLSX, CSV na podany adres mailowy
13.3.21.	System umożliwia tworzenie niestandardowych raportów w oparciu o kryteria dostępne z systemu
13.3.22.	System umożliwia tworzenie niestandardowych raportów w oparciu o wysyłanie zapytań SQL do bazy danych z poziomu konsoli zarządzającej
13.3.23.	System jest wyposażony w funkcję zarządzania oceną podatności na zagrożenia. • Automatycznego skanowania zasobów z jednoczesnym wykrywaniem zasobów w domenie a także w WorkGrupie • System posiada możliwość wykrywania zagrożeń poprzez automatyczne lub manualne skanowanie zasobów objętych zarządzaniem.
13.3.24.	System posiada funkcję wykrywania luk systemowych takich jak • Aplikacje zbliżające się do końca wsparcia • Aplikacje typu peer to peer • Aplikację wykorzystywane do udostępniania zdalnego pulpitu • Zagrożeń typu Zero Day • Zagrożenia wynikające z: ➢ Ataków na strony URL ➢ Ataków typu „Denial of Service” ➢ Ataków typu “ Brute force” ➢ Przejęcie sesji ➢ Clicjacking ➢ Ujawnienie kodu źródłowego
13.3.25.	Audyt portów TCP i UDP oraz uruchomionych na nich usługach.
13.3.26.	System posiada możliwość zdalne zamykanie na komputerach z systemem Windows i Linux
13.3.27.	System posiada dodatkowo płatny moduł do zarządzania urządzeniami sieciowymi w zakresie: • Poszukiwania luk w oprogramowaniu Firmware • Naprawiania i zarządzania lukami w zabezpieczeniach • Odnajdywania urządzeń sieciowych w organizacji.
13.3.28.	System pozwala na integrację z rozwiązaniem ServiceDesk Plus

Wdrożenie i szkolenia

Lp.	Wymagania minimalne
13.4.1.	Przygotowanie przez Zamawiającego środowiska wskazanego przez Wykonawcę, koniecznego do wdrożenia systemu (serwer pod instalację oprogramowania, dedykowana skrzynka pocztowa z dostępem do IMAP/POP, konfiguracja reguł na firewallu, certyfikat SSL, itp.)
13.4.2.	Instalacja aplikacji oraz podpięcie otrzymanej licencji, opcjonalnie przepięcie systemu z domyślnej bazy PGSQL na MS SQL Server.
13.4.3.	Rekonfiguracja aplikacji w zakresie korzystania z protokołu https.
13.4.4.	Dodanie 2 techników z przygotowaniem dla nich ról.
13.4.5.	Przygotowanie agenta i dystrybucja za pomocą GPO (AD) lub manualnie na dwóch dostarczonych komputerach.
13.4.6.	Przygotowanie i dystrybucja dwóch aktualizacji (manualnych).
13.4.7.	Konfiguracja funkcji „Test and approve”.

13.4.8.	Przygotowanie jednego raportu i konfiguracja harmonogramu wykonania.
13.4.9.	Konfiguracja domeny Zamawiającego.
13.4.10.	Wstęp do obsługi aplikacji a także omówienie metod zapewnienia ciągłości działania (backup, restore, update).
13.4.11.	Instalacja aplikacji oraz podpięcie otrzymanej licencji, opcjonalnie przepięcie systemy z domyślnej bazy PGSQL na MS SQL Server.
13.4.12.	Wszystkie prace będą realizowane przy udziale lub w konsultacji z pracownikami Zamawiającego.

Warunki świadczenia gwarancji i serwisu

Lp	Wymagania minimalne
	Dostarczane oprogramowanie musi być objęte co najmniej 36 miesięczną asystą techniczną umożliwiającą: • nielimitowane wsparcie techniczne drogą mailową i systemem zdalnej pomocy w dni robocze w godzinach od 8:00 do 16:00 – bez dodatkowych opłat, • darmowy dostęp do podstawowych uaktualnień i poprawek w Oprogramowaniu, • możliwość aktualizacji głównej wersji oprogramowania bez dodatkowych opłat, • dostęp do portalu pomocy technicznej i bazy rozwiązań.
13.5.1.	W okresie ważności asysty technicznej Wykonawca zobowiązuje się usuwać, wszelkie Awarie, Usterki i Wady w działaniu ww. oprogramowania, bez dodatkowych opłat, • Awaria – błąd uniemożliwiający eksploatację Systemu i niepozwalający na znalezienie takiego sposobu używania Systemu, aby skutecznie obejść jego przyczyny, • Usterka – błąd, nie uniemożliwiający eksploatacji Systemu lub pozwalający na skuteczne obejście jego przyczyny, • Wada – błąd powodujący niewykonywanie lub nieprawidłowe wykonywanie funkcji określonych w specyfikacji technicznej Producenta.
13.5.2.	Zgłoszenia Awarii, Usterek i Wad przyjmowane będą w godzinach od 8:00 do 16:00, w dni robocze przez serwis Wykonawcy drogą telefoniczną, pocztą elektroniczną lub poprzez dedykowany portal Wykonawcy. Wykonawca zobowiązany jest w ciągu 2 godzin potwierdzić drogą elektroniczną otrzymanie od Zamawiającego zgłoszenia dokonanego drogą telefoniczną. Adres poczty elektronicznej, numer telefonu i adres dedykowanego portalu Wykonawca wskaże w umowie.
13.5.3.	Przewidywane czasy rozwiązania: • zgłoszonej Awarii to 2 dni robocze od momentu jej zgłoszenia przez Zamawiającego, • zgłoszonej Usterki to 10 dni roboczych od momentu jej zgłoszenia przez Zamawiającego, • Wady to 20 dni roboczych od momentu jej zgłoszenia przez Zamawiającego.
13.5.4.	W przypadku braku możliwości usunięcia Awarii, Usterki lub Wady przez Wykonawcę i konieczności przekazania zgłoszenia Zamawiającego do realizacji przez Producenta oprogramowania, jest ono przekazywane niezwłocznie i realizowane zgodnie z warunkami licencji oprogramowania oraz warunkami wsparcia technicznego Producenta oprogramowania. Czas usunięcia Awarii, Usterki lub Wady zostaje w takim przypadku wydłużony i wynosi: • dla Awarii nie później niż w terminie 4 dni roboczych od momentu otrzymania zgłoszenia od Zamawiającego, • dla Usterki nie później niż w terminie 20 dni roboczych od momentu otrzymania zgłoszenia od Zamawiającego,

	• dla Wady nie później niż w terminie 40 dni roboczych od momentu otrzymania zgłoszenia od Zamawiającego.
13.5.5.	Wykonawca zobowiązuje się, na żądanie Zamawiającego, udokumentować w ciągu 3 dni od zgłoszenia żądania fakt przesłania zgłoszenia do realizacji przez Producenta,
13.5.6.	Do biegu terminów określonych w ust. 4, nie wlicza się dni ustawowo wolnych od pracy oraz godzin od 16:00 do 8:00,
13.5.7.	Wykonawca zapewni dostęp do najnowszych wersji Oprogramowania.

II.14 Wsparcie serwisowe szpitalnego systemu informatycznego HIS

Stan obecny

Zamawiający posiada i użytkuje Szpitalny System Informatyczny firmy ASSECO POLSKA S.A. o nazwie AMMS. System ten posiada integrację z:

- Radiologicznym Systemem Informatycznym RIS firmy TMS-Soft o nazwie Viso
- Laboratoryjnym Systemem Informatycznym LIS firmy MARCEL S.A. o nazwie Centrum
- Laboratoryjnym Systemem Informatycznym LIS firmy Kaft - IT Tailored solutions o nazwie InteliLab
- System wspierający pracę Pracowni Endoskopowej firmy Varimed Sp. z o.o. o nazwie Endobox
- Systemem e-zdrowia (P1) oraz powiązanymi systemami umożliwiającymi gromadzenie, przetwarzanie i udostępnianie zasobów cyfrowych o zdarzeniach medycznych pacjentów oraz indeksów elektronicznej dokumentacji medycznej (EDM).

Lp.	Element Systemu	Koniec obecnego wsparcia
14.3.1.	AMMS Ruch Chorych - Izba Przyjęć, Oddział, Statystyka, Rozliczenia NFZ)	31/01/2026
14.3.2.	AMMS - Gruper JGP	31/01/2026
14.3.3.	AMMS - Optymalizator (symulator) JGP	31/01/2026
14.3.4.	AM MS - Apteka	31/01/2026
14.3.5.	AMMS - Apteczka Oddziałowa	31/01/2026
14.3.6.	AMMS - Punkt Pobrań	31/01/2026
14.3.7.	AMMS - Zlecenia	31/01/2026
14.3.8.	AMMS Interfejs HL7 HIS LIS Marcel mikrobiologia	31/01/2026
14.3.9.	AMMS Interfejs HL7 HIS LIS Marcel analityka	31/01/2026
14.3.10.	AMMS Interfejs HL7 HIS RIS Orion	31/01/2026
14.3.11.	AMMS Dokumentacja formularzowa	31/01/2026
14.3.12.	AMMS Pracownia Diagnostyczna	31/01/2026
14.3.13.	AMMS Lecznictwo otwarte (Recepcja, Gabinet, Statystyka LO, Kontrakty NFZ)	31/01/2026
14.3.14.	Rehabilitacja	17/10/2027
14.3.15.	Blok operacyjny	17/10/2027
14.3.16.	e-ZLA	17/10/2027

14.3.17.	e-Skierowanie	17/10/2027
14.3.18.	EDM AMDX	17/10/2027
14.3.19.	e-Rejestracja, e-Wiadomości, e-Dokumentacja, e-Wywiad, e-Świadczenia	17/10/2027
14.3.20.	e-Powiadomienia	17/10/2027
14.3.21.	Zarządzanie Dokumentacją Medyczną	17/10/2027
14.3.22.	Zdarzenia Medyczne	17/10/2027
14.3.23.	Integracja AMDX - LIS Marcel	17/10/2027
14.3.24.	Integracja AMDX - LIS Roche	17/10/2027
14.3.25.	Integracja AMDX - RIS TMS	17/10/2027

Ogólny opis

Przedmiotem zamówienia jest przedłużenie wsparcia serwisowego nadzoru autorskiego tego systemu na okres 36 miesięcy.

Zakres nadzoru autorskiego

14.3.1. W ramach nadzoru autorskiego, Wykonawca zapewnia:

Lp.	Wymagania minimalne
14.3.1.1.	Udostępnienie poprawek do Oprogramowania Aplikacyjnego, w przypadku stwierdzenia przez Zamawiającego błędu Oprogramowania Aplikacyjnego: 14.3.1.1.1. W przypadku Błędu Krytycznego Oprogramowania Aplikacyjnego: • czas reakcji Wykonawcy na zgłoszenie Zamawiającego (tj. czas od otrzymania zgłoszenia do chwili podjęcia przez Wykonawcę czynności zmierzających do naprawy zgłoszonego Błędu Krytycznego Oprogramowania Aplikacyjnego) wynosi 1 Dzień Roboczy; • czas udostępnienia Zamawiającemu odpowiednich poprawek Oprogramowania Aplikacyjnego wyniesie do 3 Dni Roboczych od chwili rozpoczęcia czynności serwisowych; • w przypadku wystąpienia Błędu Krytycznego Oprogramowania Aplikacyjnego Wykonawca może wprowadzić tzw. rozwiązanie tymczasowe, doraźnie rozwiązujące problem Błędu Krytycznego Oprogramowania Aplikacyjnego; w takim przypadku dalsza obsługa usunięcia dotychczasowego Błędu Krytycznego Oprogramowania Aplikacyjnego będzie traktowana jako Błąd Zwykły Oprogramowania Aplikacyjnego; 14.3.1.1.2. W pozostałych przypadkach, określanych jako Błędy Zwykłe Oprogramowania Aplikacyjnego: • czas reakcji Wykonawcy na zgłoszenie Zamawiającego (tj. czas od otrzymania zgłoszenia do chwili podjęcia przez Wykonawcę czynności zmierzających do naprawy zgłoszonego Błędu Zwykłego Oprogramowania Aplikacyjnego) wynosi do 15 dni roboczych; • czas udostępnienia Zamawiającemu odpowiednich poprawek Oprogramowania Aplikacyjnego wyniesie do 60 Dni Roboczych od chwili rozpoczęcia czynności serwisowych;

	14.3.1.1.3. Zamawiający udostępni Wykonawcy zdalny dostęp do baz danych i Oprogramowania Aplikacyjnego dla osób wykonujących prace na rzecz realizacji przez Wykonawcę Umowy. 14.3.1.1.4. W przypadku braku możliwości udostępnienia zdalnego dostępu, czas reakcji oraz czas udostępnienia poprawek zawierających korektę zgłoszonego błędu może ulec wydłużeniu o czas niezbędny do przekazania kopii bazy danych i czas niezbędny na jej uruchomienie w siedzibie Wykonawcy. 14.3.1.1.5. W wyjątkowych przypadkach, za zgodą Zamawiającego, czas dokonania poprawek Oprogramowania Aplikacyjnego może być uzgodniony pomiędzy Wykonawcą i Zamawiającym; 14.3.1.1.6. Wykonawca udostępni Zamawiającemu system do zgłaszania i obsługę błędów; w razie trudności z rejestracją zgłoszenia w takim systemie, Zamawiający może dokonać zgłoszenia telefonicznie lub poprzez e-mail, z zastrzeżeniem konieczności niezwłocznego potwierdzenia zgłoszenia przez Wykonawcę
14.3.1.2.	Wprowadzania zmian w Oprogramowaniu Aplikacyjnym, w zakresie dotyczącym istniejącej funkcjonalności Oprogramowania Aplikacyjnego objętego Umową, w zakresie wymaganym zmianami powszechnie obowiązujących przepisów prawa lub przepisów prawa wewnętrznie obowiązujących Zamawiającego, wydanych na podstawie delegacji ustawowej, z zastrzeżeniem, że Wykonawca zobowiązany jest do: 14.3.1.2.1. przekazania Zamawiającemu informacji o nowych wersjach Oprogramowania Aplikacyjnego; 14.3.1.2.2. udostępniania uaktualnień Oprogramowania Aplikacyjnego (nowych wersji Oprogramowania Aplikacyjnego) na serwerze ftp Wykonawcy
14.3.1.3.	Możliwość pisemnego zgłoszenia propozycji modyfikacji Oprogramowania Aplikacyjnego objętego Umową, w tym zgłoszeń propozycji zmian Oprogramowania Aplikacyjnego (propozycji jego udoskonaleń, modyfikacji i rozwoju) oraz zgłoszeń zmian obejmujących dodanie nowej funkcjonalności Oprogramowania Aplikacyjnego objętego Umową, w zakresie zmian powszechnie obowiązujących przepisów prawa lub przepisów prawa wewnętrznie obowiązujących Zamawiającego, wydanych na podstawie delegacji ustawowej.
14.3.1.4.	Zamawiający ma możliwość realizacji indywidualnych zmian w Oprogramowaniu Aplikacyjnym za dodatkowym wynagrodzeniem Wykonawcy, (Modyfikacje Płatne). Warunki realizacji Modyfikacji Płatnych i wysokość wynagrodzenia dla Wykonawcy będą każdorazowo uzgadniane pomiędzy Wykonawcą i Zamawiającym.

14.3.2. Wykonawca jest odpowiedzialny za działania lub zaniechania podwykonawcy, jego przedstawicieli lub pracowników, jak za własne działania lub zaniechania. Wykonawca jest zobowiązany do sprawowania na bieżąco nadzoru nad pracami wykonywanymi przez podwykonawcę i do ich koordynacji. Powierzenie wykonania części zamówienia podwykonawcom nie zwalnia Wykonawcy z odpowiedzialności za należyte wykonanie tego zamówienia.

