

OPIS PRZEDMIOTU ZAMÓWIENIA (OPZ)

projekt pn.: „Cyfrowy ZOZ Dębica – rozwój e-usług i infrastruktury dla nowoczesnej opieki zdrowotnej” realizowanego na podstawie Wniosku o dofinansowanie nr KPOD.07.03-IP.10-0351/25, złożonego w ramach Krajowego Planu Odbudowy i Zwiększania Odporności (KPO),
komponent KPOD – Cyfryzacja w opiece zdrowotnej,
inwestycja D1.1.2 „Transformacja cyfrowa opieki zdrowotnej.



Dębica, luty 2026 r.

SPIS TREŚCI

Wstęp	4
Ogólny zarys projektu	4
Wymagania w zakresie równoważności	5
Wymagania w zakresie dostępności dla osób z niepełnosprawnościami oraz projektowania z przeznaczeniem dla wszystkich użytkowników	6
Ogólne warunki gwarancji	6
Ogólne warunki licencjonowania dostarczonych systemów informatycznych	7
Metodyka projektu	8
Etapy i ogólne zasady wdrożenia	8
Miejsce i termin realizacji przedmiotu zamówienia	9
Część I – Systemy medyczne, EDM i cyfryzacja dokumentacji	10
1. Elektroniczne podpisywanie oraz digitalizacja dokumentacji medycznej	10
2. System digitalizacji dokumentacji papierowej – 1 komplet	17
3. Urządzenia skanujące – 8 sztuk	19
3.1. Ogólny opis	19
3.2. Zakres prac	19
3.3. Wymagania dotyczące sprzętu	19
3.4. Minimalne warunki licencji na system	22
3.5. Licencja integracyjna HIS	24
3.6. Wdrożenie i szkolenia	24
3.7. Integracja systemu z działającym w placówce systemem HIS AMMS	26
3.8. Opieka nad systemem	26
3.9. Wymagania dla oprogramowania	27
3.10. Wymagane oświadczenia	30
4. Nowe funkcjonalności systemu HIS w zakresie integracji z platformą P1	31
4.1. Integracja z Rejestrem Endoprotezoplastyk	31
4.2. Ankieta Udarowa	33
4.3. Integracja z CeZ w zakresie digitalizacji karty leczenia - Ucyfrowienie + indeksacja	36
4.4. Rozszerzenie EDM o nowe dokumenty ustawowe wraz z monitorowaniem	39
4.5. Integracja z Krajowym Rejestrem Nowotworów	41
4.6. Karta uodpornień	44
4.7. Import e-Deklaracji z systemu P1	45

4.8. Upgrade Banku Krwi, Serologii, oraz Integracja z systemem e-Krew	47
4.9. Integracja z analizatorem serologicznym	54
4.10. WDSZ - Integracja z systemem digitalizacji dokumentacji	55
4.11. WDSZ - Integracja z ICPen.....	57
5. Licencja Oracle lub równoważna – 1 sztuka	58
Część II – Upgrade posiadanego systemu PACS/RIS wraz z integracją z PUI	62
1. Upgrade posiadanego systemu PACS/RIS wraz z integracją z PUI	62
Część III – Infrastruktura IT i cyberbezpieczeństwo	68
1. Serwer TYP 1 – 1 sztuka	68
2. Serwer TYP 2 – 1 sztuka.....	72
3. Rozbudowa serwerów – 1 komplet.....	76
4. Rozbudowa macierzy – 1 komplet.....	76
5. Rozbudowa serwerów NAS – 1 komplet	76
6. Deduplikator – 1 sztuka.....	76
7. Biblioteka taśmowa – 1 sztuka	78
8. Oprogramowanie do backupu i archiwizacji – 1 komplet.....	80
8.1. Oprogramowanie do backupu VM – 1 komplet	80
8.2. Archiwizacja poczty elektronicznej – 1 komplet	89
9. Oprogramowanie antywirusowe i EDR/XDR – 1 komplet	93
10. Przetątnik dostępowy PoE – 10 sztuk	105
11. Przetątnik szkieletowy – 2 sztuki	107
12. Bezprzewodowy punkt dostępowy – 14 sztuk	110
13. Rozszerzenie licencji UTM – 1 komplet	112
14. Komputer stacjonarny TYP1 – 80 sztuk.....	112
15. Komputer stacjonarny TYP 2 – 40 sztuk.....	118
16. Laptop – 4 sztuki.....	123
17. Komputer stacjonarny TYP 3 – 4 sztuki	128
18. Monitor – 4 sztuki.....	134
19. System Zarządzania Bezpieczeństwem Informacji – 1 komplet	134
20. Audyt końcowy w obszarze cyberbezpieczeństwa – 1 komplet	135
21. Szkolenia dla kadry kierowniczej i pracowników – 1 komplet.....	136
22. Instalacja, konfiguracja, wdrożenie i uruchomienie – 1 komplet.....	139

Wstęp

Niniejszy Opis Przedmiotu Zamówienia (OPZ) dotyczy realizacji projektu pn. „Cyfrowy ZOZ Dębica – rozwój e-usług i infrastruktury dla nowoczesnej opieki zdrowotnej”, realizowanego na podstawie Wniosku o dofinansowanie nr KPOD.07.03-IP.10-0351/25, złożonego w ramach Krajowego Planu Odbudowy i Zwiększania Odporności (KPO), komponent KPOD – Cyfryzacja w opiece zdrowotnej, inwestycja D1.1.2 – Rozwój cyfrowej infrastruktury szpitali.

Wszystkie parametry techniczne określone w niniejszym OPZ określają minimalne wymagania stawiane oferowanym urządzeniom, systemom i oprogramowaniu. Wykonawca nie ma prawa żądać dodatkowego wynagrodzenia, jeżeli dostarczone elementy systemów będą posiadały funkcjonalność wyższą niż wymagana niniejszym OPZ.

Ogólny zarys projektu

Projekt realizowany jest przez Zespół Opieki Zdrowotnej w Dębicy, podmiot leczniczy wykonujący działalność leczniczą w rodzaju świadczenia szpitalne, zakwalifikowany do systemu podstawowego szpitalnego zabezpieczenia świadczeń opieki zdrowotnej na II poziomie zabezpieczenia. Przedsięwzięcie jest zgodne z regulaminem naboru, zasadami kwalifikowalności wydatków oraz harmonogramem rzeczowo-finansowym określonym we Wniosku o dofinansowanie.

Celem projektu jest kompleksowa transformacja cyfrowa ZOZ w Dębicy poprzez podjęcie działań inwestycyjnych, które przyczynią się do zwiększenia dostępności, efektywności i bezpieczeństwa świadczonych usług medycznych., poprzez:

- integrację i rozbudowę systemów informatycznych szpitala,
- cyfryzację dokumentacji medycznej,
- rozwój rozwiązań opartych na sztucznej inteligencji (AI) oraz podłączenie do centralnego repozytorium danych medycznych, w tym integrację z systemem P1 oraz Platformą Usług Inteligentnych (PUI) Centrum e-Zdrowia.,
- zwiększenie poziomu cyberbezpieczeństwa przetwarzania danych medycznych,

Zakres zamówienia określony w niniejszym OPZ wynika bezpośrednio z zatwierdzonego Wniosku o dofinansowanie i obejmuje realizację zadań projektowych, których celem jest w szczególności:

- zapewnienie zgodności funkcjonujących systemów szpitalnych z obowiązującymi przepisami prawa, w tym ustawą o systemie informacji w ochronie zdrowia oraz aktami wykonawczymi Ministra Zdrowia,
- umożliwienie pełnego prowadzenia, przetwarzania, indeksowania oraz udostępniania Elektronicznej Dokumentacji Medycznej (EDM), w tym przekazywania danych do systemów centralnych,
- podniesienie poziomu bezpieczeństwa informacji i ciągłości działania systemów IT, w tym zabezpieczenie przetwarzania EDM potwierdzone audytem cyberbezpieczeństwa,
- poprawę dostępności i jakości usług zdrowotnych świadczonych na rzecz pacjentów ZOZ w Dębicy.

Przedmiot zamówienia obejmuje dostawy, usługi oraz wartości niematerialne i prawne, niezbędne do prawidłowej realizacji projektu, zgodnie z harmonogramem, budżetem oraz wskaźnikami produktu i rezultatu określonymi we Wniosku o dofinansowanie.

Zamówienie realizowane będzie w sposób zapewniający:

- osiągnięcie wszystkich wskaźników projektu, w tym integracji z systemem P1, digitalizacji dokumentacji medycznej, zabezpieczenia przetwarzania EDM oraz podłączenia do centralnego repozytorium danych medycznych w zakresie AI,
- zgodność z zasadami konkurencyjności, efektywności wydatkowania środków publicznych oraz przepisami ustawy Prawo zamówień publicznych,
- trwałość rezultatów projektu przez okres wymagany przepisami KPO.

Niniejszy OPZ stanowi podstawę do przygotowania i przeprowadzenia postępowań o udzielenie zamówień publicznych niezbędnych do realizacji projektu oraz do zawarcia umów z Wykonawcami odpowiedzialnymi za jego wykonanie. Dokument ten ma charakter nadrzędny w zakresie opisu funkcjonalnego i technicznego przedmiotu zamówienia oraz stanowi podstawę do oceny ofert, realizacji umów, odbiorów, rozliczeń oraz weryfikacji trwałości projektu. W przypadku rozbieżności pomiędzy opisem ogólnym a wymaganiami szczegółowymi, wiążące są zapisy części szczegółowych OPZ.

Wymagania w zakresie równoważności

W celu zachowania zasad neutralności technologicznej oraz uczciwej konkurencji, Zamawiający dopuszcza stosowanie rozwiązań równoważnych w stosunku do rozwiązań wyspecyfikowanych w niniejszym OPZ.

Przez rozwiązanie równoważne rozumie się rozwiązanie, które pod względem technologicznym, funkcjonalnym oraz wydajnościowym nie odbiega w sposób istotny od rozwiązań określonych w OPZ, przy czym ocenie podlegają wyłącznie te cechy i parametry, które stanowią o istocie i celu zakładanych rozwiązań technologicznych oraz posiadają swoje odpowiedniki w rozwiązaniu równoważnym.

Nie podlegają porównaniu cechy właściwe wyłącznie dla rozwiązania wyspecyfikowanego, w szczególności takie jak:

zastrzeżone patenty, własnościowe rozwiązania technologiczne, własnościowe protokoły komunikacyjne lub inne elementy o charakterze proprietarnym, o ile nie stanowią one niezbędnego elementu realizacji funkcjonalności wymaganych przez Zamawiającego.

W związku z powyższym, Wykonawca może zaproponować rozwiązania realizujące funkcjonalności określone przez Zamawiającego w sposób odmienny niż wskazany w OPZ, pod warunkiem zapewnienia co najmniej takiej samej lub bardzo zbliżonej wartości użytkowej, bezpieczeństwa, interoperacyjności oraz zgodności z obowiązującymi przepisami prawa.

Za rozwiązanie równoważne nie uznaje się rozwiązania identycznego (tożsamego), lecz rozwiązanie alternatywne, które w zakresie porównywanych cech spełnia wymagania Zamawiającego w sposób równoważny.

W przypadku zaoferowania rozwiązania równoważnego, Wykonawca zobowiązany jest wykazać jego równoważność w ofercie, w szczególności poprzez przedstawienie opisu funkcjonalnego, parametrów technicznych oraz wskazanie spełnienia wymagań określonych w niniejszym OPZ.

Wykonawca ponosi pełną odpowiedzialność za dostawę, konfigurację, integrację oraz wdrożenie w pełni funkcjonujących rozwiązań, zgodnych z niniejszym OPZ, również w przypadku gdy realizacja zamówienia wymaga pozyskania dodatkowych informacji, zawarcia niezbędnych umów licencyjnych, integracyjnych lub innych czynności niezbędnych do prawidłowego wykonania przedmiotu zamówienia.

Wymagania w zakresie dostępności dla osób z niepełnosprawnościami oraz projektowania z przeznaczeniem dla wszystkich użytkowników

Zamawiający wymaga, aby przedmiot zamówienia był zaprojektowany i wykonany z uwzględnieniem zasad dostępności dla osób z niepełnosprawnościami oraz projektowania uniwersalnego, tj. w sposób umożliwiający korzystanie z jego funkcjonalności przez możliwie najszerszą grupę użytkowników, niezależnie od ich sprawności fizycznej, sensorycznej lub poznawczej.