14.3.3. Wykonawca musi posiadać autorskie prawa majątkowe do Oprogramowania Aplikacyjnego, którego dotyczy niniejsza Umowa oraz posiadać prawo do czerpania wynagrodzenia za korzystanie z niego przez osoby trzecie.

Rozwiązanie równoważne

Zamawiający dopuszcza wymianę obecnie wykorzystywanego Szpitalnego Systemu Informatycznego HIS na rozwiązanie równoważne, która zachowa wszystkie funkcjonalności i integracje obecnie

wykorzystywanego systemu z okresem wsparcia serwisowego, które jest przedmiotem tego postępowania.

II.15 Rozbudowa zintegrowanego systemu ochrony sieci

Stan obecny

Zamawiający posiada i użytkuje zintegrowany system ochrony sieci klasy Next Generation Firewall i UTM firmy Stormshield. System jest zbudowany w postaci klastra wysokiej dostępności HA (High Availability). System zbudowany jest na 2 urządzeniach Stormshield SN710 działających w trybie Active/Passive.

Ogólny opis

Przedmiotem zamówienia jest:

15.2.1. technical upgrade użytkowanego systemu do systemu opartego na urządzeniach nowszej generacji

15.2.2. przedłużenie okresu wsparcia na oba urządzenia na okres trwałości przedsięwzięcia

Wymagania dotyczące sprzętu

Lp.	Komponent	Wymagania minimalne
15.3.1.	Obsługa sieci	Urządzenie ma posiadać wsparcie dla protokołu IPv4 oraz IPv6 co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, firewall, systemu IPS oraz usług sieciowych takich jak np. DHCP.
15.3.2.	Zapora korporacyjna (Firewall)	Urządzenie ma być wyposażone w Firewall klasy Statefull Inspection.
15.3.3.		Urządzenie ma obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT.
15.3.4.		Urządzenie ma umożliwiać ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge).
15.3.5.		Interface (GUI) do konfiguracji firewall 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, port docelowy, etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie.
15.3.6.		Administrator ma mieć możliwość budowania reguł firewall na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, użytkownika bądź grupy z bazy LDAP, pola DSCP nagłówka pakietu, przypisania kolejki QoS, określenia limitu połączeń na sekundę, godziny oraz dnia nawiązywania połączenia.
15.3.7.		Urządzenie ma umożliwiać filtrowanie jedynie na poziomie warstwy 2 modelu OSI tj. na podstawie adresów mac.
15.3.8.		Administrator ma mieć możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł firewall.

15.3.9.		Edytor reguł firewall ma posiadać wbudowany analizator reguł, który wskazuje błędy i sprzeczności w konfiguracji reguł.
15.3.10.		Urządzenie ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę LDAP (wewnętrzną oraz zewnętrzną), zewnętrzny serwer RADIUS, zewnętrzny serwer Kerberos.
15.3.11.		Urządzenie ma umożliwiać wskazanie trasy routingu dla wybranej reguły niezależnie od innych tras routingu (np. routingu domyślnego).
15.3.12.		System musi umożliwiać budowanie reguł bezpieczeństwa w oparciu o definiowane przez administratora harmonogramy czasowe.
15.3.13.	System Zapobiegania Włamaniom (IPS)	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.
15.3.14.		Moduł IPS ma być opracowany przez producenta urządzenia. Nie dopuszcza się, aby moduł IPS pochodził od zewnętrznego dostawcy.
15.3.15.		Moduł IPS ma zabezpieczać przed co najmniej 10 000 ataków i zagrożeń.
15.3.16.		Administrator ma mieć możliwość tworzenia własnych sygnatur dla systemu IPS.
15.3.17.		Moduł IPS ma nie tylko wykrywać, ale również usuwać szkodliwą zawartość w kodzie HTML oraz JavaScript żądanej przez użytkownika strony internetowej nie blokując dostępu do tej strony po usunięciu zagrożenia.
15.3.18.		Urządzenie ma umożliwiać inspekcję ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, POP3S oraz SMTPS.
15.3.19.		Administrator 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.
15.3.20.		Urządzenie ma umożliwiać ochronę między innymi przed atakami typu SQL Injection, Cross Site Scripting (XSS) oraz złośliwym kodem Web2.0.
15.3.21.		Po zakupie stosownej licencji moduł IPS ma zapewniać analizę protokołów przemysłowych co najmniej takich jak: Modbus, UMAS, S7 200-300-400, EtherNet/IP, CIP, OPC UA, OPC (DA/HDA/AE), BACnet/IP, PROFINET, SOFBUS/LACBUS, IEC 60870-5-104, IEC 61850 (MMS, Goose & SV).
15.3.22.		Urządzenie musi zapewniać automatyczną aktualizację sygnatur kontekstowych.
15.3.23.	Kształtowanie pasma (Traffic Shapping)	Urządzenie ma umożliwiać kształtowanie pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma.
15.3.24.		Ograniczenie pasma lub priorytetyzacja reguły firewall ma być możliwe względem pojedynczego połączenia, adresu IP, zautoryzowanego użytkownika, pola DSCP.
15.3.25.		Urządzenie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma, a jedynie na śledzenie konkretnego typu ruchu (monitoring).
15.3.26.		Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch.

15.3.27.	Ochrona antywirusowa	Urządzenie ma umożliwić rozbudowę o zaawansowany skaner antywirusowy dostarczany przez firmy trzecie (innych niż producent rozwiązania).
15.3.28.		Po rozbudowie administrator ma mieć możliwość określenia akcji w przypadku wykrycia zagrożenia bądź, gdy analiza skanerem antywirusowym została zakończona błędem.
15.3.29.		Skaner antywirusowy ma pochodzić od europejskiego producenta.
15.3.30.		Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym.
15.3.31.		Po rozbudowie 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 wykrycia infekcji.
15.3.32.	Ochrona antyspamowa	Urządzenie ma posiadać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM).
15.3.33.		Ochrona antyspam ma działać w oparciu o: • białe/czarne listy, • DNS RBL, • Skaner heurystyczny
15.3.34.		W przypadku ochrony w oparciu o DNS RBL administrator ma mieć możliwość modyfikowania listy serwerów RBL znajdujących się w domyślnej konfiguracji urządzenia.
15.3.35.		Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin.
15.3.36.	Wirtualne sieci prywatne (VPN)	Urządzenie ma umożliwiać stworzenie sieci VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja).
15.3.37.		Urządzenie ma wspierać co najmniej następujące typy sieci VPN: • PPTP VPN, • IPSec VPN, • SSL VPN.
15.3.38.		SSL VPN ma działać co najmniej w trybach tunelu.
15.3.39.		Producent urządzenia ma umożliwiać pobranie klienta VPN współpracującego z oferowanym rozwiązaniem.
15.3.40.		Klient SSL VPN ma być dostępny z poziomu portalu uwierzytelniania (captive portal)
15.3.41.		Urządzenie ma umożliwiać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover).
15.3.42.		Urządzenie ma umożliwiać wsparcie dla technologii XAuth, Hub ‘n’ Spoke oraz modconf.
15.3.43.		Urządzenie ma umożliwiać tworzenie tuneli IPSec Policy Based oraz Route Based.
15.3.44.	Fliltr dostępu do stron www	Urządzenie ma posiadać wbudowany filtr URL.
15.3.45.		Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 50 kategorii tematycznych stron internetowych.
15.3.46.		Administrator ma mieć możliwość dodawania własnych kategorii URL.
15.3.47.		Administrator ma mieć możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru ma być przynajmniej:

		• blokowanie dostępu do adresu URL, • zezwolenie na dostęp do adresu URL, • blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora.
15.3.48.		Administrator ma mieć możliwość skonfigurowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony.
15.3.49.		Strona blokady ma umożliwiać wykorzystanie zmiennych środowiskowych.
15.3.50.		Filtr URL musi uwzględniać komunikację po protokole HTTPS.
15.3.51.		Urządzenie ma umożliwiać identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME.
15.3.52.		Urządzenie ma umożliwiać stworzenie listy stron dostępnych po protokole HTTPS, które nie będą deszyfrowane
15.3.53.		Urządzenie musi oferować możliwość filtrowania wyników wyszukiwania z użyciem SafeSearch
15.3.54.	Uwierzytelnianie	Urządzenie ma umożliwiać uwierzytelnianie użytkowników co najmniej w oparciu o: • lokalną bazę użytkowników (wewnętrzny LDAP), • zewnętrzną bazę użytkowników (zewnętrzny LDAP), • usługę katalogową Microsoft Active Directory.
15.3.55.		Urządzenie ma umożliwiać równoczesne użycie co najmniej 5 różnych baz LDAP.
15.3.56.		Urządzenie ma umożliwiać uruchomienie specjalnego portalu (captive portal), który ma zezwalać na autoryzację użytkowników co najmniej w oparciu o protokoły: • SSL, • Radius, • Kerberos.
15.3.57.		Urządzenie ma umożliwiać transparentną autoryzację użytkowników w usłudze katalogowej Microsoft Active Directory w oparciu o co najmniej dwa mechanizmy.
15.3.58.		Co najmniej jedna z metod transparentnej autoryzacji nie może wymagać instalacji dedykowanego agenta.
15.3.59.		Autoryzacja użytkowników z Microsoft Active Directory nie może wymagać modyfikacji schematu domeny.
15.3.60.		Rozwiązanie musi mieć możliwość transparentnego uwierzytelniania użytkowników w ramach infrastruktury VDI (Virtual Desktop Infrastructure) poprzez dedykowanego agenta. Metoda ta musi wspierać co najmniej technologie Citrix Virtual Apps i Microsoft Remote Desktop Services (RDS).
15.3.61.		Urządzenie musi posiadać wbudowany moduł zapewniający podwójne uwierzytelnianie 2FA poprzez zastosowanie czasowych haseł jednorazowych (TOTP).
15.3.62.		Wbudowany moduł 2FA musi dawać możliwość wykorzystania haseł TOTP w ramach tuneli SSLVPN, IPSec, jak również logowania do portalu uwierzytelniania, webowego interfejsu administracyjnego i SSH.
15.3.63.		Rozwiązanie musi zapewniać Zero-Trust Network Access (ZTNA), dając dostęp do zasobów na podstawie analizy polityk bezpieczeństwa w

		oparciu co najmniej o weryfikację wersji systemu operacyjnego, statusu zapory sieciowej czy zainstalowanego programu antywirusowego na stacji roboczej.
15.3.64.	Administracja łączami do internetu(ISP)	Urządzenie ma umożliwiać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing).
15.3.65.		Mechanizm równoważenia obciążenia łącza internetowego ma działać w oparciu o następujące dwa mechanizmy: • równoważenie względem adresu źródłowego, • równoważenie względem połączenia.
15.3.66.		Mechanizm równoważenia obciążenia ma uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu.
15.3.67.		Urządzenie ma umożliwiać przełączenie na łącze zapasowe w przypadku awarii łącza podstawowego (tzw. Failover).
15.3.68.		Urządzenie ma wspierać mechanizm SD-WAN zapewniając automatyczną optymalizację i wybór najkorzystniejszego łącza.
15.3.69.		W zakresie SD-WAN urządzenie ma zapewniać obsługę mechanizmu SLA (monitorowanie opóźnienia, jitter, wskaźnika utraty pakietów).
15.3.70.		Monitorowanie dostępności łącza musi być możliwe w oparciu o ICMP oraz TCP.
15.3.71.	Routing (Trasowanie)	Urządzenie ma umożliwiać statyczne trasowanie pakietów.
15.3.72.		Urządzenie ma umożliwiać trasowanie połączeń IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego.
15.3.73.		Urządzenie ma umożliwiać trasowanie pakietów z poziomu wybranej reguły firewall (tzw. Policy Based Routing).
15.3.74.		Urządzenie ma umożliwiać dynamiczne trasowanie pakietów w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP.
15.3.75.		Rozwiązanie musi dawać możliwość wybrania predefiniowalnego obiektu typu blackhole.
15.3.76.	Administracja urządzeniami	Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego.
15.3.77.		Interfejs konfiguracyjny ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być możliwa zarówno poprzez niezaszyfrowany protokół HTTP, jak zaszyfrowany protokół HTTPS.
15.3.78.		Administrator ma mieć możliwość wskazania do komunikacji innego portu niż 443 TCP.
15.3.79.		Urządzenie ma umożliwiać zarządzanie przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami.
15.3.80.		Urządzenie musi oferować możliwość wykorzystania wbudowanych profili administracyjnych określających dostęp do poszczególnych modułów systemu na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis.
15.3.81.		Urządzenie ma umożliwiać zarządzenia z poziomu konsoli (SSH)
15.3.82.		Urządzenie ma umożliwiać zarządzanie poprzez dedykowaną platformę centralnego zarządzania.
15.3.83.		Interfejs konfiguracyjny platformy centralnego zarządzania ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być zabezpieczona za pomocą protokołu HTTPS.

15.3.84.		Wbudowany webowy, graficzny interfejs administracyjny urządzenia musi oferować narzędzia diagnostyczne, co najmniej ping, traceroute, nslookup.
15.3.85.		Wbudowany webowy, graficzny interfejs administracyjny musi oferować narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych.
15.3.86.		Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość zdefiniowania polityki haseł stosowanych w całym systemie w zakresie minimalnej ilości znaków czy złożoności hasła.
15.3.87.		Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość generowania skryptów z czynności wykonywanych przez administratora (script recording).
15.3.88.		System musi oferować możliwość zdefiniowania własnych obiektów sieciowych, obiektów URL, certyfikatów, usług internetowych (web services).
15.3.89.		Urządzenie musi oferować portal uwierzytelniania (captive portal) dla użytkowników.
15.3.90.		Urządzenie ma umożliwiać zapisywanie logów na wbudowanym dysku.
15.3.91.		Urządzenie ma umożliwiać eksportowanie logów na zewnętrzny serwer (syslog) z wykorzystaniem transmisji nieszyfrowanej jak i szyfrowanej (TLS).
15.3.92.		Urządzenie ma umożliwiać eksportowanie logów za pomocą protokołu IPFIX.
15.3.93.		Urządzenie ma umożliwiać eksportowanie backupu konfiguracji (kopia zapasowa) co najmniej w zakresie: • manualnego eksportu do pliku w dowolnym momencie czasu, • automatycznego eksportu do chmury producenta lub na dedykowany serwer zarządzany przez administratora, z możliwością wyboru częstotliwości co najmniej: raz dziennie, raz w tygodniu, raz w miesiącu
15.3.94.		Urządzenie ma umożliwiać odtworzenie backupu konfiguracji pochodzącego bezpośrednio z serwerów producenta lub z dedykowanego serwera zarządzanego przez administratora.
15.3.95.		Urządzenie ma umożliwiać anonimizację logów co najmniej w zakresie adresu źródłowego oraz nazwy użytkownika.
15.3.96.		Rozwiązanie musi dawać możliwość ręcznej aktualizacji baz zabezpieczeń poprzez wskazanie pliku aktualizacji w trybie offline z poziomu interfejsu graficznego.
15.3.97.	Raportowanie	Urządzenie ma posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu.
15.3.98.		System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania.
15.3.99.		System raportowania ma posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego, skanera Antyspamowego.
15.3.100.		System raportowania ma umożliwiać wygenerowanie co najmniej 25 różnych raportów.