1. Wszelkie systemy informatyczne, aplikacje, portale oraz e-usługi objęte przedmiotem zamówienia muszą spełniać wymagania dostępności cyfrowej zgodnie ze standardem WCAG 2.1 na poziomie AA, w szczególności w zakresie:
 - a. czytelności i jednoznaczności interfejsów użytkownika,
 - b. możliwości obsługi przy użyciu technologii asystujących,
 - c. odpowiedniego kontrastu, skalowalności treści oraz obsługi klawiaturowej,
 - d. zapewnienia dostępności dla osób z niepełnosprawnościami wzroku, słuchu, ruchu oraz poznawczymi.
2. W ramach dostaw sprzętu Zamawiający wymaga rozwiązań wspierających ergonomię i dostępność stanowisk pracy, w tym w szczególności:
 - a. zastosowania monitorów o zwiększonej przekątnej, poprawiających komfort pracy osób z zaburzeniami wzroku,
 - b. urządzeń mobilnych umożliwiających alternatywne formy identyfikacji i autoryzacji użytkownika,
 - c. urządzeń skanujących i digitalizujących dokumentację, ograniczających konieczność manualnej obsługi dokumentów papierowych.
3. Wdrażane systemy medyczne i okołomedyczne (w tym systemy klasy RIS/PACS) muszą być zaprojektowane w sposób zapewniający intuicyjną obsługę, ograniczenie obciążeń poznawczych personelu oraz równy dostęp do informacji medycznej, wyników badań i dokumentacji, niezależnie od poziomu kompetencji cyfrowych użytkownika.
4. Przedmiot zamówienia nie może zawierać rozwiązań prowadzących do jakiegokolwiek formy wykluczenia lub dyskryminacji użytkowników końcowych. Wymagania techniczne i funkcjonalne zostały określone w sposób neutralny, obiektywny i proporcjonalny, z poszanowaniem zasady równego traktowania.
5. Przyjęte w OPZ rozwiązania zapewniają równy dostęp do efektów realizacji zamówienia wszystkim odbiorcom usług Zamawiającego, w tym osobom z niepełnosprawnościami, seniorom oraz osobom o ograniczonych kompetencjach cyfrowych.
6. Wymiana Danych Systemowych z Zewnętrznymi).

Ogólne warunki gwarancji

1. Wszędzie tam, gdzie w niniejszym OPZ, umowie lub załącznikach do niej nie wskazano okresu gwarancji albo nie określono go w sposób odmienny, przyjmuje się okres gwarancji wynoszący 36 miesięcy, liczony od dnia podpisania bez zastrzeżeń końcowego protokołu odbioru przedmiotu zamówienia.
2. W okresie obowiązywania gwarancji Wykonawca zapewnia zdalne usuwanie usterek, awarii oraz błędów oprogramowania, a w przypadku braku możliwości skutecznego usunięcia problemu w trybie zdalnym – również usuwanie usterek w siedzibie Zamawiającego.
3. Wykonawca zobowiązany jest do zdalnego, a w razie konieczności stacjonarnego, usuwania błędów baz danych, w szczególności związanych z brakiem spójności, integralności danych lub nieprawidłowym działaniem mechanizmów bazodanowych.

4. W ramach gwarancji Wykonawca zobowiązany jest do konfiguracji oraz udzielania pomocy technicznej przy instalacji i konfiguracji oprogramowania systemowego serwerów produkcyjnych, w zakresie niezbędnym do prawidłowego funkcjonowania wdrożonych systemów.
5. Wykonawca zapewnia dokonywanie aktualizacji oprogramowania w miarę wprowadzania modyfikacji, poprawek i ulepszeń własnych aplikacji objętych przedmiotem zamówienia, o ile aktualizacje te są dostępne w ramach posiadanych przez Zamawiającego licencji.
6. Wykonawca zobowiązany jest do bieżącego informowania Zamawiającego o dostępnych aktualizacjach, poprawkach oraz zmianach oprogramowania, w szczególności tych mających istotne znaczenie dla bezpieczeństwa informacji, stabilności oraz prawidłowego funkcjonowania systemów.
7. W ramach gwarancji Wykonawca zapewnia zdalną instalację aktualizacji i poprawek, a w uzasadnionych przypadkach również ich instalację w siedzibie Zamawiającego, o ile warunki licencyjne oprogramowania komercyjnego dopuszczają pobieranie i instalowanie aktualizacji w ramach posiadanej licencji.
8. Wszystkie błędy i awarie oprogramowania ujawnione w okresie gwarancji będą usuwane na koszt Wykonawcy, bez dodatkowych opłat po stronie Zamawiającego.
9. W przypadku awarii sprzętu lub systemu skutkującej utratą lub niedostępnością danych, Wykonawca zobowiązany jest do zapewnienia rekonfiguracji lub ponownej instalacji systemów oraz przywrócenia danych z dostępnych kopii zapasowych, w zakresie wynikającym z przedmiotu zamówienia.
10. Czas naprawy oprogramowania użytkowego, o którym mowa w niniejszym OPZ, odnosi się wyłącznie do oprogramowania dostarczonego w ramach zamówienia, w odniesieniu do którego Wykonawca posiada prawną i techniczną możliwość ingerencji w kod źródłowy lub konfigurację systemu.
11. W ramach odbioru końcowego Wykonawca zobowiązany jest do przekazania kompletnej dokumentacji powykonawczej, obejmującej co najmniej:
 - opis użytych bibliotek, funkcji oraz parametrów konfiguracyjnych,
 - szczegółowy schemat baz danych systemu, z uwzględnieniem powiązań i zależności pomiędzy tabelami,
 - opis techniczny procedur aktualizacyjnych i odtworzeniowych,
 - wszelkie inne materiały uzupełniające niezbędne do prawidłowej eksploatacji, administracji oraz rozwoju wdrożonych systemów.

Ogólne warunki licencjonowania dostarczonych systemów informatycznych

1. Licencjobiorcą wszystkich licencji na oprogramowanie dostarczane w ramach realizacji przedmiotu zamówienia będzie Zamawiający – Zespół Opieki Zdrowotnej w Dębicy.
2. Oferowane licencje muszą umożliwiać legalne użytkowanie oprogramowania zgodnie z obowiązującymi przepisami prawa, w szczególności w zakresie przetwarzania danych osobowych oraz danych medycznych.
3. Licencja oprogramowania nie może ograniczać prawa Zamawiającego do rozbudowy środowiska informatycznego, w tym w szczególności:
 - zwiększenia liczby serwerów obsługujących oprogramowanie,
 - zmiany architektury środowiska (np. wydzielenia serwera aplikacyjnego, bazodanowego lub plików),
 - przeniesienia danych lub systemów pomiędzy serwerami w ramach infrastruktury Zamawiającego.

4. Licencja oprogramowania musi umożliwiać instalację i użytkowanie oprogramowania bez ograniczeń co do liczby użytkowników, komputerów klienckich oraz serwerów, na których oprogramowanie może być zainstalowane i wykorzystywane, o ile nie wskazano inaczej w wymaganiach szczegółowych OPZ.
5. Licencja na oprogramowanie nie może ograniczać sposobu pracy użytkowników końcowych, w tym w szczególności pracy w sieci lokalnej (LAN), pracy zdalnej poprzez sieć Internet lub inne bezpieczne kanały komunikacji.
6. Licencja oprogramowania nie może ograniczać prawa Zamawiającego do wykonywania kopii bezpieczeństwa oprogramowania oraz danych, w liczbie uznanej przez Zamawiającego za niezbędną, w celu zapewnienia ciągłości działania oraz bezpieczeństwa informacji.
7. Licencja oprogramowania nie może ograniczać prawa Zamawiającego do instalowania i użytkowania oprogramowania na serwerach zapasowych, uruchamianych w przypadku awarii lub niedostępności serwerów podstawowych, w tym w środowiskach wysokiej dostępności (HA) lub odtworzeniowych (DR).
8. Licencja oprogramowania nie może być przypisana do konkretnego urządzenia lub stanowiska roboczego, a Zamawiający musi mieć możliwość korzystania z oprogramowania na dowolnym komputerze klienckim spełniającym wymagania techniczne.
9. Licencja na oprogramowanie powinna mieć charakter bezterminowy, bez ograniczeń czasowych oraz bez konieczności ponoszenia dodatkowych opłat licencyjnych w celu dalszego korzystania z oprogramowania po zakończeniu realizacji projektu, z zastrzeżeniem odrębnych zasad dotyczących usług utrzymania lub wsparcia, o ile zostały przewidziane w OPZ.

Metodyka projektu

W celu efektywnej realizacji projektu wdrożeniowego rozwiązania ZSI, projekt powinien być realizowany zgodnie z zaproponowaną przez wykonawcę i zaakceptowaną przez Zamawiającego metodyką projektową zgodną ze standardami branżowymi dostępnymi powszechnie, tj. PRINCE 2, IPMA lub innymi równoważnymi standardami, w tym metodyki zwinne AGILE takie jak SCRUM.

Wykonawca jest zobowiązany wraz z zaproponowaną metodyką dostarczyć jej szczegółowy opis zawierający minimalnie strukturę zadań, podział obowiązków, ról w projekcie, harmonogram, opisy podstawowych procesów oraz dyscyplin projektowych. W razie zaproponowania równoważnej metodyki opartej o równoważne standardy Wykonawca musi wykazać ich równoważność w zakresie wskazanym w powyższym zapisie.

Etapy i ogólne zasady wdrożenia

Zamawiający oczekuje, że Wykonawca przedstawi Szczegółowy Harmonogram Rzeczowo-Finansowy opracowany zgodnie ze swoją metodyką wdrożeniową, wraz ze szczegółową strukturą zadań oraz produktów poszczególnych etapów projektu z uwzględnieniem spodziewanych przez Zamawiającego dat uruchomienia poszczególnych elementów projektu, jednak nie mniej niż w podziale na:

- prace przygotowawcze, analiza przedwdrożeniowa,
- dostawa sprzętu teleinformatycznego,
- dostawa licencji, instalacja oprogramowania na infrastrukturze Zamawiającego,
- wdrożenie poszczególnych modułów systemów w kolejności pozwalającej na optymalne obciążenie pracą zespołu Zamawiającego i Wykonawcy, obejmujące podział na: prace konfiguracyjne, szkolenia personelu, uruchomienie modułu, oddanie modułu,

- migracje danych zgodnie z wymaganiami poszczególnych modułów uwzględniające termin oraz zakres migrowanych danych

Szczegółowy opis tego zakresu musi znaleźć się w analizie przedwdrożeniowej

- zwłaszcza w zakresie terminów i danych wymaganych od Zamawiającego do przekazania Wykonawcy,
- terminy i zakresy integracji pomiędzy poszczególnymi systemami zarówno nowymi jak i obecnie używanymi. Zamawiający oczekuje, że Wykonawca określi przewidywane.

OGÓLNE WARUNKI WDROŻENIA (KPO)

Wdrożenie oprogramowania i sprzętu realizowane w ramach niniejszego zamówienia musi być przeprowadzone w sposób zapewniający osiągnięcie celów projektu finansowanego ze środków Krajowego Planu Odbudowy, w szczególności w zakresie trwałości rezultatów, interoperacyjności rozwiązań oraz zgodności z obowiązującymi przepisami prawa i wytycznymi programowymi.

O ile w Opisie Przedmiotu Zamówienia nie określono odmiennych lub szczegółowych wymagań dotyczących wdrożenia poszczególnych elementów przedmiotu zamówienia, Wykonawca zobowiązany jest do realizacji wdrożenia zgodnie z ogólnymi zasadami wdrażania systemów informatycznych oraz infrastruktury IT, obejmującymi w szczególności:

- dostawę, instalację, konfigurację i uruchomienie oprogramowania oraz sprzętu,
- zapewnienie kompatybilności z istniejącą infrastrukturą i systemami Zamawiającego,
- realizację niezbędnych integracji w celu zapewnienia ciągłości procesów i wymiany danych,
- przeprowadzenie testów potwierdzających poprawność, bezpieczeństwo i stabilność działania rozwiązania,
- przekazanie rozwiązania do użytkowania wraz z kompletną dokumentacją oraz przeszkoleniem użytkowników i administratorów.

Wdrożenie musi być realizowane zgodnie z najlepszymi praktykami branżowymi, z uwzględnieniem zasad bezpieczeństwa informacji, ochrony danych osobowych, zapewnienia ciągłości działania oraz wymagań wynikających z dokumentów programowych KPO, w tym w zakresie trwałości i efektywności wykorzystania środków publicznych.

Pełna odpowiedzialność za prawidłowe wykonanie wdrożenia, osiągnięcie wymaganej funkcjonalności oraz zgodność rozwiązania z OPZ spoczywa na Wykonawcy.

Miejsce i termin realizacji przedmiotu zamówienia

Dostawy i usługi będą realizowane w siedzibie Zamawiającego, tj.

Zespół Opieki Zdrowotnej w Dębicy, Krakowska 91, 39-200 Dębica.

Termin realizacji przedmiotu zamówienia:

od dnia podpisania umowy, nie później niż do **31.05.2026 r.**

Część I – Systemy medyczne, EDM i cyfryzacja dokumentacji

1. Elektroniczne podpisywanie oraz digitalizacja dokumentacji medycznej

1. Przedmiot zamówienia

Przedmiotem zamówienia jest rozbudowa i integracja systemu szpitalnego o możliwość elektronicznego podpisu dokumentów przez pacjenta oraz digitalizacji dokumentacji wymagającej podpisu, poprzez:

- dostawę i wdrożenie systemu digitalizacji dokumentów (dalej: System),
- integrację Systemu z HIS AMMS oraz IC Pen,
- dostawę urządzeń do zbierania podpisu, wyświetlania treści oraz skanowania dokumentów, a także czytników e-Dowodu,
- dostawę licencji,
- przeprowadzenie szkoleń,
- świadczenie opieki serwisowej wraz z nadzorem autorskim przez 36 miesięcy od zakończenia wdrożenia.