15.3.101.		System raportowania ma umożliwiać edycję konfiguracji bezpośrednio z poziomu raportu.
15.3.102.		System raportowania ma umożliwiać eksport wyników raportu do formatu CSV.
15.3.103.		Urządzenie musi posiadać możliwość rozbudowy o dedykowany system zbierania logów i tworzenia raportów w postaci wirtualnej maszyny pochodzący od tego samego producenta.
15.3.104.		Urządzenie ma umożliwiać monitorowanie swojego stanu w wykorzystanie protokołu SNMP w wersji 1, 2 i 3.
15.3.105.		Urządzenie ma umożliwiać monitorowanie ruchu sieciowego bezpośrednio w konsoli GUI, a także z poziomu konsoli (SSH).
15.3.106.	Pozostałe usługi i funkcje	Urządzenie ma umożliwiać stworzenie interfejsu zagregowanego w oparciu o protokół LACP.
15.3.107.		Urządzenie ma posiadać wbudowany serwer DHCP z możliwością dynamicznego przypisywania adresów jak i statycznego przypisywania adresu IP do adresu MAC karty sieciowej.
15.3.108.		Urządzenie ma pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP (tzw. DHCP Relay).
15.3.109.		Konfiguracja serwera DHCP ma być niezależna dla IPv4 i IPv6.
15.3.110.		Urządzenie ma umożliwiać stworzenia różnych konfiguracji DHCP dla różnych podsieci skonfigurowanych zarówno na interfejsach fizycznych jak i wirtualnych (VLAN) w zakresie określenia bramy, serwerów DNS, nazwy domeny)
15.3.111.		Urządzenie ma posiadać usługę DNS Proxy.
15.3.112.		Urządzenie ma posiadać wsparcie dla Spanning-tree protocol (RSTP/MSTP).
15.3.113.		Urządzenie musi oferować wsparcie dla IEEE 802.1Q VLAN.
15.3.114.		Urządzenie musi mieć zaimplementowane Open API.
15.3.115.		Urządzenie ma posiadać dwie niezależne partycje np. w celu zapewnienia działania na wypadek awarii podczas aktualizacji oprogramowania układowego (firmware). W tym celu ma być możliwe zsynchronizowanie aktywnej partycji z zapasową przed aktualizacją firmware lub w dowolnym innym momencie.
15.3.116.		Urządzenie musi oferować możliwość zwiększenia wydajności takich parametrów jak przepustowości firewall, IPS, Antywirus, VPN. Zwiększenie wydajności odbywa się wyłącznie przez zmianę licencji i nie wymaga ingerencji w komponenty fizyczne urządzenia czy wymianę samego urządzenia.
15.3.117.	Parametry sprzętowe	Rozwiązanie ma być dostarczone jako klaster HA dwóch urządzeń działających co najmniej w trybie Active/Passive
15.3.118.		Urządzenie ma być wyposażone w dysk SSD o pojemności co najmniej 240 GB.
15.3.119.		Urządzenie wyposażone jest w redundantne zasilanie z sygnalizacją pracy poszczególnych zasilaczy.
15.3.120.		Liczba portów Ethernet 2,5Gbps – min. 8, z możliwością rozszerzenia do 16.
15.3.121.		Liczba portów światłowodowych 10Gbps – min. 2 z możliwością rozszerzenia do 6.
15.3.122.		Urządzenie ma pozwalać na instalację modułu rozszerzeń z poniższej listy:

		• Moduł z 8 interfejsami miedzianymi 1Gbps • Moduł z 4 interfejsami miedzianymi 10Gbps • Moduł z 8 interfejsami miedzianymi 1Gbps (4 pary interfejsów w trybie bypass). • Moduł z 8 interfejsami miedzianymi 2,5Gbps. • Moduł z 8 interfejsami światłowodowymi 1Gbps. • Moduł z 4 interfejsami światłowodowymi 10Gbps. • Moduł z 2 interfejsami światłowodowymi 25Gbps.
15.3.123.		Urządzenie ma umożliwiać dostęp do Internetem za pomocą modemu 3G oraz 4G pochodzącego od dowolnego producenta.
15.3.124.		Urządzenie ma być wyposażone w min. 2, różniące się typem, porty konsolowe. Przynajmniej jeden port konsolowy ma być typu RJ45.
15.3.125.		Przepustowość Firewall (1518 bajtów UDP) – minimum 18Gbps.
15.3.126.		Przepustowość Firewall wraz z włączonym systemem IPS (1518 bajtów UDP) – minimum 10Gbps.
15.3.127.		Przepustowość filtrowania Antywirusowego – minimum 3Gbps.
15.3.128.		Przepustowość tunelu VPN przy szyfrowaniu AES-GCM – minimum 4Gbps.
15.3.129.		Liczba tuneli VPN IPSec – minimum 1 000.
15.3.130.		Liczba tuneli typu SSL VPN (tryb tunelu) – minimum 300.
15.3.131.		Obsługa interfejsów 802.11q (VLAN) – minimum 1336.
15.3.132.		Liczba równoczesnych sesji – minimum 1 000 000 i nie mniej niż 50 000 nowych sesji/sekundę.
15.3.133.		Rozwiązanie ma zostać dostarczone jako klaster HA dwóch urządzeń działających co najmniej w trybie Active/Passive
15.3.134.		Urządzenie musi być wyposażone w moduł TPM
15.3.135.		Urządzenie nie ma limitu na liczbę użytkowników.
15.3.136.		Liczba reguł filtrowania – minimum 32 768.
15.3.137.		Liczba tras statycznego routingu – minimum 5 120.
15.3.138.		Liczba tras dynamicznego routingu – minimum 10 000.
15.3.139.		Możliwość instalacji w szafie RACK 19”, wysokość urządzenia 1U.
15.3.140.		Zakres wdrożenia systemu typu Firewall: • rejestracja urządzeń • stworzenie klastra urządzeń • aktualizacja do najnowszej zalecanej wersji oprogramowania • adresacja IP urządzeń • stworzenie segmentów sieci (VLANów) • stworzenie LACP • stworzenie przykładowych polityk zezwalających na ruch pomiędzy segmentami • stworzenie profili bezpieczeństwa jak antywirus kontrola stron internetowych, kontrola aplikacji, kontrola plików • stworzenie przykładowego połączenia VPN • szkolenie • podłączenie do przełączników

Wymagania dotyczące wsparcia serwisowego

Lp.	Warunki gwarancji i serwisu
15.4.1.	Serwis podstawowy na oba urządzenia z gwarancją producenta na dostarczone elementy systemu oraz licencją dla wszystkich funkcji bezpieczeństwa na okres 36 miesięcy
15.4.2.	Zamawiający wymaga, aby naprawy gwarancyjne były wykonywane przez serwis posiadający autoryzację producenta.
15.4.3.	W okresie obowiązywania gwarancji ma być zapewnione wsparcie techniczne świadczone co najmniej drogą e-mail lub przez dedykowany do tego portal.
15.4.4.	W przypadku awarii: • Okres dostępności serwisu - 24/7/365 • Rozwiązanie zastępcze – niezwłocznie, nie później niż 2 dni od dnia przyjęcia zgłoszenia • Czas reakcji serwisu - niezwłocznie, nie później niż 4 godziny od czasu przyjęcia zgłoszenia • Czas naprawy - niezwłocznie nie później niż 4 dni roboczych od dnia przyjęcia zgłoszenia
15.4.5.	W przypadku usterki: • Okres dostępności serwisu - 24/7/365 • Rozwiązanie zastępcze – niezwłocznie nie później niż 3 dni roboczych od dnia przyjęcia zgłoszenia • Czas reakcji serwisu - niezwłocznie, nie później niż 24 godziny od czasu przyjęcia zgłoszenia • Czas naprawy - niezwłocznie nie później niż 5 dni roboczych od dnia przyjęcia zgłoszenia

Rozwiązanie równoważne

Zamawiający dopuszcza wymianę obecnie wykorzystywanego systemu ochrony sieci na rozwiązanie równoważne, które zachowa wszystkie funkcjonalności obecnie wykorzystywanego systemu i funkcjonalności modułów, które są przedmiotem tego postępowania z okresem wsparcia serwisowego, które jest przedmiotem tego postępowania.
System musi być zbudowany w postaci klastra wysokiej dostępności HA (High Availability) i działać w trybie Active/Passive.

Wymagania dla systemu ochrony sieci (stan przed realizacją tego zadania):

Lp.	Komponent	Wymagania minimalne
15.5.1.	Obsługa sieci	Urządzenie ma posiadać wsparcie dla protokołu IPv4 oraz IPv6 co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, firewall, systemu IPS oraz usług sieciowych takich jak np. DHCP.
15.5.2.	Zapora korporacyjna (Firewall)	Urządzenie ma być wyposażone w Firewall klasy Statefull Inspection.
15.5.3.		Urządzenie ma obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT.
15.5.4.		Urządzenie ma umożliwiać ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge).
15.5.5.		Interface (GUI) do konfiguracji firewall 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, port docelowy, etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie.
15.5.6.		Administrator ma mieć możliwość budowania reguł firewall na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, użytkownika bądź grupy z bazy LDAP, pola DSCP nagłówka pakietu, przypisania kolejki QoS, określenia limitu połączeń na sekundę, godziny oraz dnia nawiązywania połączenia.
15.5.7.		Urządzenie ma umożliwiać filtrowanie jedynie na poziomie warstwy 2 modelu OSI tj. na podstawie adresów mac.
15.5.8.		Administrator ma mieć możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł firewall.
15.5.9.		Edytor reguł firewall ma posiadać wbudowany analizator reguł, który wskazuje błędy i sprzeczności w konfiguracji reguł.
15.5.10.		Urządzenie ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę LDAP (wewnętrzną oraz zewnętrzną), zewnętrzny serwer RADIUS, zewnętrzny serwer Kerberos.
15.5.11.		Urządzenie ma umożliwiać wskazanie trasy routingu dla wybranej reguły niezależnie od innych tras routingu (np. routingu domyślnego).
15.5.12.	System Zapobiegania Włamaniom (IPS)	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.
15.5.13.		Moduł IPS ma być opracowany przez producenta urządzenia. Nie dopuszcza się, aby moduł IPS pochodził od zewnętrznego dostawcy.
15.5.14.		Moduł IPS ma zabezpieczać przed co najmniej 10 000 ataków i zagrożeń.
15.5.15.		Administrator ma mieć możliwość tworzenia własnych sygnatur dla systemu IPS.
15.5.16.		Moduł IPS ma nie tylko wykrywać, ale również usuwać szkodliwą zawartość w kodzie HTML oraz JavaScript żądanej przez użytkownika strony internetowej nie blokując dostępu do tej strony po usunięciu zagrożenia.
15.5.17.		Urządzenie ma umożliwiać inspekcję ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, FTPS, POP3S oraz SMTPS.
15.5.18.		Administrator 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.
15.5.19.		Urządzenie ma umożliwiać ochronę między innymi przed atakami typu SQL Injection, Cross Site Scripting (XSS) oraz złośliwym kodem Web2.0.
15.5.20.		Po zakupie stosownej licencji moduł IPS ma zapewniać analizę protokołów przemysłowych co najmniej takich jak: Modbus, UMAS, S7 200-300-400, EtherNet/IP, CIP, OPC UA, OPC (DA/HDA/AE), BACnet/IP, PROFINET, SOFBUS/LACBUS, IEC 60870-5-104, IEC 61850 (MMS, Goose & SV).

15.5.21.		Urządzenie ma posiadać moduł pasywnego skanera wnętrza sieci, który to skanuje wnętrze sieci w poszukiwaniu jej słabych punktów i potencjalnych zagrożeń.
15.5.22.		Moduł musi wykrywać typ i wersję oprogramowania sieciowego, którego ruch jest filtrowany przez urządzenie.
15.5.23.		Moduł musi działać na urządzeniu. Nie dopuszcza się stosowania rozwiązania z agentem instalowanym na komputerach w sieci.
15.5.24.		Moduł ma nie tylko wykrywać oprogramowanie, ale również wykrywać i informować o lukach i podatnościach występujących w wykrytym oprogramowaniu
15.5.25.	Kształtowanie pasma (Traffic Shapping)	Urządzenie ma umożliwiać kształtowanie pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma.
15.5.26.		Ograniczenie pasma lub priorytetyzacja reguły firewall ma być możliwe względem pojedynczego połączenia, adresu IP, zautoryzowanego użytkownika, pola DSCP.
15.5.27.		Urządzenie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma, a jedynie na śledzenie konkretnego typu ruchu (monitoring).
15.5.28.		Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch.
15.5.29.	Ochrona antywirusowa	Urządzenie ma umożliwiać zastosowanie jednego z co najmniej dwóch skanerów antywirusowych dostarczonych przez firmy trzecie (innych niż producent rozwiązania).
15.5.30.		Co najmniej jeden z dwóch skanerów antywirusowych ma być dostarczany w ramach podstawowej licencji.
15.5.31.		Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym.
15.5.32.		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 wykrycia infekcji.
15.5.33.	Ochrona antyspamowa	Urządzenie ma posiadać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM).
15.5.34.		Ochrona antyspam ma działać w oparciu o: • białe/czarne listy, • DNS RBL, • Skaner heurystyczny
15.5.35.		W przypadku ochrony w oparciu o DNS RBL administrator ma mieć możliwość modyfikowania listy serwerów RBL znajdujących się w domyślnej konfiguracji urządzenia.
15.5.36.		Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin.
15.5.37.	Wirtualne sieci prywatne (VPN)	Urządzenie ma umożliwiać stworzenie sieci VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja).
15.5.38.		Urządzenie ma wspierać co najmniej następujące typy sieci VPN: • PPTP VPN, • IPSec VPN, • SSL VPN.
15.5.39.		SSL VPN ma działać co najmniej w trybach tunelu i portalu.

15.5.40.		Producent urządzenia ma umożliwiać pobranie klienta VPN współpracującego z oferowanym rozwiązaniem.
15.5.41.		Urządzenie ma umożliwiać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover).
15.5.42.		Urządzenie ma umożliwiać wsparcie dla technologii XAuth, Hub ‘n’ Spoke oraz modconf.
15.5.43.		Urządzenie ma umożliwiać tworzenie tuneli IPSec Policy Based oraz Route Based.
15.5.44.	FIiltr dostępu do stron www	Urządzenie ma posiadać wbudowany filtr URL.
15.5.45.		Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 50 kategorii tematycznych stron internetowych.
15.5.46.		Administrator ma mieć możliwość dodawania własnych kategorii URL.
15.5.47.		Administrator ma mieć możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru ma być przynajmniej: • blokowanie dostępu do adresu URL, • zezwolenie na dostęp do adresu URL, • blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora.
15.5.48.		Administrator ma mieć możliwość skonfigurowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony.
15.5.49.		Strona blokady ma umożliwiać wykorzystanie zmiennych środowiskowych.
15.5.50.		Filtr URL musi uwzględniać komunikację po protokole HTTPS.
15.5.51.		Urządzenie ma umożliwiać identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME.
15.5.52.		Urządzenie ma umożliwiać stworzenie listy stron dostępnych po protokole HTTPS, które nie będą deszyfrowane
15.5.53.	Uwierzytelnianie	Urządzenie ma umożliwiać uwierzytelnianie użytkowników co najmniej w oparciu o: • lokalną bazę użytkowników (wewnętrzny LDAP), • zewnętrzną bazę użytkowników (zewnętrzny LDAP), • usługę katalogową Microsoft Active Directory.
15.5.54.		Urządzenie ma umożliwiać równoczesne użycie co najmniej 5 różnych baz LDAP.
15.5.55.		Urządzenie ma umożliwiać uruchomienie specjalnego portalu (captive portal), który ma zezwalać na autoryzację użytkowników co najmniej w oparciu o protokoły: • SSL, • Radius, • Kerberos.
15.5.56.		Urządzenie ma umożliwiać transparentną autoryzację użytkowników w usłudze katalogowej Microsoft Active Directory w oparciu o co najmniej dwa mechanizmy.
15.5.57.		Co najmniej jedna z metod transparentnej autoryzacji nie może wymagać instalacji dedykowanego agenta.
15.5.58.		Autoryzacja użytkowników z Microsoft Active Directory nie może wymagać modyfikacji schematu domeny.