System ma umożliwiać digitalizację pisma odręcznego, podpisu odręcznego (biometrycznego), podpisu osobistego z e-Dowodu oraz obsługę skanowania zewnętrznej dokumentacji medycznej wraz z możliwością opatrzenia jej podpisem cyfrowym.

2. Zakres prac i dostaw

W ramach zamówienia Wykonawca zobowiązany jest do:

1. Dostawy sprzętu:
 - Długopis cyfrowy – 5 szt.,
 - ekrany wraz z uchwytami – 15 szt.,
 - tablet – 46 szt.,
 - czytniki e-Dowodu – 5 szt..
2. Dostawy licencji na System w liczbie 66 szt. (lub równoważny model licencjonowania umożliwiający pracę na co najmniej 66 stanowiskach).
3. Instalacji i wdrożenia Systemu w środowisku Zamawiającego, w tym integracji z HIS AMMS i IC Pen.
4. Przeprowadzenia szkoleń dla użytkowników oraz administratorów.
5. Świadczenia opieki serwisowej wraz z nadzorem autorskim dla wszystkich licencji przez 36 miesięcy.

3. Wymagania dotyczące sprzętu

3.1. Czytnik e-Dowodu (3 szt.)

1. Klasa bezpieczeństwa minimum 4.
2. Obsługa funkcji eID oraz eSIGN.
3. Interfejs USB 2.0.
4. Zintegrowana klawiatura i wyświetlacz.
5. Klawiatura umożliwia wprowadzanie kodu PIN.
6. Podświetlany wyświetlacz LCD.

7. Rozmiar wyświetlacza nie większy niż 6,5 × 1,7 cm.
8. Wskaźnik stanu pracy.
9. Spełnienie wymogów MSWiA.
10. Gwarancja minimum 24 miesiące od dostawy; koszty napraw, części i transportu po stronie Wykonawcy.

3.2. Ekran do podpisu (15 szt.)

1. Rozdzielczość min. Full HD (1920×1080), przekątna co najmniej 13”.
2. Podłączenie do komputera przez USB-C.
3. Brak baterii.
4. Brak systemu operacyjnego (praca jako monitor).
5. Wymiary maks. 34 cm × 23 cm × 1,5 cm.
6. Waga maks. 950 g.
7. Rysik o czułości min. 4000 poziomów nacisku.
8. Możliwość trwałego przymocowania rysika i jego wymiany w razie awarii.
9. Gwarancja minimum 36 miesięcy od dostawy; koszty napraw, części i transportu po stronie Wykonawcy.

3.3. Tablet z rysikiem i etui (46 szt.)

Przedmiotem zamówienia jest dostawa 46 szt. fabrycznie nowych tabletów, nieużywanych, wolnych od wad fizycznych i prawnych, pochodzących z oficjalnego kanału dystrybucji producenta, przeznaczonych do pracy biurowej i mobilnej w jednostce Zamawiającego.

Wymagania ogólne

1. Dostarczony tablet musi być fabrycznie nowy, niepochodzący z ekspozycji ani regenerowany, pochodzić z bieżącej lub nadal produkowanej linii produktowej, posiadać komplet akcesoriów przewidzianych przez producenta, spełniać wymagania obowiązujących norm i przepisów prawa na terenie UE.
2. Minimalne wymagania techniczne
3. Ekran
 1. przekątna: min. 10 cali,
 2. technologia: LCD lub OLED,
 3. rozdzielczość: min. 1920 × 1200 px,
 4. obsługa wielodotyku.
4. Wydajność
 1. procesor wielordzeniowy,
 2. pamięć RAM: min. 4 GB,
 3. pamięć masowa: min. 64 GB.
5. Łączność
 1. Wi-Fi (standard co najmniej 802.11ac),
 2. Bluetooth,
 3. port USB typu C lub równoważny.
6. Multimedia
 1. wbudowana kamera przednia,
 2. wbudowana kamera tylna,
 3. głośniki stereo,
 4. mikrofon.
7. Zasilanie
 1. akumulator umożliwiający co najmniej 8 godzin pracy przy typowym użytkowaniu,
 2. ładowanie przewodowe.
8. Oprogramowanie

Tablet musi być dostarczony z zainstalowanym fabrycznym systemem operacyjnym producenta, systemem umożliwiającym instalację aplikacji biurowych i użytkowych, menu w języku polskim lub angielskim.

9. Tablet musi być objęty gwarancją producenta na okres co najmniej 36 miesięcy, liczoną od dnia podpisania protokołu odbioru.
10. Gwarancja realizowana jest w standardowym trybie producenta.
11. Warunki równoważności
Zamawiający dopuszcza oferowanie tabletów równoważnych, pod warunkiem spełnienia wszystkich minimalnych wymagań określonych w OPZ.

4. Minimalne wymagania licencyjne na System

1. Z chwilą dostarczenia rozwiązania (lub jego części) Wykonawca udzieli Zamawiającemu niewyłącznej licencji na czas nieokreślony od daty podpisania końcowego protokołu odbioru bez uwag, na polach eksploatacji co najmniej:
 - o wprowadzanie do pamięci komputera,
 - o korzystanie,
 - o sporządzanie kopii zapasowej,
 - o przenoszenie pomiędzy stanowiskami.
2. Licencja obejmuje prawo Zamawiającego do korzystania z dokumentów/generatorów treści wytworzonych przez System (raporty, analizy, dokumenty) w zakresie utrwalania, zwielokrotniania, publikowania i wykorzystywania w działalności Zamawiającego.
3. Licencja obowiązuje na terytorium RP.
4. Zamawiający może wykonywać prawa licencyjne przy udziale podmiotów trzecich świadczących usługi na jego rzecz.
5. Brak prawa przenoszenia licencji na inne podmioty, z wyłączeniem zmian formy prawnej lub struktury właścicielskiej Zamawiającego.
6. Wykonawca oświadcza, że dysponuje prawami do oferowanego rozwiązania lub prawem do udzielania sublicencji oraz że korzystanie z niego nie naruszy praw osób trzecich.

5. Licencja i odpowiedzialność za integrację z HIS AMMS

1. Wykonawca oświadcza, że posiada prawa do realizacji integracji lub do udzielania sublicencji w tym zakresie oraz że integracja nie narusza praw osób trzecich.
2. Po upływie 12 miesięcy od odbioru końcowego, opłaty należne dostawcy HIS za wsparcie modułu integracyjnego ponosi Zamawiający.
3. Zamawiający nie posiada kodów źródłowych HIS – Wykonawca jest zobowiązany do samodzielnej współpracy z dostawcą HIS i zapewnienia realizacji prac integracyjnych zarówno po stronie Systemu, jak i po stronie dostawcy HIS.

6. Wymagania funkcjonalne – System (oprogramowanie)

6.1. Środowisko pracy i bezpieczeństwo

1. System musi działać w odizolowanym środowisku na infrastrukturze Zamawiającego, bez dostępu do Internetu i bez połączeń poza sieć Zamawiającego.
2. System musi wykorzystywać lokalną bazę danych open-source bez kosztów licencyjnych.
3. System musi umożliwiać uruchomienie w klastrze wysokiej dostępności (HA).
4. System musi umożliwiać integrację z Active Directory oraz – dla aplikacji na Windows – SSO (Kerberos).

6.2. Formularze, szablony i wersjonowanie

1. System musi posiadać Aplikację Centralną dostępną z przeglądarki, z logowaniem użytkownika.
2. System musi umożliwiać implementację nowych formularzy przez import tła PDF i nanoszenie regionów aktywnych (pola podpisu, tekstowe, wyboru), które trafiają do wynikowego PDF i są zgodne ze specyfikacją PDF (kompatybilność z przeglądarkami PDF).
3. System musi umożliwiać obsługę innych plików PDF nie zdefiniowanych wcześniej.
4. System musi umożliwiać zarządzanie wersjami formularzy (dowolna liczba wersji, wskazanie wersji obowiązującej).

6.3. Repozytorium dokumentów w Systemie

1. System musi posiadać mechanizmy zapisywania, przechowywania i katalogowania dokumentów.
2. System musi umożliwiać tworzenie/usuwanie/zmianę nazw katalogów i podkatalogów.
3. System musi umożliwiać przenoszenie dokumentów pomiędzy katalogami oraz definiowanie katalogów domyślnych.
4. System musi umożliwiać konfigurację struktury rekordów (katalogowanie dokumentów jako rekordy wg danych z dokumentu).

6.4. Zarządzanie stanowiskami i statusami

1. System musi umożliwiać zarządzanie stanowiskami (typ urządzenia, status komunikacji), przegląd zdarzeń oraz zdalną zmianę konfiguracji.
2. System musi umożliwiać śledzenie statusu podpisywania dokumentów.
3. System musi umożliwiać nakładanie pieczętek w polach podpisu (konfigurowalnych).

6.5. Użytkownicy i uprawnienia

1. System musi posiadać panel administracyjny w Aplikacji Centralnej.
2. System musi umożliwiać tworzenie kont i zarządzanie nimi.
3. System musi umożliwiać nadawanie uprawnień w celu minimalizacji dostępu (role/grupy).

6.6. Monitoring, logi, metryki, alerty

1. System musi zbierać logi audytowe umożliwiające śledzenie działań per dokument/użytkownik/urządzenie oraz umożliwiać konfigurację retencji audytu.
2. System musi umożliwiać monitorowanie w czasie rzeczywistym wydajności (CPU/RAM/Dysk/Sieć) i centralizację logów z różnych źródeł.
3. System musi zapewnić narzędzia do budowy dashboardów i samodzielnej konfiguracji alertów oraz retencji metryk i logów.
4. System musi zapewnić mechanizmy zabezpieczeń dostępu do logów i metryk oraz możliwość raportowania i eksportu danych.

6.7. Integracje (REST, wirtualna drukarka, powiadomienia)

1. System musi umożliwiać integrację z systemami zewnętrznymi poprzez REST API.
2. System musi umożliwiać wystanie dokumentu do podpisu poprzez wirtualną drukarkę, a w razie braku pól podpisu – ręczne wskazanie ich lokalizacji.
3. System musi umożliwiać przesłanie do podpisu dowolnego PDF i „ukrycie” informacji o polach podpisu w treści dokumentu bez konieczności przekazywania ich w wywołaniu integracyjnym.
4. System musi umożliwiać cofnięcie autoryzacji integracji.
5. System musi umożliwiać automatyczne powiadomienia o podpisaniu dokumentu na wskazany webservice (bez prac po stronie dostawcy).

6.8. Podpisy

1. Podpis odręczny musi być składany w kontekście dokumentu (jak na papierze) – dokument musi być widoczny na urządzeniu podpisu.

2. System musi umożliwiać składanie pisma odręcznego również poza polami podpisu (dowolna treść).
3. System powinien wspierać podpis odręczny biometryczny (np. nacisk, znaczniki czasu) w celu weryfikacji autentyczności.
4. System musi umożliwiać podpis osobisty z e-Dowodu.
5. System musi umożliwiać podpis elektroniczny (min. PDF) podpisem osobistym oraz podpisami kwalifikowanymi różnych dostawców.

7. Wymagania funkcjonalne – urządzenia i aplikacje stanowiskowe

7.1. Aplikacja skanowania (Windows 10/11 x64)

1. Obsługa automatycznego skanowania dokumentów z możliwością podpisu (kwalifikowany/niekwalifikowany/osobisty).
2. Lokalny zapis skanów, automatyczne nazewnictwo i hasło wg szablonu (jeżeli dotyczy).
3. Pobieranie danych opisujących dokument bezpośrednio z dokumentu, regulacja kompresji, dzielenie skanów co N stron.
4. OCR bez limitów rozpoznawanych dokumentów.
5. Dzielenie kompletów z ADF, wyszukiwarka dokumentów, weryfikacja danych przed zatwierdzeniem.
6. Wymóg uwierzytelnienia użytkownika.
7. Obsługa wersji roboczych nieprzetworzonych skanów.
8. Rozpoznawanie szablonów i współrzędnych pól, dzielenie wg szablonów i dołączanie stron „bez szablonu”.
9. Możliwość ustawienia domyślnego szablonu skanowania.
10. Wsparcie urządzeń przez TWAIN.
11. Zarządzanie dokumentami przed wystąpieniem do HIS odbywa się w aplikacji Systemu na stacji roboczej podłączonej do skanera.