15.5.59.	Administracja łączami do internetu(ISP)	Urządzenie ma umożliwiać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing).
15.5.60.		Mechanizm równoważenia obciążenia łącza internetowego ma działać w oparciu o następujące dwa mechanizmy: • równoważenie względem adresu źródłowego, • równoważenie względem połączenia.
15.5.61.		Mechanizm równoważenia obciążenia ma uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu.
15.5.62.		Urządzenie ma umożliwiać przełączenie na łącze zapasowe w przypadku awarii łącza podstawowego (tzw. Failover).
15.5.63.		Urządzenie ma wspierać mechanizm SD-WAN zapewniając automatyczną optymalizację i wybór najkorzystniejszego łącza.
15.5.64.		W zakresie SD-WAN urządzenie ma zapewniać obsługę mechanizmu SLA (monitorowanie opóźnienia, jitter, wskaźnika utraty pakietów).
15.5.65.		Monitorowanie dostępności łącza musi być możliwe w oparciu o ICMP oraz TCP.
15.5.66.	Routing (Trasowanie)	Urządzenie ma umożliwiać statyczne trasowanie pakietów.
15.5.67.		Urządzenie ma umożliwiać trasowanie połączeń IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego.
15.5.68.		Urządzenie ma umożliwiać trasowanie pakietów z poziomu wybranej reguły firewall (tzw. Policy Based Routing).
15.5.69.		Urządzenie ma umożliwiać dynamiczne trasowanie pakietów w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP.
15.5.70.	Administracja urządzeniami	Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego.
15.5.71.		Interfejs konfiguracyjny ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być możliwa zarówno poprzez niezaszyfrowany protokół HTTP, jak zaszyfrowany protokół HTTPS.
15.5.72.		Administrator ma mieć możliwość wskazania do komunikacji innego portu niż 443 TCP.
15.5.73.		Urządzenie ma umożliwiać zarządzanie przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami.
15.5.74.		Urządzenie ma umożliwiać zarządzenia z poziomu konsoli (SSH)
15.5.75.		Urządzenie ma umożliwiać zarządzanie poprzez dedykowaną platformę centralnego zarządzania.
15.5.76.		Interfejs konfiguracyjny platformy centralnego zarządzania ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być zabezpieczona za pomocą protokołu HTTPS.
15.5.77.		Urządzenie ma umożliwiać zapisywanie logów na wbudowanym dysku.
15.5.78.		Urządzenie ma umożliwiać eksportowanie logów na zewnętrzny serwer (syslog) z wykorzystaniem transmisji nieszyfrowanej jak i szyfrowanej (TLS).
15.5.79.		Urządzenie ma umożliwiać eksportowanie logów za pomocą protokołu IPFIX.
15.5.80.		Urządzenie ma umożliwiać eksportowanie backupu konfiguracji (kopia zapasowa) co najmniej w zakresie: • manualnego eksportu do pliku w dowolnym momencie czasu,

		• automatycznego eksportu do chmury producenta lub na dedykowany serwer zarządzany przez administratora, z możliwością wyboru częstotliwości co najmniej: raz dziennie, raz w tygodniu, raz w miesiącu
15.5.81.		Urządzenie ma umożliwiać odtworzenie backupu konfiguracji bezpośrednio z serwerów chmury producenta lub z dedykowanego serwera zarządzanego przez administratora.
15.5.82.		Urządzenie ma umożliwiać anonimizację logów co najmniej w zakresie adresu źródłowego oraz nazwy użytkownika.
15.5.83.	Raportowanie	Urządzenie ma posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu.
15.5.84.		System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania.
15.5.85.		System raportowania ma posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego, skanera Antyspamowego.
15.5.86.		System raportowania ma umożliwiać wygenerowanie co najmniej 25 różnych raportów.
15.5.87.		System raportowania ma umożliwiać edycję konfiguracji bezpośrednio z poziomu raportu.
15.5.88.		Urządzenie musi posiadać możliwość rozbudowy o dedykowany system zbierania logów i tworzenia raportów w postaci wirtualnej maszyny pochodzący od tego samego producenta.
15.5.89.		Urządzenie ma umożliwiać monitorowanie swojego stanu w wykorzystanie protokołu SNMP w wersji 1, 2 i 3.
15.5.90.		Urządzenie ma umożliwiać monitorowanie ruchu sieciowego bezpośrednio w konsoli GUI, a także z poziomu konsoli (SSH).
15.5.91.	Pozostałe usługi i funkcje	Urządzenie ma umożliwiać stworzenie interfejsu zagregowanego w oparciu o protokół LACP.
15.5.92.		Urządzenie ma posiadać wbudowany serwer DHCP z możliwością dynamicznego przypisywania adresów jak i statycznego przypisywania adresu IP do adresu MAC karty sieciowej.
15.5.93.		Urządzenie ma pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP (tzw. DHCP Relay).
15.5.94.		Konfiguracja serwera DHCP ma być niezależna dla IPv4 i IPv6.
15.5.95.		Urządzenie ma umożliwiać stworzenia różnych konfiguracji DHCP dla różnych podsieci w zakresie określenia bramy, serwerów DNS, nazwy domeny.
15.5.96.		Urządzenie ma posiadać usługę DNS Proxy.
15.5.97.		Urządzenie ma posiadać wsparcie dla Spanning-tree protocol (RSTP/MSTP).
15.5.98.		Urządzenie ma posiadać dwie niezależne partycje np. w celu zapewnienia działania na wypadek awarii podczas aktualizacji oprogramowania układowego (firmware). W tym celu ma być możliwe zsynchronizowanie aktywnej partycji z zapasową przed aktualizacją firmware lub w dowolnym innym momencie.
15.5.99.	Parametry sprzętowe	Rozwiązanie ma być dostarczone jako klaster HA dwóch urządzeń działających co najmniej w trybie Active/Passive
15.5.100.		Urządzenie ma być wyposażone w dysk SSD o pojemności co najmniej 240 GB.

15.5.101.		Liczba portów Ethernet 10/100/1000Mbps – min. 8, z możliwością rozszerzenia do 16.
15.5.102.		Urządzenie ma pozwalać na instalację modułu rozszerzeń z poniższej listy: • Moduł z 8 interfejsami miedzianymi 10/100/1000Mbps • Moduł z 4 interfejsami miedzianymi 10Gbps • Moduł z 8 interfejsami światłowodowymi 1Gbps • Moduł z 4 interfejsami światłowodowymi 10Gbps
15.5.103.		Urządzenie ma umożliwiać dostęp do Internetem za pomocą modemu 3G oraz 4G pochodzącego od dowolnego producenta.
15.5.104.		Przepustowość Firewall (1518 bajtów UDP) – minimum 15Gbps.
15.5.105.		Przepustowość Firewall wraz z włączonym systemem IPS (1518 bajtów UDP) – minimum 8Gbps.
15.5.106.		Przepustowość filtrowania Antywirusowego – minimum 2Gbps.
15.5.107.		Przepustowość tunelu VPN przy szyfrowaniu AES-GCM – minimum 3Gbps.
15.5.108.		Maksymalna liczba tuneli VPN IPSec – minimum 1 000.
15.5.109.		Maksymalna liczba tuneli typu SSL VPN (tryb tunelu) – minimum 150.
15.5.110.		Maksymalna liczba tuneli typu SSL VPN (tryb portalu) – minimum 150.
15.5.111.		Obsługa interfejsów 802.11q (VLAN) – minimum 256.
15.5.112.		Liczba równoczesnych sesji – minimum 1 000 000 i nie mniej niż 50 000 nowych sesji/sekundę.
15.5.113.		Urządzenie nie ma limitu na liczbę użytkowników.
15.5.114.		Liczba reguł filtrowania – minimum 16 384.
15.5.115.		Liczba tras statycznego routingu – minimum 2 048.
15.5.116.		Liczba tras dynamicznego routingu – minimum 10 000.
15.5.117.		Możliwość instalacji w szafie RACK 19”, wysokość urządzenia 1U.

II.16 Szkolenia z zakresu cyberbezpieczeństwa

Cel zamówienia

Celem zamówienia jest przeprowadzenie cyklu szkoleń w zakresie cyberbezpieczeństwa dla:

16.1.1. Kadry kierowniczej szpitala z zakresu:
- Podstaw prawnych w obszarze cyberbezpieczeństwa
- Typów ataków wraz z przykładami
- Reagowania na incydenty
- Wykonywania testów bezpieczeństwa.
- Roli kadry zarządzającej w procesach bezpieczeństwa
- Innych bieżących zagrożeń

16.1.2. Pracowników administracji i pracowników medycznych z zakresu:
- Podstawowych zasad cyberhigieny
- Typów ataków wraz z przykładami
- Reagowania na incydenty
- Odpowiedzialności prawnej
- Innych bieżących zagrożeń

Opis ogólny

Przedmiotem zamówienia jest kompleksowa usługa podnoszenia świadomości i kompetencji cyberbezpieczeństwa w Regionalnym Szpitalu w Kołobrzegu wraz z dostawą materiałów szkoleniowych i realizacją szkoleń uzupełniających przez okres 36 miesięcy. Szkolenia muszą być w dwóch formach:

- w postaci szkolenia stacjonarnego w siedzibie Zamawiającego dla kadry zarządzającej (jedno szkolenie w roku, przez okres 36 miesięcy),
- w postaci e-learningu dla pracowników medycznych i administracji Zamawiającego.

Wymagania w stosunku do szkolenia stacjonarnego dla kadry kierowniczej z zakresu cyberbezpieczeństwa

Lp.	Parametr (wymagania minimalne)
16.3.1.	Szkolenia zostaną przeprowadzone w formie stacjonarnej w siedzibie Zamawiającego dla maksymalnie 40 Uczestników w jednej grupie.
16.3.2.	Jednostką czasową szkolenia jest 1 godzina szkoleniowa (45 minut).
16.3.3.	Zamawiający oczekuje szkolenia dla 3 grup szkoleniowych przeprowadzonych w jednym dniu, w godzinach 8.00 – 15.00 w terminie uzgodnionym przez Zamawiającego. Szkolenia będą trwały po 2h dla każdej grupy z przerwą 15 minutową między sesjami.
16.3.4.	Szkolenia będą prowadzone w języku polskim.
16.3.5.	Szkolenia prowadzone będą na podstawie zaakceptowanego przez Zamawiającego harmonogramu zawierającego zakres merytoryczny, dostarczonego przez Wykonawcę Zamawiającemu przed podpisaniem umowy.
16.3.6.	Zamawiający w ramach postępowania planuje zakup 3 szkoleń (jedno szkolenie w roku, odbywające się w pierwszych kwartałach roku 2026, 2027 i 2028).
16.3.7.	Minimalny zakres tematyczny szkolenia: 16.3.7.1. Wprowadzenie do tematyki związanej z ochroną przed cyberzagrożeniami. Bezpieczeństwo informacji w świetle rozwijających się technologii. 16.3.7.2. System zarządzania bezpieczeństwem informacji wynikających z ISO/IEC 27001, a cyberbezpieczeństwo. Kluczowe obszary. 16.3.7.3. Przegląd zagrożeń dla bezpieczeństwa informacji przetwarzanych formą tradycyjną oraz elektroniczną. 16.3.7.4. Źródła zagrożeń związanych z bezpieczeństwem informacji oraz ich klasyfikacja w oparciu o możliwe zdarzenia i straty dla organizacji. 16.3.7.5. Zarządzanie ryzykiem, jako kluczowy element ochrony. Podejście praktyczne. 16.3.7.6. Typy ataków - najczęstsze praktyki i sposoby wyłudzania, oszustw lub kradzieży informacji z organizacji: • wykradanie danych, • phishing i zaawansowane techniki wykorzystywane przez cyberprzestępców, • ataki socjotechniczne, • malware, • kontrola dostępu, • działania pracowników wewnętrznych na szkodę organizacji, • techniki manipulacji, • biały wywiad, • ataki destrukcyjne,

	16.3.7.7. Studium przypadku: atak ukierunkowany (APT) na osoby zarządzające i zbudowanie planu ataku. 16.3.7.8. Podstawy prawne w obszarze cyberbezpieczeństwa 16.3.7.9. Reagowanie na incydenty 16.3.7.10. Wykonywania badań bezpieczeństwa 16.3.7.11. Rola kadry zarządzającej w procesach bezpieczeństwa
16.3.8.	Osoba prowadząca szkolenie winna posiadać ważne na dzień realizacji szkolenia certyfikaty: • Audytor wiodący ISO/IEC 27001:2022 Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności • Audytor wiodący ISO/IEC 27701 - System Zarządzania Informacjami o Prywatności • Audytor wiodący ISO/IEC 27018 – Kodeks postępowania w zakresie ochrony informacji umożliwiających identyfikację osoby w chmurach publicznych działających jako podmioty przetwarzające PII
16.3.9.	Osoby uczestniczące w szkoleniu muszą otrzymać imienny certyfikat uczestnictwa przesłany w formie elektronicznej w ciągu 14 dni po jego ukończeniu.