7.2. Stanowisko z ekranem do podpisu (Windows 10/11 x64)

1. Ekran na stałe połączony z komputerem; digitalizacja w czasie rzeczywistym.
2. Możliwość prezentacji treści multimedialnych na ekranie w trybie bezczynności (konfiguracja w panelu admin).
3. Edycja pól aktywnych podczas podpisywania (tekst, wybór, checkbox).
4. Utrzymanie stałego połączenia aplikacji z serwerem (wywołanie dokumentu bez aktywności użytkownika).
5. Funkcje zoom/pan dokumentu.
6. Operator ma podgląd i kontrolę procesu na swoim monitorze (synchronizacja widoków).
7. Synchronizacja musi działać w czasie rzeczywistym i być realizowana lokalnie (bez obciążania sieci).
8. Możliwość logowania wielu użytkowników i przetaczania kont.

8. Integracja z HIS AMMS

Wykonawca – we współpracy z dostawcą HIS – zapewni co najmniej:

1. Dodawanie szablonów dokumentów do integracji poprzez edytor Systemu.
2. Wypełnianie pól aktywnych danymi pacjenta i jednostki organizacyjnej pobieranymi z AMMS.
3. Powiązanie klasy dokumentacji AMMS z szablonem.
4. Dostosowanie istniejących szablonów AMMS do obsługi digitalizacji (znaczniki pól podpisu/tekst/wybór + możliwość przekazania dokumentu do Systemu).

5. Dla dokumentów z pkt 4 – możliwość uzupełnienia dokumentu o dane wpisywane w formularzu AMMS przy generowaniu.
6. Generowanie dokumentu z widoku Dokumentacji Medycznej AMMS dla konkretnego pacjenta.
7. Jednoznaczne powiązanie dokumentu z pacjentem i kontekstem utworzenia.
8. Wybór urządzenia docelowego do podpisu:
 - automatycznie na stacji roboczej (długopis cyfrowy/ekran),
 - ręcznie z listy (tablety mobilne),przy czym System udostępni AMMS interfejs sieciowy do pobrania listy urządzeń.
9. Wskazanie urządzenia docelowego poprzez słownik AMMS.
10. Automatyczne udostępnienie podpisanego dokumentu w AMMS w widoku Dokumentacji Medycznej z powiązaniem do klasy dokumentu i szablonu.
11. Parametr AMMS określający zapis jako nowy dokument vs. nowa wersja dokumentu tego samego typu.
12. Uwierzytelnianie do Systemu danymi AMMS oraz – jeśli dostępne – logowanie domenowe.
13. Możliwość załączenia zeskanowanej dokumentacji dostarczonej przez pacjenta do Dokumentacji Medycznej AMMS wraz ze wskazaniem pacjenta i klasy dokumentu bezpośrednio w aplikacji Systemu.

9. Wdrożenie i szkolenia

9.1. Zakres wdrożenia

Wykonawca zrealizuje co najmniej:

1. Modyfikację oprogramowania na maszynie wirtualnej w infrastrukturze Zamawiającego.
2. Rozmieszczenie sprzętu na stanowiskach wskazanych przez Zamawiającego.
3. Instalację oprogramowania na stanowiskach lub dostarczenie instalatorów do instalacji domenowej.
4. Konfigurację i parametryzację współpracy z urządzeniami.
5. Uruchomienie integracji HIS–System w uzgodnieniu z dostawcą AMMS.
6. Przekazanie zestawu parametrów/zmiennych wymaganych do działania integracji.
7. Przekazanie dokumentacji powdrożeniowej.

Zamawiający może wskazać w trakcie wdrożenia mniejszą liczbę stanowisk do uruchomienia; pozostałe instalacje Wykonawca wykona w ramach serwisu, nie później niż 20 dni roboczych od zlecenia.

9.2. Szkolenia

1. Szkolenia obejmą użytkowników (personel medyczny) i administratorów.
2. Tryb: audytoryjny i/lub stanowiskowy (dwa terminy na stanowisko).
3. Plan szkolenia dla ok. 35 osób (liczba dokładna do 10 dni od umowy).
4. Każdy uczestnik ma przejść pełen proces: generowanie dokumentu → podpis → zapis w systemie.
5. Wykonawca zapewni potwierdzenia uczestnictwa.
6. Szkolenia w dni robocze 8:00–15:00; możliwość przejścia na tryb zdalny w sytuacji epidemiologicznej.
7. Materiały: filmy instruktażowe lub instrukcje stanowiskowe.
8. Harmonogram szkoleń: propozycja min. 3 dni robocze przed startem; uwagi Zamawiającego uwzględniane lub nowa propozycja w 2 dni robocze.
9. Szkolenia mogą zostać przesunięte poza okres wdrożenia; Wykonawca zrealizuje je w ramach serwisu nie później niż 30 dni roboczych od zlecenia.

10. Opieka serwisowa – 36 miesięcy (SLA)

Wykonawca zapewni przez 36 miesięcy:

- nowe wersje, poprawki bezpieczeństwa, hotfixy,
- prace programistyczne/konfiguracyjne w razie awarii,
- wsparcie techniczne w godzinach 8:00–16:00 (dni robocze),
- realizację SLA:

Czas reakcji: do 2h roboczych (od rejestracji zgłoszenia do przyjęcia).

Awaria krytyczna: usunięcie do 8h roboczych od końca reakcji (dopuszczalne obejście tymczasowe).

Wada aplikacji: do 5 dni roboczych.

Usterka programistyczna: do 10 dni roboczych.

Konsultacje: do 10 dni roboczych.

11. Kryteria odbioru produktu

Produkt zostanie uznany za zgodny z OPZ, jeżeli spełni łącznie następujące kryteria:

1. Dostarczono sprzęt w ilościach: 10 ekranów, 5 skanerów typ 1, 1 skaner typ 2, 5 czytników e-Dowodu oraz spełnia on minimalne parametry i gwarancje.
2. Dostarczono licencje w liczbie 16 i uruchomiono System w środowisku Zamawiającego bez dostępu do Internetu.
3. System działa w HA (jeżeli wdrażane) i integruje się z AD (oraz SSO Kerberos dla aplikacji Windows).
4. System umożliwia tworzenie formularzy z tła PDF, pola aktywne, wersjonowanie formularzy oraz obsługę dowolnych PDF.
5. System umożliwia podpis odręczny kontekstowy na ekranie, podpis biometryczny oraz podpis osobisty z e-Dowodu i podpisy kwalifikowane.
6. System umożliwia skanowanie, OCR bez limitów, dzielenie kompletów, wersje robocze i obsługę TWAIN.
7. Integracja z HIS AMMS spełnia zakres funkcji określony w OPZ (szablony, dane pacjenta, powiązania klas dokumentów, wybór urzędzeń, zapis dokumentu i wersjonowanie).
8. Zrealizowano szkolenia (min. zgodnie z harmonogramem) i przekazano dokumentację powdrożeniową.
9. Uruchomiono serwis i kanał zgłoszeń oraz potwierdzono parametry SLA.

12. Prawo weryfikacji rozwiązania

Zamawiający zastrzega prawo do wezwania Wykonawcy do prezentacji rozwiązania (całości lub części) w celu weryfikacji zgodności z OPZ (demo, środowisko testowe, dokumentacja techniczna). Brak wykazania zgodności może skutkować odrzuceniem oferty jako niezgodnej z OPZ.

13. Wymagane oświadczenia

Wraz z ofertą Wykonawca złoży oświadczenie producenta HIS AMMS potwierdzające, że integracja oferowanego Systemu z HIS AMMS spełnia wymagania funkcjonalne określone w OPZ (zakres integracji opisany w pkt 8).

2. System digitalizacji dokumentacji papierowej – 1 komplet

1. Przedmiot zamówienia

Przedmiotem zamówienia jest zakup, dostawa, wdrożenie oraz utrzymanie systemu digitalizacji dokumentacji papierowej, przeznaczonego do przetwarzania dokumentacji medycznej, wraz z integracją z funkcjonującym u Zamawiającego systemem HIS AMMS/EDM oraz zapewnieniem zgodności z krajowymi wymaganiami w zakresie Elektronicznej Dokumentacji Medycznej (EDM), w tym przekazywania danych do systemu P1 zgodnie ze standardem HL7 CDA.

Zakres zamówienia obejmuje w szczególności:

- dostarczenie licencji systemowych XSM wraz z modułem integracji z HIS AMMS/EDM,
- dostarczenie i konfigurację modułów podpisu elektronicznego,
- dostarczenie i konfigurację serwera skanowania,
- integrację z repozytorium EDM Zamawiającego,
- wdrożenie systemu w środowisku Zamawiającego,
- przeprowadzenie szkoleń dla użytkowników i administratorów,
- zapewnienie wsparcia serwisowego i utrzymaniowego w okresie trwałości projektu.

2. Cel realizacji zamówienia

Celem realizacji zamówienia jest zapewnienie Zamawiającemu narzędzia umożliwiającego:

- digitalizację (skanowanie) papierowej dokumentacji medycznej,
- indeksację zeskanowanych dokumentów w kontekście właściwego pacjenta,
- bezpieczne zdeponowanie dokumentacji w Repozytorium EDM,
- dostęp do zeskanowanej dokumentacji z poziomu systemu HIS,
- przekazywanie EDM do systemu P1 zgodnie z obowiązującymi wymaganiami technicznymi i prawnymi.

3. Zakres funkcjonalny systemu

3.1. Digitalizacja dokumentacji papierowej

System musi umożliwiać:

- skanowanie dokumentacji papierowej przy wykorzystaniu dedykowanego serwera skanowania,
- obsługę różnych formatów dokumentów medycznych,
- automatyczne lub półautomatyczne przypisywanie dokumentów do właściwego pacjenta.

3.2. Integracja z HIS AMMS/EDM

Integracja z systemem HIS AMMS/EDM polega na:

- wykorzystaniu istniejącego API integracyjnego HIS oraz Repozytorium EDM,
- zdeponowaniu zeskanowanej dokumentacji medycznej w Repozytorium EDM,
- zapewnieniu dostępu do zeskanowanych dokumentów z poziomu systemu HIS w kontekście właściwego pacjenta.

Produkt nie wymaga integracji wewnętrznych – opiera się wyłącznie na integracji zewnętrznej z systemem HIS/EDM.

3.3. Indeksacja i EDM

System musi umożliwiać:

- indeksację dokumentów zgodnie z wymaganiami EDM,
- generowanie i obsługę dokumentów zgodnych ze standardem HL7 CDA,
- przekazywanie dokumentacji do systemu P1.

3.4. Podpis elektroniczny

System musi zapewniać:

- obsługę podpisu elektronicznego (kwalifikowanego, zaufanego lub osobistego – zgodnie z obowiązującymi przepisami),
- możliwość podpisywania dokumentów przed ich zdeponowaniem w Repozytorium EDM.

4. Wymagania techniczne i organizacyjne

4.1. Warunki startowe

- System HIS AMMS oraz AMDX w wersji zgodnej z rekomendacją producenta na moment wdrożenia.
- Dostępna licencja: AMDX/CONFIG/REGISTER_INTEGRATED_SYSTEM (1 dodatkowe zdarzenie).

4.2. Wymagania techniczne

- Zapewniona poprawna komunikacja sieciowa pomiędzy serwerem/serwerami systemu digitalizacji (Xerrex/XSM) a usługami AMMS oraz AMDX.
- System musi działać w infrastrukturze Zamawiającego lub infrastrukturze wskazanej przez Zamawiającego.

4.3. Wymagania organizacyjne

- Przekazanie przez Zamawiającego informacji niezbędnych do połączenia systemu zewnętrznego z usługami integracyjnymi HIS/EDM.
- Dodanie nowego systemu domyślnego po stronie AMDX.
- Utworzenie i przypisanie użytkownika systemowego do integracji oraz przekazanie jego danych dostawcy systemu digitalizacji.

5. Wdrożenie systemu

Wdrożenie systemu musi obejmować co najmniej:

1. Dodanie i aktywację wymaganych licencji.
2. Konfigurację integracji po stronie AMDX (system domyślny, użytkownik systemowy).
3. Konfigurację systemu digitalizacji po stronie Wykonawcy.
4. Testy integracyjne i funkcjonalne.
5. Uruchomienie produkcyjne systemu.

6. Szkolenia

Wykonawca zapewni:

- szkolenia dla użytkowników końcowych (obsługa skanowania, indeksacji i dostępu do dokumentów),
- szkolenia dla administratorów systemu,
- materiały szkoleniowe w formie elektronicznej.

7. Kryteria odbioru

Za spełnienie przedmiotu zamówienia uznaje się w szczególności:

- możliwość skanowania i zapisu dokumentacji w Repozytorium EDM,
- dostęp do zeskanowanych dokumentów z poziomu systemu HIS w kontekście właściwego pacjenta,
- poprawne przekazywanie dokumentów EDM do systemu P1,
- pozytywne zakończenie testów integracyjnych i akceptacyjnych.

8. Wsparcie serwisowe i utrzymanie

Wykonawca zapewni wsparcie serwisowe systemu w okresie trwałości projektu, obejmujące:

- usuwanie błędów i awarii,

- aktualizacje systemu wynikające ze zmian przepisów lub wymagań technicznych (w tym P1),
- wsparcie techniczne dla administratorów Zamawiającego.