Wymagania w stosunku do szkoleń w postaci e-learningu dla pracowników administracji i pracowników medycznych z zakresu cyberbezpieczeństwa

Lp.	Parametr (wymagania minimalne)
16.4.1.	zkolenia muszą być w formie gotowego produktu dostarczanego Zamawiającemu w ciągu 14 dni od podpisania umowy. Zamawiający musi mieć możliwość swobodnego wykorzystania szkoleń bez ograniczeń czasowych oraz liczby uczestników. Szkolenie powinno być dostarczone w modelu on premises, jako licencja wieczysta z możliwością instalacji szkolenia w infrastrukturze Zamawiającego na platformie e-learningowej Moodle.
16.4.2.	Szkolenie musi być w postaci oddzielnych lekcji dla każdej z kategorii z niżej opisanego zakresu. Jedna lekcja szkolenia powinna zawierać minimum 30 slajdów. Czas jednej lekcji (tematu) powinien oscylować w granicach 20-30 min. Lekcje powinny być multimedialne z wykorzystaniem scenek rodzajowych z możliwością odtworzenia w postaci dźwiękowej z użyciem lektora. Nie mogą to być same zdjęcia, definicje lub zagadnienia opisane w formie tekstowej i odtwarzane w postaci dźwiękowej. Podczas lekcji powinna być na bieżąco weryfikowana wiedza użytkownika poprzez np. ćwiczenia sprawdzające. Szkolenie nie może być w formie video learningu, tzn. z nagranym i odtworzonym ekspertem.
16.4.3.	Szkolenie musi posiadać oddzielne lekcje dla co najmniej następujących zagadnień: 16.4.3.1. Zakres tematyczny dla bezpieczeństwa teleinformatycznego A. Czym jest bezpieczeństwo informacji; B. Aspekty prawne związane z bezpieczeństwem informacji; C. Phishing; D. Zasady korzystania z Internetu; E. Zasady korzystania z portali społecznościowych; F. Zasady korzystania z poczty elektronicznej i zagrożenia z tym związane; G. Zasady korzystania z bezpiecznych haseł; H. Zagrożenia i sposoby zabezpieczania sprzętu mobilnego; I. Metody pozyskiwania informacji (socjotechnika); J. Bezpieczeństwo w zakresie płatności elektronicznych;

	K. Bezpieczeństwo fizyczne w zakresie zabezpieczania pomieszczeń, dokumentacji, sprzętu IT; L. Ransomware; M. Menedżer haseł; N. Techniki stosowane przez cyberprzestępców; O. Uważaj by nie zostać „mułem finansowym”; P. Bezpieczeństwo w sieciach bezprzewodowych; Q. Praca zdalna; R. Vishing; S. Bezpieczeństwo danych podczas rozmowy telefonicznej; T. Fake news i dezinformacja; U. Cloud – praca w chmurze; V. NIS 2 - nowa dyrektywa UE - nowy poziom bezpieczeństwa; W. Spoofing; X. Wprowadzenie do ochrony danych osobowych; Y. RODO w sektorze zdrowia.
16.4.4.	Szkolenie musi posiadać atrakcyjną formę przekazu materiału, zachęcającą osoby uczące się do aktywnego odbywania szkolenia. Zamawiający wymaga atrakcyjnej formy przekazu materiału szkolenia. Atrakcyjna forma to m.in. grafika oparta na scenkach, postaciach, dialogach, przykładach, ćwiczeniach, testach sprawdzających wiedzę oraz dźwięk – głos lektorów indywidualny dla każdej z postaci występujących w szkoleniu.
16.4.5.	Szkolenie musi posiadać interaktywną formę, zwiększającą zaangażowanie osób uczących się. Szkolenie musi zostać wyposażone w elementy interakcji (np. kliknięcia, ćwiczenia), tak aby uczestnik był aktywny podczas szkolenia i nie miał możliwości zaliczenia szkolenia w sposób bierny tj. poprzez samoczynne odtworzenia filmu / szkolenia.
16.4.6.	Lekcje szkolenia muszą kłaść duży nacisk na umiejętności praktyczne, nie tylko teorię bezpieczeństwa IT. W celu zwiększenia praktycznej przydatności szkolenia musi ono zostać opracowane tak, aby zajęcia kładły większy nacisk na umiejętności praktyczne użytkowników komputerów (np. wykrywanie sytuacji zagrożenia w trakcie korzystania z serwisów społecznościowych, właściwe postępowanie w razie incydentu) niż samą teorię bezpieczeństwa IT.
16.4.7.	Cały materiał szkolenia musi być dostępny w języku polskim i przedstawiony w sposób zrozumiały przez osoby nietechniczne.
16.4.8.	Szkolenie musi posiadać wysoką jakość merytoryczną przygotowanego scenariusza. Scenariusz szkolenia musi zostać opracowany we współpracy z ekspertem bezpieczeństwa IT posiadającym certyfikaty: • Audytor wiodący ISO/IEC 27001:2022 Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności • Audytor wiodący ISO/IEC 27701 - System Zarządzania Informacjami o Prywatności • Audytor wiodący ISO/IEC 27018 – Kodeks postępowania w zakresie ochrony informacji umożliwiających identyfikację osoby w chmurach publicznych działających jako podmioty przetwarzające PII
16.4.9.	Wymagania techniczne: Szkolenie w wersji elektronicznej musi być zgodne ze standardem umożliwiającym prezentację na platformie MOODLE w wersji 4.0 lub wyższej. Szkolenie powinno być dostarczone w technologii HTML5. Szkolenia powinny być podzielone tematycznie w taki sposób, aby można było operować (zarządzać dostępnością, harmonogramem, itp.) poszczególnymi tematami z osobna.

16.4.10.	Warunki licencji: Wykonawca udzieli Zamawiającemu wieczystej, nieograniczonej czasowo licencji na szkolenie. Szacunkowa liczba osób do przeszkolenia wynosi 2500 pracowników, licencja zostanie udzielona na nieograniczoną liczbę pracowników.
16.4.11.	Wykonawca na etapie złożenia oferty, przed wyborem najkorzystniejszej oferty, na żądanie Zamawiającego, udostępni dostęp do oferowanej platformy szkoleniowej, na jednym koncie testowym, w celu weryfikacji spełnienia wymagań.
16.4.12.	Zamawiający oczekuje w ciągu trwania całej umowy dostarczenia co najmniej 5 nowych szkoleń i aktualizacje wcześniej zakupionych w przypadku zmian przepisów.
16.4.13.	Test z imiennym certyfikatem ukończenia kursu.

II.17 Wsparcie serwisowe laboratoryjnego systemu informatycznego LIS.

Stan obecny

Zamawiający posiada i użytkuje Laboratoryjny System Informatyczny firmy MARCEL S.A. o nazwie Centrum. System ten posiada "głęboką" integrację ze szpitalnym systemem informatycznym HIS AMMS firmy ASSECO POLSKA S.A.

Lp.	Element Systemu	Liczba użytkowanych elementów
17.1.1. `	Moduł Bazowy (zakład/laboratorium/baza danych)	--1--
17.1.2.	Moduł Mikrobiologia	--1--
17.1.3.	Moduł Serologia	--1--
17.1.4.	Moduł Bank Krwi	--1--
17.1.5.	Moduł Integracja (wymiana z HIS – kontrahenci wewnętrzni)	--1--
17.1.6.	Opcja Finanse (fakturowanie i rejestry faktur)	--1--
17.1.7.		
17.1.8.	Liczba laboratoriów objętych Systemem	--1--
17.1.9.	Liczba stanowisk (stacji roboczych) Systemu	--7--
17.1.10.	Liczba podłączonych analizatorów	--3--

Ogólny opis

Przedmiotem zamówienia jest przedłużenie wsparcia serwisowego tego systemu na okres 36 miesięcy

Zakres usług serwisowych

17.3.1. Zakres usług podstawowych wykonywanych przez Wykonawcę

Lp.	Wymagania minimalne
17.3.1.1.	Prowadzenie cyklicznych szkoleń Administratorów LSI Centrum. Szkolenie może odbyć się stacjonarnie, w siedzibie Zamawiającego lub na życzenie Zamawiającego zdalnie, w wymiarze nieprzekraczającym trzech dni na kwartał.
17.3.1.2.	Generowanie/przedłużenie ważności kodów aktywacyjnych Programu.
17.3.1.3.	Reakcja na zgłaszane przez Zamawiającego awarie i usuwanie możliwych do usunięcia ich skutków, z wyłączeniem awarii spowodowanych działaniem niezgodnym z instrukcjami użytkownika Systemu lub postanowieniami Umowy.
17.3.1.4.	Przyjmowanie i załatwianie reklamacji.
17.3.1.5.	Usuwanie błędów oprogramowania: • uniemożliwiających pracę (krytyczne) - w trybie i na warunkach jak awarie, • pozostałych - w ramach planowych aktualizacji oprogramowania.
17.3.1.6.	Wprowadzanie wynikających ze zmian przepisów prawnych aktualizacji użytkowanej wersji Systemu, wraz z aktualizacją dokumentacji użytkowej.
17.3.1.7.	Rekonfiguracje nie udostępnionych Zamawiającemu, niezbędnych do prawidłowej pracy Systemu ustawień sterujących jego pracą, w tym również podłączonych do Systemu analizatorów, w ramach posiadanych licencji. Zgłoszenie potrzeb w tym zakresie wymaga formy pisemnej (w tym e-mail).
17.3.1.8.	Udzielanie konsultacji w zakresie: • trudności w wykonaniu czynności operatorskich, • diagnostyki problemów związanych z oprogramowaniem Systemu, • implementacji i konfiguracji Systemu u Zamawiającego.
17.3.1.9.	Diagnozowanie uszkodzeń i naprawy okablowania transmisyjnego analizatorów podłączonych do Systemu.
17.3.1.10.	Diagnozowanie uszkodzeń, naprawa i zapewnienie sprawności technicznej urządzeń komputerowych (za wyjątkiem eksploatacyjnego zużycia drukarek) - wyłącznie w przypadku, gdy Umowa Serwisowa obejmuje opiekę nad sprzętem, w zakresie tej opieki.
17.3.1.11.	Analiza potrzeb i przekazywanie Zamawiającemu zaleceń w zakresie modernizacji, ewentualnie wymiany sprzętu komputerowego na nowy. W przypadku zgłoszenia przez Serwis bezpośredniego zagrożenia awarią, brak reakcji Zamawiającego może stanowić podstawę do zawieszenia lub zmiany warunków prowadzenia usług serwisowych.
17.3.1.12.	Okresowe sprawdzanie wydajności serwera.

17.3.2. Zakres usług pozostałych wykonywanych przez Wykonawcę:

Lp.	Wymagania minimalne
17.3.2.1.	Niezbędne reinstalacje serwerów. W przypadku maszyn fizycznych reinstalacje będą wykonywane w siedzibie Zamawiającego lub w miarę możliwości zdalnie. Dostarczenie sprzętu do siedziby Zamawiającego zapewnia Wykonawca.
17.3.2.2.	Analizy, diagnozowanie przyczyn i lokalizacja awarii Systemu, wyjaśnianie zgłoszeń i wsparcie Zamawiającego w zakresie interpretacji funkcjonalności, zmian konfiguracji, organizacji pracy i działania Systemu, w tym odtworzenie historii dostępu do danych.
17.3.2.3.	Analizy oraz diagnozowanie przyczyn nieprawidłowości w komunikacji analizatorów z Systemem.

17.3.2.4.	Konsultacje dotyczące reinstalacji infrastruktury sprzętowej, w tym wymiany/podłączania stacji roboczych, skanerów dokumentów, drukarek wyników, drukarek i skanerów kodów kreskowych oraz drukarek fiskalnych.
17.3.2.5.	Przeprowadzenie (na zgłoszenie Zamawiającego - nie częściej niż raz w roku) audytu, obejmującego kontrolę poprawności gromadzonych danych, weryfikację organizacji pracy z Systemem i ocenę potrzeb Zamawiającego w tym zakresie.
17.3.2.6.	Możliwość konfiguracji wykonywania kopii bezpieczeństwa bazy danych Systemu na zasobie udostępnionym przez Zamawiającego w tym zakresie.
17.3.2.7.	Konfiguracja i przeniesienie danych – prace związane z wymianą serwera.
17.3.2.8.	Konfiguracje stacji roboczych w przypadku konieczności ich wymiany, naprawy lub po reinstalacji systemu operacyjnego.

17.3.3. Warunki prowadzenia prac serwisowych:

Lp.	Wymagania minimalne
17.3.3.1.	O ile Zamawiający nie postanowi inaczej, przygotowanie i instalacja oprogramowania serwerów odbywa się w siedzibie Zamawiającego.
17.3.3.2.	Kontakty Zamawiającego z Wykonawcą dokonywane są wyłącznie za pośrednictwem wyznaczonego przez Zamawiającego Administratora Systemu lub kierownika laboratorium. W wyjątkowych wypadkach (w przypadku zgłoszenia awarii krytycznej), dopuszcza się kontakt innej osoby.
17.3.3.3.	Zamawiający, korzystając z Systemu, zobowiązany jest do przestrzegania zasad zawartych w przekazanych instrukcjach, wskazówkach eksploatacyjnych, zaleceniach i warunkach prowadzenia serwisu, w tym zasad zapewniających unifikację i jednolitą identyfikację danych wykorzystywanych w wymianie informacji z otoczeniem.
17.3.3.4.	Uruchomienie Systemu po awarii, usunięcie możliwych do usunięcia jej skutków, w tym ewentualne odtworzenie bazy danych z ostatniej prawidłowo wykonanej kopii bezpieczeństwa, nastąpi w terminie nie dłuższym niż 24 godziny od chwili przyjęcia zgłoszenia.
17.3.3.5.	Przyjmowanie zgłoszeń przez Wykonawcę: • zgłoszenia awarii oraz zlecenia serwisowe przyjmowane są w dni robocze, w godzinach 08:00 – 15:00 • telefonicznie pod wskazanym w umowie • pocztą elektroniczną wskazany w umowie, • w dni robocze w godzinach od 16.00 do 8.00 dnia następnego oraz w niedziele i święta - wyłącznie konsultacje w przypadku awarii: telefonicznie, pod dyżurnym numerem telefonu wskazanym w umowie Zgłoszenie do Serwisu powinno zawierać: • nazwę jednostki,3 • datę i godzinę zgłoszenia, • opis problemu, • dane kontaktowe osoby koordynującej/uprawnionej do potwierdzenia wykonania czynności.
17.3.3.6.	Z wyjątkiem zgłoszeń awarii, zgłoszenia przesłane drogą elektroniczną są obsługiwane w pierwszej kolejności.

17.3.3.7.	Usługi serwisowe, z wyjątkiem usług związanych z usuwaniem awarii i ich bezpośrednich skutków, wykonywane są w dni robocze w godzinach 08:00 – 16:00 Realizacja prac planowych poza wskazanymi godzinami wymaga oddzielnych ustaleń.
17.3.3.8.	Szkolenia administratorów Systemu odbywają się w formie cyklicznych spotkań w siedzibie Wykonawcy lub w razie konieczności zdalne. Zamawiający ma prawo do uczestnictwa w nieograniczonej liczbie spotkań szkoleniowych. Spotkania są bezpłatne. Wykonawca nie zapewnia zakwaterowania w ramach szkolenia.
17.3.3.9.	W okresie wdrożenia Systemu administratorem danych Systemu jest Wykonawca.
17.3.3.10.	Po okresie wdrożenia Systemu administratorem danych jest Zamawiający, w zakresie wszystkich danych (w tym konfiguracyjnych i sterujących automatycznymi funkcjami Systemu), do których dostęp wynika z posiadanych przez niego uprawnień. Standardowe usługi serwisowe nie obejmują ingerencji Wykonawcy w takie dane.
17.3.3.11.	Wszelkie ingerencje Wykonawcy w dane administrowane przez Zamawiającego, niezależnie od warunków takich ingerencji, wymagają pisemnego (również e-mail) zlecenia uprawnionego przedstawiciela Zamawiającego. Wyjątkiem jest ingerencja związana z usunięciem awarii, dla której podstawą jest zgłoszenie awarii, jednak i w tym przypadku pracownik serwisu realizujący zgłoszenie serwisowe może zażądać pisemnej dyspozycji.
17.3.3.12.	Aktualizacje Systemu wykonywane są automatycznie przez Wykonawcę, z powiadomieniem Zamawiającego. Wyjątkiem są aktualizacje (wynikające z przepisów prawa) znacząco zmieniające funkcjonalność Systemu lub organizację pracy, których termin i tryb przeprowadzenia jest z Zamawiającym uzgadniany.
17.3.3.13.	Zamawiający dopuszcza prawo do przerwy w pracy Systemu (1) raz w roku na niezbędny czas, w terminie uzgodnionym z Zamawiającym, w celu przeprowadzenia prac konserwacyjno-aktualizacyjnych.
17.3.3.14.	Usługi serwisowe realizowane są w sposób zdalny, z wykorzystaniem udostępnionego przez Zamawiającego łącza serwisowego. Połączenie jest realizowane przez szyfrowany tunel pakietu OpenVPN. Serwer VPN znajduje się w siedzibie Zamawiającego, a na serwerze Zamawiającego zainstalowany będzie klient usługi. Zamawiający na potrzeby utrzymania tunelu serwisowego zapewni Wykonawcy łącze internetowe o odpowiedniej przepustowości oraz wspólnie uzgodnione adresy i porty
17.3.3.15.	Usługi serwisowe nie obejmują usuwania skutków awarii Systemu lub jego elementów, ani napraw wynikających z: • instalacji, czy też wymiany części lub akcesoriów komputerowych (w przypadku serwera wirtualnego również zmiany parametrów, zasobów lub priorytetów) bez wcześniejszego uzgodnienia z Wykonawcą, • instalacji, uruchamiania lub eksploatacji oprogramowania innego niż objęte umową (formatowanie, odtwarzanie zawartości dysków, usuwanie skutków działania wirusów, rekonfiguracje zasobów itp.), • ingerencji (przez osoby nieuprawnione) w oprogramowanie lub bazy danych, w tym z braku zabezpieczenia przed dostępem osób nieuprawnionych oraz utratą danych spowodowaną w/w działaniami, • nieprawidłowej pracy Systemu spowodowanej wadami urządzeń, sprzętu komputerowego, niewłaściwą instalacją i działaniem systemów operacyjnych bądź sieciowych, awarii sieci energetycznej lub zaistnienia okoliczności siły wyższej, jak również odtwarzania danych uszkodzonych w wyniku awarii oraz usuwania skutków

	awarii innych niż niezbędne do uruchomienia Systemu, z wyjątkiem odtwarzania z ostatniej nieuszkodzonej kopii bezpieczeństwa.
17.3.3.16.	Zamawiający jest zobowiązany do udzielenia Wykonawcy pomocy w wykonaniu czynności serwisowych w formie udziału oddelegowanych do tego celu pracowników Zamawiającego, w tym administratora Systemu i/lub pracowników odpowiednich służ technicznych.
17.3.3.17.	Interwencje serwisowe w warunkach braku zdalnego dostępu do Systemu, jak również braku możliwości dostępu (do danych lub sprzętu), w przypadku, gdy jest on niezbędny do usunięcia awarii, zwalnia Wykonawcę z dotrzymania terminu jej usunięcia i obliguje Zamawiającego do zwrotu kosztów ewentualnego dojazdu serwisowego.
17.3.3.18.	Wykonawca ma prawo zażądać od Zamawiającego doprowadzenia (w zakresie mu dostępnym) konfiguracji danych do zgodności z zasadami zawartymi w przekazanych instrukcjach wskazówkach eksploatacyjnych, zaleceniach i warunkach prowadzenia serwisu, w szczególności z zasadami zapewniającymi unifikację i jednolitą identyfikację danych. W przypadku braku takiej zgodności, Wykonawca ma prawo odmówić wykonania usługi serwisowej, zmienić termin jej realizacji lub zażądać zwrotu wynikających z tego tytułu dodatkowych kosztów.
17.3.3.19.	Warunkiem wykonania usługi serwisowej jest, w razie konieczności, udostępnienie Serwisowi przez Zamawiającego materiałów informacyjno-instalacyjnych (instrukcje, opisy, nośniki instalacyjne, certyfikaty, kable przyłączeniowe itp.) dotyczących komputera, akcesoriów komputerowych, przyrządu zintegrowanego z komputerem wyposażonego w dodatkowe oprogramowanie lub oprogramowania innego niż autorstwa Wykonawcy
17.3.3.20.	W przypadku zastosowania w Systemie serwera wirtualnego, w celu zdiagnozowania przyczyn awarii, Wykonawca może zażądać od Zamawiającego dodatkowych informacji lub czynności: • dostępności do danych z logów parametrów pracy maszyny, • obecności i współpracy uprawnionego administratora maszyny wirtualnej przy usuwaniu awarii, • obowiązkowego przekazywania informacji o parametrach, przydzielonych serwerowi zasobach i stopniu ich wykorzystania, • obowiązkowego bezzwłocznego informowania o zmianach, wyłączeniach, awariach i nieprawidłowościach w działaniu serwera gospodarza mogących mieć wpływ na pracę serwera wirtualnego Systemu.
17.3.3.21.	Po uzgodnieniu z Zamawiającym, Wykonawca może dokonywać: 17.3.3.21.1. zmian w istniejącym oprogramowaniu, dołączania nowych lub zmiana istniejących funkcjonalności, za wyjątkiem przewidzianych możliwościami konfiguracyjnymi Systemu i zmian wymaganych przepisami, 17.3.3.21.2. napraw uszkodzeń baz danych (z wyjątkiem odtwarzania z kopii), 17.3.3.21.3. instalacji infrastruktury technicznej (sieć, stacje robocze, drukarki, wyposażenie), 17.3.3.21.4. czynności związanych z funkcjonalnościami oferowanymi jako odrębne usługi – realizowanymi w oparciu o osobne ustalenia/umowy (automatyczna publikacja wyników badań przez serwer www, wymiana informacji z innymi systemami, organizacja i zarządzanie strukturami wielkolaboratoryjnymi, itp.), 17.3.3.21.5. diagnostyki infrastruktury sieciowej Zamawiającego, 17.3.3.21.6. diagnostyki i rozwiązywania problemów z łączem internetowym Zamawiającego,

	17.3.3.21.7.	wymiany materiałów eksploatacyjnych sprzętu komputerowego,
	17.3.3.21.8.	wymiany serwera fizycznego na wirtualny,
	17.3.3.21.9.	w przypadku zastosowania serwera wirtualnego, weryfikacji problemów po stronie „gospodarza”,
	17.3.3.21.10.	odtwarzania pełnego zapisu serwera w dowolnym momencie z pełnowartościowej kopii odkładanej na serwerze głównym,
	17.3.3.21.11.	szybkiego odtwarzania pełnego środowiska produkcyjnego z kopii cyklicznie wykonywanych na serwerze zapasowym Zamawiającego,
	17.3.3.21.12.	monitorowania procesów na serwerze z wykorzystaniem oprogramowania NAGIOS lub alternatywnego zatwierdzonego przez Zamawiającego,
	17.3.3.21.13.	uruchomienia i utrzymania szyfrowanego łącza VPN na zasobach Zamawiającego,
	17.3.3.21.14.	aktualizacji oprogramowania związanego z wdrażaniem nowych funkcjonalności,
	17.3.3.21.15.	podłączenia/wymiany analizatorów,
	17.3.3.21.16.	przełączenia analizatora do innej stacji roboczej,
	17.3.3.21.17.	usuwania możliwych do usunięcia skutków nieprawidłowego działania Zamawiającego po wcześniejszym zgłoszeniu tego faktu Zamawiającemu,
	17.3.3.21.18.	modyfikacji dedykowanych formularzy,
	17.3.3.21.19.	przygotowywaniu zestawień z bazy danych,
	17.3.3.21.20.	usuwaniu skutków awarii, które wystąpiły z przyczyn niezależnych od Wykonawcy,
	17.3.3.21.21.	diagnostyki uszkodzonej bazy danych wraz z określeniem możliwości i kosztów odzyskania utraconych danych lub ich odzyskanie,
	17.3.3.21.22.	rekonfiguracji funkcji podpisu elektronicznego przy zmianach dostawcy usługi oraz aktualizacji oprogramowania.

Rozwiązanie równoważne

Zamawiający dopuszcza wymianę obecnie wykorzystywanego Laboratoryjnego Systemu Informatycznego LIS na rozwiązanie równoważne, które zachowa wszystkie funkcjonalności i integracje obecnie wykorzystywanego systemu z okresem wsparcia serwisowego, które jest przedmiotem tego postępowania.

Wymagania minimalne dla Laboratoryjnego Systemu Informatycznego (LIS)

Lp.	Wymagania funkcjonalne
Właściwości systemu	
17.4.1.	Oprogramowanie 100% w języku polskim, graficzny interfejs użytkownika.
17.4.2.	Jednokrotna rejestracja danych – raz zapisane dane nie wymagają powtórnego wpisywania.
17.4.3.	Obsługa dowolnej liczby pracowni: możliwość działania laboratoriów analityki i serologii transfuzjologicznej w na oddzielnych bazach. Możliwość selektywnego widoku na danych stacjach roboczych uwzględniającego widoczność/ukrycie wybranych zleceń.
17.4.4.	Możliwość uruchamiania poszczególnych funkcji systemu (np. rejestracja zleceń) z różnych stanowisk (w ramach posiadanych licencji).
17.4.5.	Możliwość podłączenia i współpracy z drukarką fiskalną.

17.4.6.	Podłączenie i automatyczna rejestracja wyników z oferowanych analizatorów oraz innych aparatów wskazanych przez Zamawiającego, w łącznej liczbie 3 szt.
17.4.7.	Architektura klient/serwer.
17.4.8.	Licencja na minimum: bez limitu użytkowników, minimum: 7 stacji roboczych, minimum: 3 podłączonych analizatorów
17.4.9.	Liczbę licencji na oprogramowanie komunikacyjne podłączonych do systemu analizatorów należy rozumieć jako niezależną od konkretnych typów aparatów. Wymiana analizatora lub zmiana miejsca podłączenia, o ile nie zwiększa łącznej ilości podłączonych aparatów – nie wymaga zmian w dotychczasowych, ani uzyskania nowych licencji.
17.4.10.	Automatyczne (bez udziału użytkownika) tworzenie kopii bezpieczeństwa we wskazanym miejscu, możliwość tworzenia dodatkowych kopii zabezpieczających na żądanie użytkownika.
17.4.11.	Prowadzenie zdalnego serwisu poprzez łącze internetowe. 24. W ramach umowy serwisowej całodobowe (24h, 7 dni w tygodniu) wsparcie techniczne oraz aktualizacja oprogramowania.
17.4.12.	W ramach posiadanych licencji użytkownik ma dostęp do konfiguracji i rekonfiguracji danych sterujących automatyczną pracą systemu.
17.4.13.	**Rejestracja pacjentów i zleceń diagnostycznych:**
17.4.14.	Prowadzenie kartoteki pacjentów i ich rejestracja, łącznie z datą przyjęcia do szpitala oraz identyfikacja pacjenta na podstawie różnych danych: demograficznych, nr księgi głównej, identyfikatora zewnętrznego.
17.4.15.	Rejestracja zleceń (wszystkie badania), od zleceniodawców szpitalnych i zewnętrznych, w tym: • rejestracja godzin: rejestracji zlecenia, pobrania, przyjęcia materiału, • dokumentacja materiału z wykorzystaniem rozbudowywanego przez użytkownika słownika materiałów, możliwość szczegółowego opisania materiału w zleceniu, • możliwość rejestrowania danych z wywiadu (przyjmowane leki, zastosowane i planowane leczenie, sugerowany kierunek diagnozy itp.). • możliwość wpisania danych: objętość dobowej zbiórki moczu, waga pacjenta automatycznie wykorzystywanych w procesie analitycznym do wyliczania wyników zleconych badań.
17.4.16.	Całkowicie automatyczny dobór cen dla wykonywanych badań, umożliwiający: • dobór różnych cen za badanie dla różnych płatników, • przypisanie badań różnym płatnikom, bez rejestracji osobnych zleceń, • rejestrację grupy (pakietu) badań o cenie różnej od sumy cen składowych, • zlecenie badania (po ustalonej cenie) wykonywanego na koszt laboratorium, • przydział ceny z cennika „domyślnego” w przypadku niekompletnych danych kwalifikujących przydział właściwego cennika (lub braku w nim ceny), • blokadę rejestracji badania, do którego nie można automatycznie dobrać ceny.
17.4.17.	Automatyczne rozliczanie zleceń, z uwzględnieniem specjalnych ich rodzajów (Cito, Dyżury, itp.), w tym: 8.4.17.1. możliwość definiowania własnych rodzajów zleceń, 8.4.17.2. możliwość automatycznego doboru różnych cen tego samego badania dla różnych płatników i w zależności od rodzaju zlecenia (włącznie z rodzajami zleceń zdefiniowanymi przez użytkownika), 8.4.17.3. możliwość użycia zdefiniowanego rodzaju zlecenia jako filtru w zestawieniach.

17.4.18.	Automatyczne uwzględnianie w rozliczaniu zleceń kilku różnych stawek VAT dla tej samej usługi, w zależności od przeznaczenia wyniku.
17.4.19.	Możliwość podłączenia i współpracy z drukarkami fiskalnymi, prowadzenie towarzyszących im rejestrów sprzedaży i rejestrów paragonów fiskalnych, z możliwością równoczesnego użycia kilku takich drukarek i rejestrów.
17.4.20.	Możliwość dopisania badania do istniejącego zlecenia, bez konieczności ponownego rejestrowania danych administracyjnych.
17.4.21.	Prowadzenie głównej książki zleceń i możliwość jej wydruku.
17.4.22.	Możliwość automatycznego (na podstawie zarejestrowanych zleceń) wystawiania rachunków indywidualnych dla pacjentów oraz rachunków/faktur zbiorczych dla płatników.
17.4.23.	**Proces analityczny:**
17.4.24.	Prowadzenie książek zleceń i wyników w pracowniach, automatycznie sprzężonych z książką główną.
17.4.25.	Definiowanie w dowolnym czasie i automatyczne prowadzenie ksiąg (ewidencji/list) wg wymagań Zamawiającego, z możliwością: • grupowania i numeracji wg zadanego porządku, • użycia przy wydruku wyników: numeracji z księgi i specjalnych (przypisanych do księgi) formularzy, • filtrowania wyników odpowiednio do przynależności do księgi.
17.4.26.	Automatyczne kierowanie badań do stanowisk, na których mają być wykonane, z uwzględnieniem alternatywnych metod wykonywania, w tym możliwość przekierowywania badań do innej pracowni.
17.4.27.	Pełna automatyka sterowania analizatorami diagnostycznymi (programowanie, wysyłanie zleceń, odbiór wyników, przesłanie informacji technicznych), uwzględniająca specyfikę aparatów serologicznych
17.4.28.	Możliwość wyboru liczby i rodzaju badań do wykonania, zmiany kolejności, przerwania, powtórzenia, wpisania wyniku manualnie, zatwierdzenia – w miarę możliwości obsługiwanego stanowiska (analizatora).
17.4.29.	Możliwość alternatywnego wykonywania tych samych badań na kilku (różnych lub takich samych) analizatorach – oprogramowanie musi umożliwiać automatyczny (bez wskazywania przez użytkownika) przydział próbek do analizatorów/pracowni z uwzględnieniem: • możliwości zadania przez użytkownika reguł przydziału, • możliwości wystąpienia nieokreślonej (jedna lub kilka) liczby próbek tego samego materiału, • automatycznego programowania i odbioru wyników z któregokolwiek takiego analizatora, bez wskazywania, na którym zostaną lub zostały wykonane, • optymalizacji wykorzystania analizatorów – wykonywanie badań wg zadanych kryteriów optymalizacji (czas pracy, repertuar aparatu, obciążenie).
17.4.30.	Możliwość manualnego wprowadzania wyników z wykorzystaniem otwartej dla użytkownika kartoteki skrótów tekstowych.
17.4.31.	Przyspieszona, automatyczna obsługa zleceń pilnych.
17.4.32.	Automatyczny dobór wartości referencyjnych i automatyczne flagowanie wyników, w tym flagowanie wyników będących tekstowymi opisami, z możliwością dowolnej liczby zakresów referencyjnych, osobno dla każdej metody wykonania badania.
17.4.33.	Możliwość automatycznego zastępowania wyniku liczbowego (poza wskazanym zakresem) odpowiednim tekstem.