9. Postanowienia końcowe

System musi być zgodny z obowiązującymi przepisami prawa, w szczególności w zakresie ochrony danych osobowych oraz prowadzenia dokumentacji medycznej, a także z wytycznymi Centrum e-Zdrowia dotyczącymi EDM i systemu P1.

3. Urządzenia skanujące – 8 sztuk

3.1. Ogólny opis

Przedmiotem zamówienia jest dostawa sprzętu i wdrożenie systemu do automatycznej digitalizacji dokumentacji (dalej: System). System ma zapewniać możliwość skanowania zewnętrznej dokumentacji medycznej z opcją opatrzenia jej podpisem cyfrowym.

Zakup sprzętu służącego do digitalizacji dokumentacji papierowej obejmującej co najmniej kartę informacyjną z leczenia szpitalnego wraz z programami i systemami informatycznymi współpracującymi z nabywanymi sprzętami do digitalizacji. System powinien być zintegrowany z systemami posiadanymi przez Zamawiającego - HIS AMMS.

3.2. Zakres prac

W ramach zamówienia Wykonawca zobowiązany jest do:

1. Dostawy sprzętu umożliwiającego wykonanie funkcjonalności Systemu – skanery a4 (6 sztuk), skanery A3 (2 sztuki)
2. Dostawy 8 licencji na system do urządzeń skanujących w integracji z HIS AMMS.
3. Instalacji i wdrożenia systemu automatycznej digitalizacji dokumentacji wraz z integracją z posiadanym środowiskiem systemu Medycznego HIS AMMS w jednostce Zamawiającego.
4. Przeprowadzenia odpowiednich szkoleń w zakresie administrowania i użytkowania Systemu.
5. Świadczenia opieki serwisowej wraz z nadzorem autorskim dla wszystkich przekazywanych licencji na System przez okres 36 miesięcy od daty zakończenia wdrożenia.

3.3. Wymagania dotyczące sprzętu

a) Skaner A4 – 6 szt.

Typ skanera	Skaner z automatycznym podajnikiem dokumentów ADF
Tryb skanowania	Skanowanie dwustronne jednoprzebiegowe (duplex); kolor/skala szarości/monochromatyczny
Przeznaczenie urządzenia	Skanowanie dokumentów o różnych formatach i gramaturach bez konieczności ich wcześniejszej segregacji
Wbudowana pamięć RAM	minimum 2GB
Format skanowanych dokumentów	A4 i mniejsze
Ilość układów optycznych	2 - możliwość skanowania w trybie duplex z ADF
Element światłoczuły dla ADF	podwójny CIS
Prędkość skanowania dla 300 DPI tryb cz&b, skala szarości, kolor	minimum 30 arkuszy/min, minimum 60 obrazów/min
Rozdzielczość optyczna	600 DPI

Rozdzielczość wyjściowa	75-1200 DPI
Panel kontrolny	1.5 cala LED
Automatyczny podajnik dokumentów	80 arkuszy A4 o gramaturze 80g/m2
Tryb skanowania kopert	Skanowanie kopert A4 i mniejszych przy użyciu ADF za pomocą prostej ścieżki prowadzenia papieru
Poprawa jakości skanowanych dokumentów	Likwidacja przekosu, automatyczne rozpoznawanie wielkości i rozmiaru dokumentu, usuwanie kolorów; skanowanie dwustrumieniowe kolor i czarno-biały za jednym przebiegiem; interaktywna regulacja koloru, regulacja jasności i kontrastu, automatyczna rotacja dokumentu, automatyczne wykrywanie koloru, inteligentne wygładzanie koloru tła, inteligentne wypełnienie krawędzi obrazu, scalanie obrazów, wykrywanie pustych stron na podstawie procentowej zawartości oraz rozmiarze pliku, filtrowanie smug, filtr ostrości, usuwanie dziurek po dziurkaczu (okrągłe oraz prostokątne)
Format plik wyjściowego	tiff, jpg, bmp, pdf, pdf przeszukiwalny do j. polskiego, doc,xls oraz rtf do j. polskiego
Wsparcie dla sterowników	TWAIN oraz ISIS
Interfejs komunikacyjny z PC	USB 3.0 lub szybszy
Obciążenie dzienne	minimum 5 000 skanów
Maksymalna wspierana przez skaner długość dokumentu	2800 mm
Zakres gramatury skanowanych dokumentów dla ADF	od 34g/m2 do 413g/m2
Czujnik podwójnych pobrań dokumentów ultrasonnic	z regulacją czułości z poziomu sterownika TWAIN i ISIS
Wsparcie producenta dla skanowania kart	tak - do 1.4mm
Aplikacja do odczytu kodów kreskowych	tak
Wspierane systemy operacyjne dla sterowników TWAIN oraz ISIS	Windows 10, Windows 11, Windows Server 2019, Windows Server 2022, Linux Ubuntu 18.04 i wyższe
Gwarancja	36 miesięcy NBD
Wymiary zewnętrzne - rozłożony z tacami podawczymi i odbiorczymi	232x312x269mm
Waga	do 4,5kg
Pobór mocy	tryb pracy do 20W, do 0.3W w trybie czuwania
Ochrona środowiska	Oferowany sprzęt musi spełniać wymogi specyfikacji technicznej Energy Star 3.2 i posiadać oznaczenie znakiem usługowym ENERGY STAR lub spełniać kryteria efektywności energetycznej co najmniej równoważne z koniecznymi do uzyskania takiego oznaczenia. Zgodność z normą EPEAT Gold.

b) Skaner A3 – 2 szt.

Typ skanera	Skaner z automatycznym podajnikiem dokumentów ADF oraz możliwością późniejszej rozbudowy o dedykowany podajnik płaski formatu A3 (tego samego producenta).
Tryb skanowania	Skanowanie dwustronne jednoprzebiegowe (duplex); kolor/skala szarości/monochromatyczny
Przeznaczenie urządzenia	Skanowanie dokumentów o różnych formatach i gramaturach bez konieczności ich wcześniejszej segregacji, skanowanie dokumentów długich
Format skanowanych dokumentów	A3 i mniejsze
Ilość układów optycznych	2 - możliwość skanowania w trybie duplex z ADF
Element światłoczuły dla ADF	2x CIS
Typ oświetlenia	LED
Prędkość skanowania ADF dla 300DPI tryb cz&b, kolor i skala szarości	60 arkuszy/min, 120 obrazów/min
Rozdzielczość optyczna	600 DPI
Rozdzielczość wyjściowa dla ADF	100-1200 DPI
Panel kontrolny	3.5 cala kolorowy dotykowy ekran LCD z możliwością predefiniowania profili skanowania i uruchamiania ich z poziomu skanera wraz z możliwością indywidualnego opisu zadań w języku polskim. Interfejs użytkownika i wyświetlane komunikaty muszą być w języku polskim.
Automatyczny podajnik dokumentów	z pobieraniem arkuszy od góry, regulowany min. w 3 stopniach na 300 arkuszy o gramaturze 80g/m ²
Tryb skanowania kopert	skanowanie kopert i grubych dokumentów A3 przy użyciu ADF za pomocą prostej ścieżki prowadzenia papieru
Funkcje poprawy jakości skanowanych dokumentów dostępne z poziomu sterownika TWAIN jak i ISIS	Likwidacja przekosu, automatyczne rozpoznawanie wielkości i rozmiaru dokumentu, usuwanie kolorów; skanowanie dwustrumieniowe kolor i czarno-biały za jednym przebiegiem; interaktywna regulacja koloru, regulacja jasności i kontrastu, automatyczna rotacja dokumentu, automatyczne wykrywanie koloru, inteligentne wygładzanie koloru tła, inteligentne wypełnienie krawędzi obrazu, scalanie obrazów, wykrywanie pustych stron na podstawie możliwego do zdefiniowania konkretnego procentowego stopnia zaczernienia strony, wykrywanie pustych stron na podstawie definiowalnego rozmiaru pliku, filtrowanie smug, filtr ostrości, układanie dokumentów na tacy wyjściowej,
Format pliku wyjściowego	Tiff, jpg, bmp, pdf, pdf/A, pdf przeszukiwalny do j. polskiego, rtf do j. polskiego, xml z wartością odczytanego kodu kreskowego
Format pliku indeksowego	Możliwość generowania pliku xml lub csv - zawierającego informację na temat wartości odczytanego kodu kreskowego np.: Interleaved 2 of 5, Code 3 of 9, Code 128, Codabar, UPC-A, UPC-E, EAN-13, EAN-8, PDF417, QR code.

Skanowanie zgodne z FADGI	TAK - skaner musi mieć możliwość wybrania trybu skanowania zgodnego z FADGI (Federal Agencies Digital Guidelines Initiative). Przełącznik trybu FADGI musi być dostępny z poziomu dotykowego panelu sterowania w skanerze.
Wsparcie dla sterowników	TWAIN, ISIS oraz Linux
Interfejs komunikacyjny z PC	USB 3.2 lub szybszy, LAN 10/100/1000 wbudowany w urządzenie
Obciążenie dzienne	25 000 skanów
Maksymalna wspierana przez skaner długość dokumentu	4000 mm
Zakres gramatury skanowanych dokumentów dla ADF	34–433 g/m ²
Czujnik podwójnych pobrań dokumentów	ultrasonik z interaktywnym przywracaniem wykrycia wielu arkuszy
Ochrona dokumentów przed zgnieceniem za pomocą czujnika akustycznego	tak - z regulacją czułości z poziomu sterownika
Wspierane systemy operacyjne dla sterowników TWAIN oraz ISIS	Windows 7 SP1 (wersja 32-bitowa i 64-bitowa), Windows 8 (wersja 32-bitowa i 64-bitowa), Windows 8.1 (wersja 32-bitowa i 64-bitowa), Windows 10 (wersja 32-bitowa i 64-bitowa), Windows Server 2012 x64, Windows Server 2016 x64, Linux Ubuntu 18.04
Moduł nadruku (post printer)	możliwość zainstalowania modułu nadruku generującego druk (np.data, liczba skanów) na dokumencie
Odczyt kodów kreskowych	przeplatany 2 z 5, kod 3 z 9, kod 128, Codabar, UPC-A, UPC-E, EAN-13, EAN-8, PDF417, QR
Gwarancja	12 miesięcy
Waga	do 18kg
Pobór mocy	tryb pracy <50W, tryb uśpienia <4W, tryb czytania <0.3W
Deklaracja zgodności	CE
Ochrona Środowiska	Energy Star, EPEAT, ROHS.
Wymagane oświadczenia do złożenia wraz z ofertą	Oświadczenie producenta, że w przypadku nie wywiązania się z obowiązków gwarancyjnych oferenta przejmie na siebie wszelkie zobowiązania związane z serwisem urządzeń. Oświadczenie potwierdzające pochodzenie oferowanego sprzętu z oficjalnego polskiego kanału dystrybucji, podpisane przez producenta. Serwis gwarancyjny oraz konserwacja urządzeń musi być świadczona przez organizację serwisową producenta lub certyfikowanego przez niego do świadczenia usług serwisowych jego przedstawiciela na rynku polskim, posiadającego swoją placówkę serwisową na terenie Polski. Dokumenty potwierdzające spełnienie ww. należy dołączyć do oferty.

3.4. Minimalne warunki licencji na system

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:

- a. wprowadzanie do pamięci komputera,
 - b. korzystanie,
 - c. sporządzanie kopii zapasowej,
 - d. przenoszenie pomiędzy stanowiskami.
2. Zamawiający w ramach udzielonej licencji uprawniony będzie do korzystania z wygenerowanych za pomocą danego rozwiązania dokumentów (np. raportów, analiz) w szczególności poprzez:
- a. opracowanie, w tym zmianę, adaptację, tłumaczenie,
 - b. 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,
 - c. publiczne rozpowszechnianie, w tym: wyświetlanie, odtwarzanie w dowolnym systemie lub standardzie, a także publiczne udostępnianie w taki sposób, aby każdy mógł mieć do nich dostęp w miejscu i czasie przez siebie wybranym,
 - d. wprowadzanie do sieci multimedialnych oraz Internetu,
 - e. umieszczanie w publikacjach drukowanych (w tym m.in. ulotki, foldery, plakaty),
 - f. umieszczanie w publikacjach elektronicznych oraz aplikacjach elektronicznych,
 - g. umieszczanie w prezentacjach i materiałach prasowych,
 - h. umieszczania w spotach i filmach reklamowych.
3. Licencja, o której mowa w ust. 1 i 2 uprawnia Zamawiającego do korzystania z rozwiązania na terytorium Rzeczypospolitej Polskiej.
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, zleceńbiorców oraz innych osób współpracujących z Zamawiającym.
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.
6. Wykonawca składając ofertę oświadcza, iż:
- a. 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
 - b. 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
 - c. udzielenie licencji zgodnie z ofertą, jak również korzystanie przez Zamawiającego z przedmiotów własności intelektualnej zaoferowanych przez Wykonawcę nie będzie stanowić naruszenia praw osób trzecich.

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

3.5. Licencja integracyjna HIS

1. Wykonawca składając ofertę oświadcza, iż w zakresie integracji oferowanego Systemu z systemem HIS Zamawiającego:
 - a. 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
 - b. 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
 - c. udzielenie licencji zgodnie z ofertą, jak również korzystanie przez Zamawiającego z przedmiotów własności intelektualnej zaoferowanych przez Wykonawcę nie będzie stanowić naruszenia praw osób trzecich.
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.
3. Po upływie 36 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.
4. Zamawiający podkreśla, iż nie dysponuje kodami źródłowymi do systemu HIS Zamawiającego. Wykonawca w ramach realizacji prac zobowiązany będzie do samodzielnego kontaktu z dostawcą HIS Zamawiającego i zapewnienia wykonania wszelkich prac integracyjnych zarówno od strony dostarczanego Systemu, jak i dostawcy HIS.

3.6. Wdrożenie i szkolenia

1. W ramach realizacji przedmiotu zamówienia, Wykonawca zobowiązany jest do przeprowadzenia wdrożenia systemu w następującym zakresie:
 - a) modyfikacja oprogramowania na maszynie wirtualnej w infrastrukturze sieciowej Zamawiającego;
 - b) rozmieszczenie dostarczanych sprzętów na stanowiskach roboczych wskazanych przez Zamawiającego;
 - c) 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;
 - d) konfiguracja i parametryzacja dostarczonego oprogramowania do współpracy z dostarczonym sprzętem;
 - e) w porozumieniu z dostawcą systemu dzierżynowego HIS uruchomienie integracji między systemem HIS a dostarczanym systemem;

- f) przekazanie Zamawiającemu zestawu zmiennych i parametrów wymaganych do poprawnego działania integracji między systemem HIS a dostarczanym systemem;
- g) przeprowadzenie szkoleń z zakresu działania systemu dla użytkowników systemu (personelu medycznego);
- h) przeprowadzenie szkoleń z zakresu administrowania infrastrukturą i konfiguracją systemu dla administratorów szpitala;
- i) dostarczenie dokumentacji powdrożeniowej.

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.

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 20 osób; dokładna liczba osób do przeszkolenia zostanie przekazana Wykonawcy w terminie do 10 dni od zawarcia umowy.

a) Wykonawca jest zobowiązany do umożliwienia każdemu uczestnikowi szkolenia aktywnego uczestnictwa w szkoleniu polegającego na indywidualnym przejściu całego procesu związanego z zeskanowaniem i zapisaniem dokumentu w systemie.

b) Wykonawca jest zobowiązany do uzyskania i udostępnienia Zamawiającemu potwierdzenia uczestnictwa od każdego z uczestników szkoleń.

c) Wykonawca jest zobowiązany przedstawić Zamawiającemu propozycję szczegółowego harmonogramu szkoleń nie później niż na 3 dni robocze przed planowanym rozpoczęciem szkoleń.

d) 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.

e) 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.

f) Wykonawca przekaze Zamawiającemu materiały instruktażowe w postaci filmów instruktażowych lub instrukcji stanowiskowych, umożliwiających wykonanie samodzielnego szkolenia dla personelu szpitala.

g) 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.

4. Wykonawca przekaze Zamawiającemu Dokumentację powdrożeniową po zakończeniu wszystkich prac wdrożeniowych aktualną na dzień odbioru końcowego. Dokumentacja powdrożeniowa ma obejmować:

- a) raport z wykonanych prac wdrożeniowych
- b) zestawienie personelu uczestniczącego w szkoleniach
- c) instrukcję obsługi systemu
- d) wykaz zmiennych i parametrów ustawionych dla systemu
- e) informacje na temat dostępnego sposobu zgłaszania awarii i usterek w działaniu systemu
- f) wykaz procedur wymaganych dla poprawnego działania systemu, które administrator systemu szpitalnego ma przeprowadzać na serwerze i dostarczonym systemie

3.7. Integracja systemu z działającym w placówce systemem HIS AMMS

1. W ramach realizacji przedmiotu zamówienia Wykonawca zobowiązany jest w porozumieniu z dostawcą systemu HIS AMMS do przeprowadzenia modyfikacji systemu w szczególności polegających na:
 - a) 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
 - b) umożliwieniu przestania zeskanowanego dokumentu pod konkretnego pacjenta, bez konieczności otwierania systemu HIS
 - c) 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

3.8. Opieka nad systemem

W ramach opieki serwisowej nad Systemem Wykonawca w okresie 36 miesięcy świadczyć będzie następujące usługi/ wykonywać będzie następujące prace:

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

3.9. Wymagania dla oprogramowania

1. Ogólne – System do digitalizacji (dalej: System)

- a. System musi umożliwiać pracę w odizolowanym środowisku na infrastrukturze Zamawiającego, bez dostępu do Internetu lub jakichkolwiek połączeń sieciowych poza infrastrukturę teleinformatyczną Zamawiającego
- b. System musi umożliwiać działanie na lokalnej bazie danych dostępnej w modelu open-source - bez kosztów licencji.
- c. System musi umożliwiać uruchomienie w lokalnym klastrze wysokiej dostępności w celu zapewnienia działania Systemu w przypadku awarii części infrastruktury.
- d. System musi umożliwiać integrację do lokalnej domeny Active Directory Zamawiającego w celu uniknięcia tworzenia nowych kont dla użytkowników końcowych. Ponadto dla aplikacji uruchamianych przez użytkownika końcowego na komputerach z systemem operacyjnym Windows, niezbędna jest możliwość logowania jednokrotnego (SSO) za pośrednictwem wykorzystywanego protokołu Kerberos.
- e. 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).
- f. System musi posiadać Aplikację Centralną, dostępną z poziomu przeglądarki Internetowej, wymagającą logowania na konto użytkownika.
- g. System ma umożliwiać implementację nowych formularzy do Systemu poprzez import do aplikacji edytora (będącej elementem Systemu) tła dokumentu w postaci PDF (tzn. obrazu niezmienniej 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).
- h. System musi umożliwiać obsługę innych plików PDF niezdefiniowanych wcześniej w Systemie.
- i. 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.
- j. Repozytorium dokumentów:
 - System musi posiadać wbudowane mechanizmy zapisywania, przechowywania i katalogowania dokumentów w ramach Systemu,
 - System musi umożliwiać samodzielne tworzenie, usuwanie i zmianę nazwy katalogów i podkatalogów możliwych do przeglądania z poziomu Aplikacji Centralnej.
 - System musi umożliwiać przenoszenie dokumentów pomiędzy katalogami oraz definiowanie domyślnych katalogów zapisu dokumentów.

- 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.
- k. 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.
- l. System musi umożliwiać śledzenie statusu podpisywania poszczególnych dokumentów.
- m. System musi umożliwiać nakładanie w polach podpisu pieczętek konfigurowalnych w Systemie.
- n. System musi udostępniać panel administracyjny dostępny z poziomu Aplikacji Centralnej.
- o. System musi umożliwiać tworzenie kont użytkowników i zarządzanie nimi z poziomu panelu administracyjnego.
- p. System musi umożliwiać nadawanie użytkownikom uprawnień w celu minimalizacji dostępu dla różnych grup użytkowników.
- q. Monitoring pracy systemu
 - System musi zbierać logi audytowe w celu prześledzenia działań związanych z określonym dokumentem, użytkownikiem, urządzeniem itp. Musi istnieć możliwość konfiguracji odrębnej polityki retencji danych typu audytowego.
 - Zamawiający wymaga, aby system umożliwiał monitorowanie wydajności systemów, aplikacji itp. w czasie rzeczywistym, z dostępem do danych na żywo bez opóźnień.
 - System musi zbierać metryki dotyczące wykorzystania CPU, pamięci RAM, przestrzeni dyskowej oraz sieci, zarówno z Systemu, bez konieczności specjalistycznej konfiguracji.
 - Zamawiający wymaga centralizacji logów z różnych źródeł (serwery, aplikacje, integracje itp.) w jednym miejscu, umożliwiając łatwe przeszukiwanie i analizowanie tych danych.
 - Konieczne jest posiadanie łatwego w użyciu narzędzia do tworzenia wizualizacji (dashboardów) metryk i logów, które można dostosować do potrzeb Zamawiającego bez konieczności wsparcia zewnętrznego.
 - Wymagamy, aby system umożliwiał samodzielną konfigurację alertów w oparciu o ustalone progi i metryki. Powiadomienia muszą być dostarczane na różne kanały, a cała konfiguracja powinna być dostępna bez interwencji dostawcy.
 - System musi umożliwiać konfigurację retencji danych, umożliwiającą konfigurację okresu przechowywania metryk i logów.
 - System musi wspierać monitorowanie działania i zbieranie metryk niezależnie od sposobu uruchomienia (klaster, jedna instancja).
 - Zamawiający wymaga, aby system zapewniał mechanizmy zabezpieczeń dostępu do logów i metryk.

- Możliwość tworzenia raportów i eksportu danych – Konieczność generowania raportów na podstawie zebranych metryk i logów oraz eksportu tych danych do innych systemów.

r. Integracje

- System musi umożliwiać otwartą integrację z systemami zewnętrznymi za pomocą API w technologii REST.
- System umożliwia wystanie 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.
- 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.
- System musi umożliwiać cofnięcie autoryzacji dla danej integracji w celu zabezpieczenia przed wyciekiem.
- System musi posiadać funkcjonalność ustawiania automatycznych powiadomień o podpisaniu dokumentu na wskazany webservice w celu umożliwienia integracji bez konieczności wykonania prac po stronie Wykonawcy.

s. Podpisy:

- 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.
- 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.
- System powinien umożliwiać opatrzenie dokumentów elektronicznym podpisem odręcznym (biometrycznym). System powinien gromadzić informacje takie jak siła nacisku czy znaczniki czasowe umożliwiające weryfikację autentyczności podpisu.
- System niezależnie powinien umożliwiać opatrzenie dokumentów podpisem osobistym z e-Dowodu.
- System musi posiadać moduł podpisu elektronicznego umożliwiający opatrzenie dokumentu (co najmniej PDF) za pomocą podpisu osobistego w e-dowodzie oraz podpisów kwalifikowanych różnych dostawców dostępnych na polskim rynku.

2. Wymagania związane z urządzeniami

a. Skaner

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

- 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.
- System musi umożliwiać pobieranie bezpośrednio z dokumentu danych opisujących dokument
- System musi umożliwiać regulację stopnia kompresji plików.
- System musi umożliwiać przed rozpoczęciem skanowania ustawienie dzielenia skanowanych dokumentów co wybraną liczbę stron.
- System musi posiadać funkcjonalność optycznego rozpoznawania znaków (OCR) bez limitów rozpoznawanych dokumentów.
- System musi umożliwiać automatyczne uzupełnianie kolejnych danych w polach dokumentu na podstawie takich samych danych wcześniej poprawnie wprowadzonych w szablonie.
- System musi mieć funkcję dzielenia kompletów dokumentów skanowanych seryjnie z automatycznego podajnika dokumentów urządzenia skanującego.
- System musi posiadać wbudowaną wyszukiwarkę dokumentów.
- System musi umożliwiać weryfikację poprawności rozpoznanych lub wprowadzonych danych przed ich zatwierdzeniem.
- System musi wymagać uwierzytelnienia (zalogowania) użytkownika.
- System musi umożliwiać zapisywanie wersji roboczych nieprzetworzonych dokumentów zeskanowanych w celu powrotu do pracy nad nimi po uruchomieniu kolejnej sesji.
- 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 przestania go do systemu.
- System musi posiadać funkcjonalność dzielenia dokumentów według szablonów i automatycznego dołączania do nich dowolnej ilości stron niebędących szablonami.
- System musi umożliwiać ustawienie domyślnego szablonu skanowania, który będzie automatycznie wskazywany w sytuacji, gdy nie będzie możliwe rozpoznanie szablonu dla skanowanego dokumentu.
- System musi umożliwiać współpracę z urządzeniami skanującymi działającymi za pośrednictwem protokołu TWAIN.
- 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

3.10. 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

4. Nowe funkcjonalności systemu HIS w zakresie integracji z platformą P1

4.1. Integracja z Rejestrem Endoprotezoplastyki

1. Przedmiot zamówienia

Przedmiotem zamówienia jest dostawa, konfiguracja, uruchomienie oraz integracja modułu Ankieta Endoprotezoplastyki – pełnej w systemie HIS, wraz z zapewnieniem komunikacji z zewnętrznym systemem Rejestr Endoprotezoplastyki (RE) prowadzonym przez Narodowy Fundusz Zdrowia, a także przeprowadzenie testów odbiorowych i przygotowanie produktu do eksploatacji produkcyjnej.

2. Wymagania funkcjonalne

2.1. Ewidencja Ankiety endoprotezoplastyki – pełnej

1. System musi umożliwiać tworzenie, edycję i przegląd Ankiety endoprotezoplastyki – pełnej.
2. System musi obsługiwać trzy rodzaje Ankiety pełnej:
 - o rozliczeniową,
 - o rozliczeniową – inna grupa JGP,
 - o statystyczną.
3. System musi umożliwiać zbiorczy przegląd Ankiety endoprotezoplastyki z poziomu:
 - o modułu Oddział HIS,
 - o modułu Statystyka RCH HIS.