17.4.34.	Rejestracja błędów wykonania oraz błędów preanalitycznych.
17.4.35.	Określanie, analiza i sygnalizacja przekroczenia krytycznych wartości wyników badań.
17.4.36.	Dwustopniowe zatwierdzanie: 1) „techniczna" akceptacja wyniku i 2) autoryzacja diagnosty, w tym walidacja wyniku, wspólny widok wyników ze wszystkich pracowni, walidowanych poprzednich wyników pacjenta, funkcje „delta check". Możliwość wyboru trybu pracy: z zatwierdzaniem jedno- lub dwustopniowym. Autoryzacja wyniku wspomagana podglądem wydruku w jego ostatecznej postaci.
17.4.37.	Możliwość zdalnej, autoryzacji wyników przez diagnostę, z zapewnieniem mu wglądu do danych niezbędnych do podjęcia decyzji - co najmniej do wyników badań, materiałów, pacjentów i wyników kontroli jakości realizowane przez szyfrowane połączenie tunelem VPN.
17.4.38.	Automatyczne (w tle) naliczanie kosztów, z uwzględnieniem metod i powtórzeń.
17.4.39.	Wygodne katalogowanie miejsca przechowywania próbek po wykonaniu oznaczeń, możliwość późniejszego odszukania próbki wg danych zapisanych w systemie.
Wydawanie wyników:	
17.4.40.	Możliwość prawnie skutecznego elektronicznego wraz ze znacznikiem czasu podpisywania wyników, w tym składania podpisu zdalnie, za pośrednictwem publicznej sieci Internet.
17.4.41.	Określanie porządku (kolejności) ustawienia badań/parametrów, niezależnie dla: wyświetlania na ekranie, drukowania na wynikach, w tabelach cen.
17.4.42.	Automatyczna kwalifikacja wyniku do wydruku/podpisu elektronicznego/przesyłki w formie komunikatu HL7.
17.4.43.	Drukowanie wyników dla pacjentów w tym możliwość rezerwacji użycia wybranych formularzy dla wskazanych zleceniodawców.
17.4.44.	Ewidencja wydawania wyników (papierowych) z zaznaczeniem czasu (daty i godziny) wydania i informacją o osobie wydającej i odbierającej wynik.
17.4.45.	Automatyczna (na podstawie zadanych kryteriów) kwalifikacja wyniku do: wydruku / podpisu elektronicznego.
17.4.46.	Archiwizacja pełnych wyników diagnostycznych wraz z opisami i uwagami.
Automatyczna identyfikacja materiału:	
17.4.47.	System znakowania kodami paskowymi nie wymagający drukarek tych kodów.
17.4.48.	Możliwość znakowania materiału w miejscu pobrania, nie w laboratorium.
17.4.49.	Jednoznaczna identyfikacja pacjenta, zlecenia i każdej próbki materiału w oparciu o kod paskowy, również rozróżnianie materiałów w ramach jednego zlecenia.
17.4.50.	Nieograniczone czasowo wykrycie i możliwość blokady użycia w systemie dwóch probówek z identycznym kodem kreskowym.
17.4.51.	Wykorzystanie kodów kreskowych we współpracy z analizatorami.
17.4.52.	Funkcja „przyjęcia materiału", umożliwiająca rejestrację materiału z równoczesną weryfikacją zlecenia (wykrycie zleceń, do których brak materiału, oraz materiału, do którego brak zlecenia), uwzględnienie tego faktu w procesie analitycznym.
Kontrola jakości i wiarygodności wyników:	
17.4.53.	Kartoteka materiałów kontrolnych i procedur.
17.4.54.	Automatyczne przygotowywanie Kart Kontroli.
17.4.55.	Rejestracja i ewidencja wyników prób kontrolnych.
17.4.56.	Analizy: odtwarzalności, powtarzalności, precyzji.
17.4.57.	Wykresy LJ.
17.4.58.	Analiza Westgarda (w seriach i pomiędzy, reguły proste i złożone, indywidualny dobór reguł).

17.4.59.	Możliwość wyłączenia wyniku z analizy kontrolnej oraz oznaczenia wyniku kontrolnego komentarzem/opisem.
17.4.60.	Statystyczna analiza wyników liczbowych (wszystkie wyniki, każdy parametr): średnia, SD, zmiany w czasie, zawężanie kryteriów (okres od-do, grupy wiekowe).
Zestawienia statystyczne i raporty:	
17.4.61.	Statystyka i zestawienia w dwustopniowych podziałach na: płatników, zleceniodawców, punkty pobrań, oddziały, lekarzy, analizatory, pracownie.
17.4.62.	Dodatkowe filtry uwzględniające wybór/wykluczenie wybranych elementów.
17.4.63.	Zestawienia ilościowe/kosztowe/wartościowe, imienne.
17.4.64.	Zestawienia uwzględniające/wyszczególniające używane typy zleceń.
17.4.65.	Grupowanie danych (w ramach wybranego podziału) i sumowanie w grupach.
17.4.66.	Dostępny za pomocą popularnych przeglądarek moduł umożliwiający tworzenie zestawień statystycznych, w tym: • ilości badań (zleconych, zatwierdzonych, przed przyjęciem, po przyjęciu materiału) w podziale na co najmniej zleceniodawców, płatników, pracownie, materiał • ilości wyników (z uwzględnieniem metody i parametru badania) w normie, poniżej i powyżej normy, z możliwością wyboru zakresu liczbowego wyniku, • średniego czasu wykonania badań (od pobrania do zatwierdzenia, od przyjęcia do zatwierdzenia, od pobrania do przyjęcia materiału) z podziałami na zleceniodawców, materiał, wybrane badanie. Tworzenie szablonów zestawień z późniejszą możliwością ich edycji. Eksport przygotowanych zestawień do plików w formacje pdf, xls, csv.
Użytkownicy, bezpieczeństwo danych:	
17.4.67.	System uprawnień przyznawanych użytkownikom, umożliwiający ochronę danych konfiguracyjnych, osobowych, medycznych i finansowych.
17.4.68.	Automatyczne dokumentowanie wszystkich zapisów i zmian w danych, w tym wpisów i poprawek dotyczących danych pacjentów, zleceń, wyników, finansów i parametrów konfigurujących, zawierające co najmniej zapis kto, kiedy i jakiej dokonał zmiany bądź wpisu.
17.4.69.	Zabezpieczenie dostępu do danych zgodnie z obowiązującymi przepisami (w tym ustawy o ochronie danych osobowych). Logowanie użytkowników na poziomie aplikacji przy pomocy kluczy i certyfikatów RSA – alternatywnie do haseł.
17.4.70.	Rejestracja, śledzenie i odtwarzanie czynności ważnych dla procesu analitycznego (godzina pobrania, rejestracji zlecenia, planowana godzina wykonania badania, przyjęcia materiału, wykonania, zatwierdzenia, wydruku/wydania), z podaniem kto i kiedy wykonał, z uwidocznieniem tej informacji na wydruku wyniku.
17.4.71.	Możliwość manualnej korekty skutków działania procedur automatycznych, z sygnalizacją wystąpienia takiej sytuacji.
17.4.72.	Możliwość uruchamiania poszczególnych funkcji systemu (np. rejestracja zleceń) z różnych stanowisk (w ramach posiadanych licencji).
17.4.73.	W ramach posiadanych licencji użytkownik ma dostęp do konfiguracji i rekonfiguracji danych sterujących automatyczną pracą systemu.
Komunikacja zewnętrzna	
17.4.74.	Możliwość współpracy z innymi laboratoriami w zakresie automatycznego tworzenia wysyłkowych list zleceń i zwrotnego odbioru wyników wraz z rozliczeniem tych badań.
17.4.75.	Możliwość automatycznej współpracy w zakresie przyjmowania zleceń i odsyłania wyników, wg standardu HL7, z systemem HIS, innymi LSI.

17.4.76.	Możliwość pracy w systemie rozproszonym w kilku lokalizacjach (laboratoriach), udokumentowana minimum jednym wdrożeniem takiego systemu, obejmującego laboratorium centralne i co najmniej 2 laboratoria satelitarne, działające autonomicznie (i niezależnie od połączeń telekomunikacyjnych) i automatycznie zarządzane poprzez konfigurację jednej bazy centralnej.
17.4.77.	Możliwość automatycznej ekspedycji elektronicznie podpisanych (prawnie skutecznie) wyników do wybranych zleceniodawców w formie elektronicznej
17.4.78.	Możliwość automatycznej publikacji zatwierdzonych wyników w sieci wewnętrznej (Intranet), dostępnych dla odbiorców za pomocą popularnych przeglądarek web, z uwzględnieniem systemu uprawnień ograniczającego taki dostęp do podmiotów uprawnionych.
17.4.79.	Niezależne, autonomiczne oprogramowanie umożliwiające zlecanie badań z zewnętrznych punktów pobrań przez sieć wewnętrzną (Intranet) za pomocą popularnych przeglądarek web, z automatyczną rejestracją takich zleceń w systemie.
17.4.80.	Generowanie dokumentów wynikowych zgodnych z PIK HL7 CDA
17.4.81.	Dostawa repozytorium EDM dla badań komercyjnych
Lp.	**Moduły Pracownia Serologii Transfuzjologicznej i Szpitalny Bank Krwi**
17.4.82.	Oprogramowanie 100% w języku polskim, jednokrotna rejestracja danych (raz zapisane dane nie wymagają powtórnego wpisywania).
17.4.83.	Oferent zapewni: 17.4.83.1. oprogramowanie (licencja na 7 szt. stacji roboczych, licencja na 3 szt. analizatorów), 17.4.83.2. instalacje systemu LIS, 17.4.83.3. szkolenie z obsługi dostarczonego oprogramowania LIS (5 dni roboczych)
17.4.84.	Prowadzenie: 17.4.84.1. kartoteki składników wraz z ich historią (ruchy magazynowe, wyniki wykonanych badań i przetoczenie/utylizacja); 17.4.84.2. kartoteki pacjentów z ich historią serologiczną (co najmniej w zakresie przetoczeń, powikłań i wyników wykonanych badań) z automatyczną sygnalizacją dawniejszych problemów serologicznych (co najmniej informacja o wcześniejszych powikłaniach, przeciwciałach, konsultacjach i fenotypie), automatycznie prezentowaną wykonawcy badania pacjenta z wcześniejszymi problemami, z możliwością ich współdzielenia z innymi jednostkami (udostępniania/przyjmowania danych).
17.4.85.	Prowadzenie (wprowadzanie, modyfikacja/aktualizacja, przechowywanie, prezentacja, wydruk) dokumentacji elektronicznej (rejestry i księgi) w pełnym zakresie danych przewidzianym prawem dla pracowni serologii transfuzjologicznej, banku krwi i pracowni konsultacyjnej, w tym prowadzenie rejestrów dokumentów wraz z ich treścią, w odniesieniu do donacyjnych i niedonacyjnych składników krwi, w tym: 17.4.85.1. księga grup krwi, 17.4.85.2. księga prób zgodności, 17.4.85.3. zamówienia zbiorcze do dostawców, 17.4.85.4. zamówienia indywidualne do dostawców, 17.4.85.5. zamówienia otrzymane indywidualne i zbiorcze, 17.4.85.6. zlecenia wykonania badań, 17.4.85.7. wyniki badań (grup krwi, przeciwciał, prób krzyżowych i kwalifikacji kobiet do podania immunoglobuliny, inne określone obowiązującymi przepisami), 17.4.85.8. wyniki konsultacji,

	17.4.85.9. dokumenty przychodu i rozchodu, 17.4.85.10. protokoły transportu, 17.4.85.11. wydania (w tym do pilnej transfuzji i dla noworodków), 17.4.85.12. zwroty, 17.4.85.13. reklamacje, 17.4.85.14. likwidacje 17.4.85.15. oraz elektronicznie podpisanymi oryginałami: 17.4.85.16. wyniki badań (grup krwi, przeciwciał, prób krzyżowych i kwalifikacji kobiet do podania immunoglobuliny, inne określone obowiązującymi przepisami), 17.4.85.17. wyniki konsultacji
17.4.86.	Możliwość automatycznej współpracy (wymiana danych) z analizatorami m.in. automatyczne przyjmowanie i archiwizowanie w bazie danych: 17.4.86.1. odczytanych przez analizator stopni aglutynacji, 17.4.86.2. obrazów zeskanowanych przez analizator kaset, 17.4.86.3. informacji o osobach dokonujących manualnych modyfikacji i akceptacji,
17.4.87.	Obsługa niedonacyjnych składników krwi (np. czynniki krzepnięcia)
17.4.88.	Możliwość wydruku wyniku próby zgodności i karty wydania krwi dla noworodka dla pojedynczych donacji.
17.4.89.	Manualne wprowadzanie wyników serologicznych, zapewniające: 17.4.89.1. wprowadzenie pełnego protokołu wraz ze stopniami aglutynacji, 17.4.89.2. automatyczną weryfikację zgodności protokołu z wydawanym wynikiem i znaną z historii pacjenta jego dotychczasową grupą krwi i Rh, 17.4.89.3. opisywanie wyników, również uzyskanych automatycznie 17.4.89.4. automatyczne potwierdzenie grupy krwi
17.4.90.	Automatyczna identyfikacja materiału: kodem kreskowym materiału pobranego od pacjenta oraz składników i ich parametrów zgodnie ze specyfikacją ISBT128.
17.4.91.	Wprowadzanie wszystkich danych z etykiety składnika za pomocą czytnika (skanera) kodów kreskowych.
17.4.92.	Możliwość archiwizacji dokumentów (np. zewnętrzne wyniki grup krwi, wyniki badań konsultacyjnych, zgody pacjenta) poprzez wskanowywanie do kartoteki pacjenta
17.4.93.	W stosunku do wybranych parametrów rejestracji musi być określenie ich bezwzględnej wymagalności, automatycznie egzekwowanej podczas wprowadzania danych.
17.4.94.	Automatyczne ostrzeżenia podczas rejestracji zamówienia składników krwi niezgodnych z historią serologiczną pacjenta oraz automatyczna blokada wydania składnika niezgodnego, z możliwością pominięcia blokady w przypadkach przewidzianych przez prawo.
17.4.95.	Automatyczne ostrzeżenia podczas wydawania składnika dla pacjenta z niepotwierdzoną grupą krwi
17.4.96.	Automatyczne naliczanie cen składników krwi przy rejestrowaniu dokumentów przychodu, na podstawie konfigurowalnych cenników, uwzględniające rodzaje, odmiany i zastosowane dodatkowe procesy technologiczne.
17.4.97.	Obsługa Pracowni Serologicznej i Banku Krwi na wspólnej bazie, ze wspólną kartoteką pacjentów, składników krwi oraz wyników.
17.4.98.	Dostawa gotowych etykiet z kodami kreskowymi (w kolorze różowym) w ilości odpowiadającej liczbie wykonywanych badań.
17.4.99.	Możliwość tworzenia raportów i zestawień: z wykonanych usług, gospodarki magazynowej krwi z uwzględnieniem cenników i kodów NFZ
17.4.100.	Autoryzacja sprawozdań z badań kwalifikowanym podpisem elektronicznym.