2.2. Automatyzacja i podpowiadanie danych

1. System musi zapewniać automatyczne kopiowanie danych w ramach jednego pobytu pacjenta, w szczególności:
 - o leków stale przyjmowanych,
 - o leków podanych,
 - o leków wystawionych na recepcie,
 - o zaleceń lekarskich,
 - o skierowań na rehabilitację.
2. System musi podpowiadać w Ankiecie endoprotezoplastyki dane dotyczące:
 - o poprzedniego i następnego pobytu pacjenta,
 - o parametrów jednostkowych pacjenta (waga, wzrost, BMI),
 - o daty operacji oraz operatora,
 - o daty operacji pierwotnej i miejsca jej wykonania.

2.3. Autoryzacja i podpis

1. System musi umożliwiać autoryzację danych Ankiety endoprotezoplastyki.
2. System musi zapewniać podpisanie Ankiety w postaci elektronicznej, zgodnie z konfiguracją parametru systemowego rodzaju podpisu.

3. Integracja z Rejestrem Endoprotezoplastyki (RE)

3.1. Komunikacja zewnętrzna

1. System musi zapewniać dwukierunkową komunikację z systemem Rejestr Endoprotezoplastyki (RE).
2. Komunikacja musi odbywać się:
 - o poprzez API SOAP,
 - o za pośrednictwem Platformy Integracyjnej HIS – moduł ENDO.
3. Dane Ankiety muszą być przekazywane w formacie XML, zgodnie z usługami udostępnionymi przez NFZ.

3.2. Funkcje komunikacyjne

System musi umożliwiać:

1. Logowanie do systemu RE w celu uwierzytelnienia i autoryzacji.
2. Wysyłkę Ankiety endoprotezoplastyki – pełnej:
 - w wersji roboczej,
 - w wersji oficjalnej.
3. Wysyłkę korekty Ankiety endoprotezoplastyki – pełnej.
4. Anulowanie wersji roboczej Ankiety endoprotezoplastyki – pełnej w RE.
5. Obsługę i prezentację komunikatów błędów zwracanych przez system RE.
6. Import słowników z systemu RE.

4. Zależności między modułami HIS

1. Funkcjonalność Ankiety endoprotezoplastyki musi korzystać z danych hospitalizacji pacjenta dostępnych w modułach:
 - Izba Przyjęć HIS,
 - Oddział HIS,w zakresie m.in.: skierowań, trybu przyjęcia, wyników badań, podań leków, recept, zaleceń lekarskich i skierowań na rehabilitację.
2. Funkcjonalność musi korzystać z danych dotyczących zabiegu endoprotezoplastyki rejestrowanych w modułach:
 - Blok Operacyjny HIS,
 - Oddział HIS.
3. Konfiguracja komunikacji z systemem RE musi być realizowana z poziomu Panelu Administracyjnego HIS.

5. Kryteria odbioru produktu

Produkt zostanie uznany za zgodny z OPZ, jeżeli spełni łącznie następujące kryteria:

1. Umożliwia tworzenie i edycję Ankiety endoprotezoplastyki – pełnej w trzech wymaganych rodzajach.
2. Zapewnia kopiowanie leków, zaleceń oraz skierowań w ramach pobytu pacjenta.
3. Zapewnia podpowiadanie danych historycznych i klinicznych pacjenta.
4. Umożliwia autoryzację i podpis elektroniczny Ankiety.
5. Zapewnia poprawną komunikację z systemem RE.
6. Umożliwia wysyłkę Ankiety w wersji roboczej i oficjalnej.
7. Poprawnie prezentuje statusy i komunikaty zwrotne z RE.
8. Umożliwia wysyłkę korekty Ankiety.
9. Umożliwia anulowanie wersji roboczej Ankiety w RE.
10. Obsługuje import słowników z RE.
11. Umożliwia zbiorczy przegląd Ankiet endoprotezoplastyki.

6. Wymagania do uruchomienia produktu

6.1. Warunki startowe

1. Dostępna i aktywna licencja: ANKIETA_ENDO.
2. Działająca i poprawnie skonfigurowana komunikacja z NFZ.
3. Prawidłowo skonfigurowane logowanie do NFZ (systemowe i użytkowników).
4. Zaimportowane aktualne słowniki z systemu RE.

6.2. Wymagania techniczne

1. Zainstalowana Platforma Integracyjna HIS – moduł ENDO.

6.3. Wymagania organizacyjne

1. Jednostka posiada aktywną umowę z NFZ na realizację świadczeń w zakresie endoprotez stawowych.
2. Nadane uprawnienia operatorom:
 - o w Portalu SZOI / Portalu Świadczeniodawcy,
 - o w systemie KAAS-MGR-SYS do systemu RE.
3. Nadane w systemie HIS uprawnienia do Ankiety endoprotezoplastyki:
 - o Odczyt,
 - o Wpis,
 - o Autoryzacja,
 - o Modyfikacja.

7. Zakres wdrożenia i konfiguracji

W ramach realizacji zamówienia Wykonawca zobowiązany jest do:

1. Instalacji Platformy Integracyjnej – usługi ENDO oraz przetęczenia adresów na środowisko produkcyjne.
2. Wgrania licencji ANKIETA_ENDO.
3. Weryfikacji konfiguracji komunikacji z NFZ.
4. Weryfikacji i konfiguracji logowania do NFZ (systemowej i użytkowników).
5. Importu słowników z systemu RE.
6. Nadania i weryfikacji uprawnień użytkowników.
7. Konfiguracji parametrów systemowych, w tym:
 - o SzynaIntegr\AdresPI,
 - o AE\RODZAJ_PODPISU.
8. Konfiguracji dokumentacji medycznej związanej z Ankietą endoprotezoplastyki.

4.2. Ankieta Udarowa

1. Przedmiot zamówienia

Przedmiotem zamówienia jest dostawa, konfiguracja, uruchomienie oraz integracja modułu Ankieta Udarowa w systemie HIS AMMS, obejmującego ewidencję danych klinicznych pacjentów z udarem mózgu oraz zapewnienie komunikacji z zewnętrznym systemem Ankiety Medyczne (AM) prowadzonym przez Narodowy Fundusz Zdrowia, wraz z przeprowadzeniem testów odbiorowych i przygotowaniem rozwiązania do eksploatacji produkcyjnej.

2. Wymagania funkcjonalne

2.1. Ewidencja Ankiety udarowej

1. System musi zapewniać tworzenie, edycję oraz przegląd Ankiety udarowej.
2. System musi obsługiwać cztery modele prowadzenia Ankiety udarowej:
 - o z trombektomią mechaniczną,
 - o bez trombektomii,
 - o z przekazaniem pacjenta na trombektomię,
 - o ze skierowaniem na trombektomię przez inny szpital.
3. System musi umożliwiać zbiorczy przegląd Ankiety udarowych z poziomu:
 - o modułu Oddział HIS,
 - o modułu Statystyka RCH HIS.

2.2. Automatyczne podpowiadanie danych

1. System musi zapewniać automatyczne podpowiadanie danych klinicznych i organizacyjnych w Ankiecie udarowej, w szczególności:
 - danych dotyczących przybycia pacjenta do szpitala,
 - badań diagnostycznych mózgu,
 - zastosowanego leczenia,
 - danych trombektomii mechanicznej,
 - dat rozpoczęcia rehabilitacji,
 - danych wypisowych, w tym informacji o zgonie.
2. Dane muszą pochodzić z właściwych modułów HIS i być prezentowane w sposób umożliwiający ich weryfikację oraz edycję.

2.3. Autoryzacja i podpis

1. System musi umożliwiać autoryzację danych Ankiety udarowej.
2. System musi zapewniać podpisanie Ankiety udarowej w postaci elektronicznej, zgodnie z parametrami konfiguracyjnymi systemu.

3. Integracja z systemem Ankiety Medyczne (AM)

3.1. Komunikacja zewnętrzna

1. System musi zapewniać dwukierunkową komunikację z systemem Ankiety Medyczne (AM).
2. Komunikacja musi być realizowana:
 - poprzez API SOAP,
 - za pośrednictwem Platformy Integracyjnej HIS – moduł RAUT.
3. Zawartość Ankiety udarowej musi być przekazywana w formacie XML, zgodnie z usługami udostępnionymi przez NFZ.

3.2. Funkcjonalności komunikacyjne

System musi umożliwiać:

1. Logowanie do systemu AM w celu uwierzytelnienia i autoryzacji.
2. Wysyłkę Ankiety udarowej:
 - w wersji roboczej,
 - w wersji oficjalnej.
3. Obsługę i prezentację komunikatów błędów zwracanych przez system AM.
4. Wysyłkę korekty Ankiety udarowej.
5. Anulowanie Ankiety udarowej w systemie AM.
6. Bezpośrednie wywołanie (przejsię) do Ankiety udarowej z systemu HIS w systemie AM.

4. Zależności między modułami HIS

1. Funkcjonalność Ankiety udarowej musi korzystać z danych hospitalizacji pacjenta wprowadzonych w modułach:
 - Izba Przyjęć HIS,
 - Oddział HIS,w szczególności w zakresie: skierowania, trybu przyjęcia, rozpoznań, badań diagnostycznych, leczenia, rehabilitacji oraz danych wypisowych w przypadku zgonu.
2. Funkcjonalność musi korzystać z danych dotyczących zabiegu trombektomii mechanicznej, rejestrowanych w modułach:
 - Blok Operacyjny HIS,
 - Oddział HIS.

3. Konfiguracja komunikacji z systemem AM musi być realizowana z poziomu Panelu Administracyjnego HIS.

5. Kryteria odbioru produktu

Produkt zostanie uznany za zgodny z OPZ, jeżeli spełni łącznie następujące kryteria:

1. Umożliwia tworzenie i edycję Ankiety udarowej w czterech wymaganych modelach obsługi.
2. Zapewnia automatyczne podpowiadanie danych klinicznych i organizacyjnych.
3. Umożliwia autoryzację i podpis elektroniczny Ankiety udarowej.
4. Zapewnia poprawną komunikację z systemem Ankiety Medyczne (AM).
5. Umożliwia wysyłkę Ankiety w wersji roboczej i oficjalnej.
6. Poprawnie prezentuje statusy i komunikaty zwrotne z systemu AM.
7. Umożliwia wysyłkę korekty Ankiety.
8. Umożliwia anulowanie Ankiety udarowej.
9. Umożliwia podgląd danych zabiegu trombektomii mechanicznej zarejestrowanego w Bloku Operacyjnym.
10. Umożliwia bezpośrednie przejście do Ankiety w systemie AM.
11. Umożliwia zbiorczy przegląd Ankiety udarowych.

6. Wymagania do uruchomienia produktu

6.1. Warunki startowe

1. Dostępna i aktywna licencja: ANKIETA_UDAR.
2. Działająca komunikacja z NFZ.
3. Prawidłowo skonfigurowane logowanie do NFZ (systemowe i użytkowników).

6.2. Wymagania techniczne

1. Zainstalowana Platforma Integracyjna HIS – moduł RAUT.

6.3. Wymagania organizacyjne

1. Jednostka lecznicza musi:
 - o posiadać aktywną umowę z NFZ w rodzaju leczenie szpitalne lub w ramach PSZ,
 - o wykonywać zabiegi trombektomii mechanicznej.
2. Nadane uprawnienia operatorom:
 - o w Portalu SZOI / Portalu Świadczeniodawcy,
 - o w systemie centralnym KAAS-MGR-SYS do systemu AM.
3. Nadane w systemie AMMS uprawnienia do Ankiety udarowej:
 - o Odczyt,
 - o Wpis,
 - o Autoryzacja,
 - o Modyfikacja.

7. Zakres wdrożenia i konfiguracji

W ramach realizacji zamówienia Wykonawca zobowiązany jest do:

1. Instalacji Platformy Integracyjnej – usługi RAUT oraz przełączenia adresów na środowisko produkcyjne.
2. Wgrania licencji ANKIETA_UDAR.
3. Weryfikacji konfiguracji komunikacji z NFZ.
4. Weryfikacji i konfiguracji logowania do NFZ (systemowej i użytkowników).
5. Weryfikacji konfiguracji JOS.
6. Nadania i weryfikacji uprawnień użytkowników.
7. Konfiguracji parametrów systemowych, w tym:

- SzynaIntegr\AdresPI,
- ANK_UDAR\PROC\,
- AU\RODZAJ_PODPISU.

8. Konfiguracji dokumentacji medycznej związanej z Ankieta udarową.

4.3. Integracja z CeZ w zakresie digitalizacji karty leczenia - Ucyfrowienie + indeksacja

1. Przedmiot zamówienia

Przedmiotem zamówienia jest wdrożenie i uruchomienie funkcjonalności wspierających indeksowanie zdigitalizowanej dokumentacji medycznej w Platformie P1, w szczególności kart informacyjnych, wraz z mechanizmami:

- monitorowania poziomu indeksacji,
- reindeksacji dokumentów,
- obsługi błędów indeksacji,
- generowania dokumentów elektronicznych PIK HL7 CDA na podstawie dokumentów zeskanowanych,
- integracji z repozytorium EDM oraz Platformą P1.