17.4.101.	Automatyczna, zgodna z protokołem HL7 wymiana z innymi jednostkami (HIS) danych i dokumentów (łącznie z podpisanymi elektronicznie), w zakresie zamówień indywidualnych, zleceń na wykonanie badań, wyników badań, informacji o wydanych składnikach
17.4.102.	Dostawa repozytorium EDM dla badań komercyjnych
17.4.103.	Automatyczne (bez udziału użytkownika) tworzenie kopii bezpieczeństwa we wskazanym miejscu, możliwość tworzenia dodatkowych kopii zabezpieczających na żądanie użytkownika.
17.4.104.	Prowadzenie zdalnego serwisu poprzez szyfrowane łącze internetowe.
17.4.105.	W ramach umowy serwisowej całodobowe (24h, 7 dni w tygodniu) wsparcie techniczne oraz aktualizacja oprogramowania.
Lp.	**Moduł Mikrobiologia**
17.4.106.	Elastyczny system rejestracji zleceń mikrobiologicznych, uwzględniający: 17.4.106.1. automatyczny rozdział rejestrowanego zlecenia wg materiałów diagnostycznych 17.4.106.2. nadawanie zleceniom zawierającym badania mikrobiologiczne indywidualnej numeracji rocznej/kwartalnej/miesięcznej 17.4.106.3. automatyczna rejestracja podłoży hodowlanych oraz wstępnych procedur/działań wraz ze zleconym badaniem.
17.4.107.	Rejestrowanie przeprowadzanych w procesie diagnostycznym zużytych położy, dodatkowych działań, identyfikacji i wykonanych antybiogramów z możliwością ich rozliczania w zestawieniach kosztowych
17.4.108.	Różnicowanie naliczania cen/kosztów badań mikrobiologicznych w zależności od liczby wyhodowanych organizmów i wykonanych antybiogramów.
17.4.109.	Wykorzystanie rejestrowanych danych do prowadzonych książek pracy oraz raportów rozliczeniowych
17.4.110.	Karty Pracy - wydruki kart pracy dla pojedynczych zleceń lub wydruk książki pracy w opcjach 2, 3, 4 i więcej zleceń na stronie.
17.4.111.	Zintegrowany, specjalistyczny ekran do opracowywania wyników dodatnich z widokiem czasu hospitalizacji, możliwością podglądu historii wyników pacjenta, podziałem na okna do: • rejestracji podłoży, • rejestracji i opisów wykonywanych działań, • rejestracji i opisu wykrytych patogenów, mechanizmów oporności • rejestracji i wprowadzania wyników lekowrażliwości
17.4.112.	Elektroniczna książka pracy – rejestracja zużywanych podłoży oraz zapisywanie poszczególnych etapów pracy (działań/procedur) wraz z możliwością wprowadzania obserwacji.
17.4.113.	Identyfikacja podłoży - automatycznie generowanie i wydruk etykiet identyfikacyjnych dla podłoży hodowlanych. Identyfikator w postaci kodu kreskowego oraz drukowanych danych pacjenta/zlecenia pozwalający na szybkie, niezawodne (także bez użycia czytnika kodów kreskowych) rozpoznawanie hodowli oraz natychmiastowe odszukanie danego izolatu w LIS.
17.4.114.	Stale aktualizowana kartoteka drobnoustrojów.
17.4.115.	Otwarta dla Użytkownika kartoteka mechanizmów oporności i stałych opisów dla drobnoustrojów.
17.4.116.	Otwarta dla Użytkownika tabela przydziału atrybutów dla drobnoustrojów (mechanizmów oporności i stałych opisów).
17.4.117.	Otwarta dla Użytkownika kartoteka skrótów wyników tekstowych.
17.4.118.	Możliwość konfiguracji antybiogramów dedykowanych dla grup organizmów. W antybiogramach:

	• dedykowana stała lista antybiotyków oraz możliwość do rejestrowania dowolnego antybiotyku, • możliwość wprowadzania stref zahamowania wzrostu w celu automatycznego wyliczenia wyniku lekowrażliwości, • możliwość wprowadzania wartości Break Point .
17.4.119.	Możliwość prezentowania na wydrukach wyników lekowrażliwości, w postaci ostatecznego wyniku oporności (W,O,WZE lub R<S,I) , wartości MIC, opcjonalnie także wartości Break Point oraz BMQ (indeks skuteczności antybiotyku).
17.4.120.	Konfiguracja badań czystościowych umożliwiająca zarejestrowanie dowolnej ilości prób z podaniem lokalizacji i miejsca pobrania każdej z próbek. Dostosowany do badań czystościowych formularz wydruku wyników.
17.4.121.	Raporty mikrobiologiczne obejmujące: • zestawienia ilościowe przebadanych pacjentów/przypadków/identyfikacji/ dostarczonych materiałów/wyhodowanych organizmów w dwóch poziomach podziałowych z możliwością rozbudowanego filtrowania (zleceniodawcy/płatnicy/ organizmy/antybiotyki); • zestawienia lekowrażliwości (także rozkłady wartości MIC) wyhodowanych szczepów w dwóch poziomach podziałowych z możliwością rozbudowanego filtrowania; (zleceniodawcy/płatnicy/organizmy/antybiotyki) • zestawienia skuteczności antybiotyków z możliwością rozbudowanego filtrowania; (zleceniodawcy/płatnicy/organizmy/antybiotyki); • zestawienia prezentujące profile lekooporności wyhodowanych szczepów; • mapa mikrobiologiczna o otwartej dla Użytkownika konfiguracji kolumn; • zestawienia wyhodowanych szczepów z uwzględnieniem wykrytych mechanizmów oporności oraz lekowrażliwości; • wykonywane raporty uwzględniają podział na materiały pobrane >/< 72 godzin od czasu rozpoczęcia hospitalizacji; • tworząc raport Użytkownik może wybrać treść zestawienia: liczba pacjentów / liczba przypadków (pacjent badany w czasie 60 dni) / liczba identyfikacji; • wszystkie rodzaje raportów mają możliwość wygenerowania wykresów kołowych lub słupkowych, eksportu do pliku PDF, arkuszy kalkulacyjnych oraz plików csv; • możliwość konfiguracji podręcznych szablonów dla okresowo wykonywanych raportów; • możliwość uwzględniania w raportach wyników badań molekularnych i antygenowych.
17.4.122.	Konfiguracja badań czystościowych umożliwiająca zarejestrowanie dowolnej ilości prób z podaniem lokalizacji i miejsca pobrania każdej z próbek. Dostosowany do badań czystościowych formularz wydruku wyników.
17.4.123.	Moduł generowania i ewidencji druków zgłoszeń do sanepidu (ZLB1,ZLB2,ZLB3) oraz zgłoszeń wyizolowanych szczepów do KORLD i KOROUN. Możliwość generowania zgłoszeń dla wyników badań molekularnych i antygenowych.

II.18 Rozbudowa systemu backupowego

Stan obecny

Zamawiający obecnie wykorzystuje oprogramowanie firmy służące do wykonywania backupu, replikacji oraz zarządzania danymi w środowiskach wirtualnych i chmurowych firmy Veeam pod nazwą Veeam Backup & Replication Enterprise Plus na 2 CPU.

Ogólny opis

Przedmiotem zamówienia jest przedłużenie wsparcia do posiadanego systemu Veeam Backup & Replication Enterprise Plus na 2 CPU o 24 miesiące oraz rozszerzenie tej licencji o dodatkowe 2 CPU ze wsparciem 36 miesięcy. Równoważnie Zamawiający akceptuje zaoferowanie oprogramowania backup na 4 CPU ze wsparciem na 36 miesięcy spełniającego specyfikację z punktu II.18.3.

Wymagania dla oprogramowania

Lp.	Wymagania minimalne
18.3.1.	Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 7.x i 8.0 oraz Microsoft Hyper-V 2012, 2012R2, 2016, 2019 i 2022. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej.
18.3.2.	Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux.
18.3.3.	Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej.
18.3.4.	Oprogramowanie musi tworzyć “samowystarczalne” archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków.
18.3.5.	Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji.
18.3.6.	Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu.
18.3.7.	Oprogramowanie musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć jedną wirtualną pulę pamięci na kopie zapasowe. Wymagane jest wsparcie dla nieograniczonej liczby pamięci masowych to takiej puli.
18.3.8.	Oprogramowanie musi pozwalać na tworzenie repozytorium kopii zapasowych bezpośrednio na zasobach Microsoft Azure Blob, Google Cloud Storage, Amazon S3, Wasabi Cloud Storage oraz na innych kompatybilnych z S3 przestrzeniach obiektowych. Dodatkowo, oprogramowanie musi wspierać archiwizowanie tych danych do Microsoft Azure Archive Blob Storage oraz Amazon S3 Glacier.
18.3.9.	Oprogramowanie musi wspierać niezmienność kopii zapasowych na potrzeby ochrony przed ransomware poprzez niedopuszczenie do usunięcia lub modyfikacji kopii zapasowej w zadanym okresie czasu.
18.3.10.	Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania.

18.3.11.	Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL, Oracle oraz PostgreSQL (w tym odtwarzanie point-in-time).
18.3.12.	Oprogramowanie musi zapewniać możliwość delegacji uprawnień do odtwarzania na portalu.
18.3.13.	Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API.
18.3.14.	Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji.
18.3.15.	Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji.
18.3.16.	Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania.
18.3.17.	Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.
18.3.18.	Oprogramowanie musi posiadać natywne mechanizmy uwierzytelniania wieloskładnikowego (MFA) w celu dostępu do konsoli administracyjnej.
18.3.19.	Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej.
18.3.20.	Oprogramowanie musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych.
18.3.21.	Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta musi być dostępna na wszystkich wspieranych platformach wirtualizacyjnych z dokładnością do pojedynczego datastoru.
18.3.22.	Oprogramowanie musi zapewniać tworzenie kopii zapasowych z bezpośrednim wykorzystaniem snapshotów macierzowych. Musi też zapewniać odtwarzanie maszyn wirtualnych z takich snapshotów. Proces wykonania kopii zapasowej nie może wymagać użycia jakichkolwiek hostów tymczasowych. Opisana funkcjonalność powinna działać w środowisku VMware.
18.3.23.	Oprogramowanie musi posiadać wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją VMware.
18.3.24.	Oprogramowanie musi wspierać kopiowanie backupów oraz zasobów plikowych na taśmy.
18.3.25.	Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son).
18.3.26.	Oprogramowanie musi wspierać bezpośrednią integrację z urządzeniami deduplikacyjnymi. Minimalnie wsparcie wymagane dla Dell DataDomain, HPE StoreOnce, ExaGrid, Fujitsu CS800, Quantum DXi oraz Infinidat InfiniGuard.
18.3.27.	Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016, 2019 lub 2022 z systemem pliku ReFS jako repozytorium backupu. Podobna funkcjonalność musi być zapewniona dla repozytoriów opartych o linuxowy system plików XFS.
18.3.28.	Oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN.
18.3.29.	Oprogramowanie musi mieć możliwość replikacji asynchronicznej włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere pomiędzy hostami ESXi oraz pomiędzy hostami Hyper-V. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji.
18.3.30.	Oprogramowanie musi mieć możliwość replikacji ciągłej, opartej o VMware VAIO, włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere. Dla replikacji ciągłej musi być możliwość zdefiniowania dziennika pozwalającego na odzyskanie danych z dowolnego punku w ramach ustalonego parametru RPO.
18.3.31.	Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik.

18.3.32.	Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding).
18.3.33.	Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN).
18.3.34.	Oprogramowanie musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware, Hyper-V oraz Nutanix AHV niezależnie od rodzaju storage'u użytego do przechowywania kopii zapasowych.
18.3.35.	Dodatkowo dla środowiska vSphere, Hyper-V i Nutanix AHV powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna).
18.3.36.	Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w hypervisor. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie musi realizować taką migrację swoimi mechanizmami.
18.3.37.	Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSpehre.
18.3.38.	Oprogramowanie musi pozwalać na uruchomienie zasobów plikowych SMB oraz baz danych MS SQL i Oracle bezpośrednio ze skompresowanego i skompresowanego pliku backupu. Dodatkowo wspierana musi być migracja on-line tak uruchomionych zasobów na środowisko produkcyjne.
18.3.39.	Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków.
18.3.40.	Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform.
18.3.41.	Oprogramowanie musi umożliwić odtworzenie plików/folderów lub ich uprawnień na maszynę operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików
18.3.42.	Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy natywnego API dla platformy VMware i PowerShell Direct dla platformy Hyper-V.
18.3.43.	Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, BSD, Solaris, Mac, Novell
18.3.44.	Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM oraz Windows Storage Spaces.
18.3.45.	Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej.
18.3.46.	Oprogramowanie musi wspierać granularne odtwarzanie obiektów Active Directory takich jak konta komputerów, konta użytkowników, dowolnych atrybutów, rekordów DNS zintegrowanych z AD, Microsoft System Objects, certyfikatów CA, elementów AD Sites oraz pozwalać na odtworzenie haseł.
18.3.47.	Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2013SP1 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects"). Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego.
18.3.48.	Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2008 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku point-in-time, całych baz lub pojedynczych tabeli, widoków oraz procedur.
18.3.49.	Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2013 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku całych witryn, bibliotek oraz pojedynczych dokumentów wraz z historią ich wersji.

18.3.50.	Oprogramowanie musi wspierać granularne odtwarzanie baz danych Oracle z opcją odtwarzanie point-in-time wraz z włączonym Oracle DataGuard. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Windows oraz Linux.
18.3.51.	Oprogramowanie musi wspierać granularne odtwarzanie baz danych PostgreSQL z opcją odtwarzanie point-in-time. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Linux.
18.3.52.	Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez Oracle RMAN
18.3.53.	Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez SAP HANA, SAP Oracle
18.3.54.	Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez MS SQL VDI
18.3.55.	Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN
18.3.56.	Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu. Powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna)
18.3.57.	Dla VMware'a oprogramowanie musi pozwalać na uruchomienie takiego środowiska dla replik maszyn wirtualnych oraz bezpośrednio ze snapshotów macierzowych stworzonych na wspieranych urządzeniach.
18.3.58.	Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem
18.3.59.	Oprogramowanie musi umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem jakichkolwiek danych. Integracja musi być zapewniona minimalnie dla Windows Defender, Symantec Protection Engine oraz ESET NOD32.
18.3.60.	Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego.
18.3.61.	Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 7.x i 8.0 oraz Microsoft Hyper-V 2012, 2012R2, 2016, 2019 i 2022. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej.

II.19 Audyt końcowy

Zakres audytu:

19.1. Przeprowadzenie audytu końcowego zgodnie z wymaganiami konkursu „Inwestycja D1.1.2 Przeprowadzenie audytu końcowego zgodnie z wymaganiami konkursu „Inwestycja D1.1.2 Przyspieszenie procesów transformacji cyfrowej ochrony zdrowia poprzez dalszy rozwój usług cyfrowych w ochronie zdrowia" - https://www.gov.pl/web/zdrowie/inwestycja-d112-przyspieszenie-procesow-transformacji-cyfrowej-ochrony-zdrowia-poprzez-dalszy-rozwoj-uslug-cyfrowych-w-ochronie-zdrowia-nabor-konkurencyjny

19.2. Przeprowadzenie Audytu końcowego w obszarze cyberbezpieczeństwa wskazującego na co najmniej dokonanie pozytywnej lub warunkowo pozytywnej oceny podmiotu w oparciu o kryteria wskazane w Ankiecie weryfikacji dojrzałości w zakresie cyberbezpieczeństwa jako

obligatoryjne, jak również nieobligatoryjne „11.04 Zał. 3 do Wniosku - Ankieta weryfikacji dojrzałości w zakresie cyberbezpieczeństwa.docx”
https://www.gov.pl/attachment/107a9c04-1e7c-4d00-bbf0-5f60255d22da

19.3. Przeprowadzenie audytu bezpieczeństwa informacji, obejmującego zarówno analizę dokumentacji, jak i praktyczną weryfikację stosowanych zabezpieczeń u Zamawiającego.

19.4. Audyt potwierdzający osiągnięcie wskaźnika D21.R2 Zabezpieczenie przetwarzania elektronicznej dokumentacji medycznej potwierdzone audytem bezpieczeństwa

19.5. Raport audytorski, zawierający:

- wnioski generalne
- wskazanie i omówienie niezgodności z wymaganiami
- rekomendacje i zakres niezbędnych zmian organizacyjno-technicznych
- analiza dot. osiągnięcie wskaźnika D21.R2

19.6. Audyt końcowy winien uwzględniać wymagania Ustawy z dnia 5 lipca 2028r o Krajowym Systemie Cyberbezpieczeństwa w zakresie wszystkich obszarów wskazanych w ankiecie weryfikacji dojrzałości w zakresie cyberbezpieczeństwa, w tym nieobligatoryjne punkty ankiety, które zostały określone w Ankiecie weryfikacji dojrzałości w zakresie cyberbezpieczeństwa złożonej wraz z Wnioskiem o dofinansowanie.