Rozwiązanie musi działać w środowisku HIS Zamawiającego, zintegrowanym z repozytorium EDM oraz komponentem komunikacyjnym P1.

2. Zakres funkcjonalny zamówienia

2.1. Monitorowanie indeksacji dokumentów

1. System musi umożliwiać monitorowanie poziomu zaindeksowania dokumentów (kart informacyjnych), w tym:
 - dokumentów przekazanych do centralnego repozytorium Centrum e-Zdrowia,
 - dokumentów zdigitalizowanych z papierowej dokumentacji medycznej.
2. Monitorowanie musi być możliwe:
 - w podziale na jednostki organizacyjne,
 - z dokładnością miesięczną,
 - na poziomie kierowników poszczególnych jednostek organizacyjnych.
3. System musi prezentować wskaźniki indeksacji oraz zestawienia liczby dokumentów:
 - poprawnie zaindeksowanych,
 - oczekujących na indeksację,
 - z błędami indeksacji.

2.2. Reindeksacja i obsługa błędów

1. System musi umożliwiać:
 - ponowną wysyłkę indeksów do P1,
 - przegląd błędów indeksacji z poziomu graficznego interfejsu użytkownika HIS.
2. Reindeksacja musi być dostępna:
 - z poziomu GUI HIS,
 - bezpośrednio z ekranu dokumentacji medycznej w danych pobytu pacjenta,
 - w trybie synchronicznym (na żądanie użytkownika).
3. System musi umożliwiać wymuszenie reindeksacji z poziomu GUI repozytorium EDM.
4. System musi umożliwiać:
 - przebudowę indeksu dokumentu,

- ponowną wysyłkę indeksu do P1 bez konieczności tworzenia i podpisywania nowej wersji dokumentu, w przypadku braku identyfikatora Zdarzenia Medycznego (ID ZM).

2.3. Automatyczna reindeksacja

1. System musi realizować automatyczną reindeksację dokumentów, dla których ustala przyczyna braku możliwości indeksacji, np.:
 - opóźnione przekazanie Zdarzenia Medycznego.
2. Proces automatycznej reindeksacji:
 - działa w tle,
 - opiera się na dostarczonej konfiguracji,
 - nie wymaga interwencji użytkownika.

2.4. Tworzenie dokumentów elektronicznych

1. System musi umożliwiać tworzenie dokumentów elektronicznych zgodnych z szablonem PIK HL7 CDA:
 - na podstawie dokumentów zeskanowanych,
 - zarejestrowanych wcześniej w systemie jako dokumenty papierowe.
2. Utworzone dokumenty muszą być:
 - utrwalane w repozytorium EDM,
 - gotowe do indeksacji w Platformie P1.

2.5. Poświadczenie zgodności dokumentów

1. System musi umożliwiać poświadczenie zgodności dokumentu zdigitalizowanego z oryginałem poprzez:
 - złożenie podpisu elektronicznego.
2. Informacja o podpisie musi być zapisana w repozytorium EDM i uwzględniona w procesie indeksacji.

2.6. Integracja z Platformą P1

1. Rozwiązanie musi być zintegrowane z Platformą P1 zgodnie z udostępnioną specyfikacją usług:
 - w zakresie obsługi dokumentów zdigitalizowanych,
 - w zakresie przekazywania indeksów EDM.
2. System musi umożliwiać:
 - przygotowanie listy dokumentów podlegających indeksowaniu w P1,
 - identyfikację dokumentów niezaindeksowanych,
 - prezentację problemów indeksacji wraz z ich statusem.

2.7. Wsparcie użytkownika i działania naprawcze

1. System musi:
 - prezentować listę problemów związanych z indeksacją dokumentów w P1,
 - wskazywać działania naprawcze możliwe do wykonania przez użytkownika.
2. Użytkownik musi mieć bezpośredni dostęp do funkcjonalności realizujących wskazane działania naprawcze.

3. Integracje i zależności

3.1. Integracje zewnętrzne

- Integracja z Platformą P1 w zakresie obsługi dokumentów zdigitalizowanych oraz ich indeksacji.

3.2. Zależności między modułami

- Funkcjonalność opiera się na:
 - systemie HIS,
 - repozytorium EDM,
 - komponente odpowiedzialnym za komunikację z Platformą P1.
- Wszystkie komponenty muszą być ze sobą zintegrowane i działać w ramach jednego ekosystemu HIS.

4. Kryteria odbioru produktu

Produkt zostanie uznany za zgodny funkcjonalnie, jeżeli spełnione zostaną łącznie następujące kryteria:

1. System umożliwia monitorowanie poziomu zaindeksowania dokumentów (kart informacyjnych), w tym dokumentów zdigitalizowanych, oraz prezentuje poprawne statystyki zgodne z faktyczną liczbą dokumentów lub indeksów.
2. System umożliwia tworzenie dokumentów elektronicznych zgodnych z PIK HL7 CDA na podstawie dokumentów zeskanowanych oraz ich zapis w repozytorium EDM.
3. System umożliwia przekazywanie dokumentów zdigitalizowanych i ich indeksów do Platformy P1 zgodnie ze specyfikacją usług.
4. System umożliwia wymuszenie wysyłki indeksu dokumentu EDM do P1 z poziomu GUI HIS i GUI repozytorium EDM.
5. System poprawnie obsługuje automatyczną oraz ręczną reindeksację dokumentów.
6. System prezentuje listę błędów indeksacji oraz umożliwia realizację działań naprawczych.

5. Wymagania do uruchomienia produktu

5.1. Warunki startowe

1. Aktywna licencja na funkcjonalność.
2. Działająca integracja z Platformą P1 w zakresie wymiany EDM.
3. Skonfigurowane repozytorium EDM.

5.2. Wymagania techniczne

1. Rozwiązanie opiera się na istniejących komponentach HIS, EDM oraz P1.
2. Dopuszcza się wykorzystanie zewnętrznych urządzeń skanujących, przy czym Zamawiający zapewnia zasoby zgodne z wymaganiami producentów tych urządzeń.

5.3. Wymagania organizacyjne

1. Podmiot musi być zintegrowany z Platformą P1, w szczególności:
 - posiadać aktywne konto w P1,
 - posiadać aktualne certyfikaty dostępowe.
2. W przypadku wykorzystania systemów zewnętrznych – wymagane posiadanie odpowiednich licencji integracyjnych.

6. Opis wdrożenia

W ramach wdrożenia Wykonawca zrealizuje co najmniej:

1. Uzupelnienie i weryfikację konfiguracji systemu HIS, repozytorium EDM oraz komponentów P1 w zakresie indeksacji dokumentów zdigitalizowanych.
2. Ewentualną konfigurację integracji z urządzeniami skanującymi (jeżeli są wykorzystywane).

3. Testy poprawności:
 - tworzenia dokumentów PIK HL7 CDA,
 - podpisu elektronicznego,
 - indeksacji i reindeksacji dokumentów w Platformie P1.
4. Przekazanie informacji powdrożeniowej i potwierdzenie gotowości rozwiązania do odbioru.

4.4. Rozszerzenie EDM o nowe dokumenty ustawowe wraz z monitorowaniem

1. Przedmiot zamówienia

Przedmiotem zamówienia jest dostawa, konfiguracja i uruchomienie funkcjonalności systemu HIS umożliwiającej generowanie, obsługę oraz wymianę Elektronicznej Dokumentacji Medycznej (EDM), wraz z integracją z Platformą P1, w tym obsługą dokumentów specjalistycznych oraz monitorowaniem poziomu ich indeksacji.

2. Wymagania funkcjonalne

2.1. Generowanie dokumentów EDM

1. System HIS musi umożliwiać generowanie dokumentów medycznych w postaci elektronicznej, zgodnie z obowiązującymi standardami oraz przepisami prawa, w zakresie przypisanym do systemu HIS.
2. System musi obsługiwać generowanie co najmniej następujących typów dokumentów:
 - opisy badań histopatologicznych,
 - 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 (orzeczenia lekarskie oraz wytyczne wynikające z warunków lub stanowiska pracy).
3. System musi uwzględniać przypadki, w których określone dokumenty (np. Patient Summary) są generowane po stronie Platformy P1, a nie bezpośrednio w HIS.

2.2. Integracja z Platformą P1

1. System musi umożliwiać integrację z Platformą P1 w zakresie obsługi i wymiany EDM.
2. Integracja musi obejmować następujące typy dokumentów:
 - 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.
3. System musi umożliwiać:
 - przekazywanie dokumentów EDM do P1,

- przekazywanie indeksów dokumentów do P1 – w zależności od dostępnych usług dla danego typu dokumentu.
- 4. W zakresie Krajowej Sieci Onkologicznej (KSO) system musi zapewniać wymianę danych w standardzie FHIR dla:
 - karty e-DILO,
 - planu leczenia onkologicznego.

2.3. Monitorowanie indeksacji EDM w P1

1. System musi umożliwiać monitorowanie stanu indeksacji dokumentów EDM w Platformie P1.
2. Monitorowanie musi być dostępne:
 - na poziomie zbiorczych statystyk,
 - z dokładnością do typu dokumentu,
 - z możliwością określenia przedziału czasowego.
3. System musi umożliwiać analizę:
 - wzrostu procentowego,
 - wzrostu liczbowegopoziomu zaindeksowanej EDM, w szczególności w zakresie wyników badań laboratoryjnych oraz opisów badań diagnostycznych.

3. Integracje

3.1. Integracje wewnętrzne

1. W realizacji procesów objętych zamówieniem muszą uczestniczyć:
 - system HIS,
 - repozytorium EDM,
 - komponenty brzegowe odpowiedzialne za komunikację z Platformą P1.

3.2. Integracje zewnętrzne

1. Rozwiązanie musi obejmować integrację z Platformą P1:
 - poprzez usługi ogólnej wymiany EDM,
 - oraz usługi dedykowane dla określonych typów dokumentów (np. Patient Summary, e-DILO).

4. Zależności między modułami

1. Funkcjonalność musi opierać się na:
 - systemie HIS,
 - repozytorium EDM,
 - komponentach odpowiedzialnych za komunikację z Platformą P1.
2. Wszystkie elementy muszą być ze sobą logicznie i technicznie zintegrowane w sposób zapewniający spójność danych i ciągłość procesów medycznych.

5. Kryteria odbioru produktu

Produkt zostanie uznany za zgodny z OPZ, jeżeli spełni łącznie następujące kryteria:

1. Umożliwia generowanie dokumentów EDM zgodnie z obowiązującymi formatami i przepisami prawa.
2. Umożliwia przekazywanie dokumentów lub ich indeksów do Platformy P1, zgodnie z dostępnymi usługami.
3. Umożliwia wyszukiwanie i pobieranie dokumentów określonych typów w ramach Platformy P1.

4. Zapewnia dostęp do statystyk wykorzystania usług centralnych P1.
5. Umożliwia monitorowanie zwiększenia poziomu zaindeksowanej EDM, w szczególności w zakresie wyników badań laboratoryjnych oraz opisów badań diagnostycznych.
6. Zapewnia wymianę danych w standardzie FHIR w zakresie KSO (e-DILO i plan leczenia onkologicznego).

6. Wymagania do uruchomienia produktu

6.1. Warunki startowe

1. Posiadanie licencji na wymaganą funkcjonalność systemu HIS.
2. Działająca integracja z Platformą P1 w zakresie wymiany EDM.

6.2. Wymagania techniczne

1. W zakresie KSO – zapewnienie zasobów sprzętowych i systemowych dla komponentu odpowiedzialnego za komunikację z usługami FHIR (analogicznych jak dla komponentu brzegowego Zdarzeń Medycznych).
2. W pozostałym zakresie rozwiązanie musi wykorzystywać istniejące komponenty infrastruktury.
3. W przypadku braku rezerw wydajnościowych na maszynach obsługujących instalacje AMDX oraz adapter P1, zaleca się zwiększenie zasobów o około **10%**.

6.3. Wymagania organizacyjne

1. Podmiot leczniczy musi być zintegrowany z Platformą P1, w szczególności:
 - posiadać aktywne konto podmiotu w P1,
 - posiadać aktualne certyfikaty dostępowe.

7. Zakres wdrożenia i konfiguracji

W ramach realizacji zamówienia Wykonawca zobowiązany jest do:

1. Aktualizacji komponentów AMDX oraz adaptera P1.
2. Instalacji komponentów odpowiedzialnych za integrację z usługami FHIR w zakresie KSO.
3. Uzupełnienia i weryfikacji konfiguracji systemowej zgodnie z dostarczoną dokumentacją, w szczególności:
 - konfiguracji adresów nowych usług Platformy P1,
 - parametrów komunikacyjnych i bezpieczeństwa.

4.5. Integracja z Krajowym Rejestrem Nowotworów

1. Przedmiot zamówienia

Przedmiotem zamówienia jest dostawa, konfiguracja i uruchomienie modułu integracyjnego umożliwiającego przekazywanie danych do rejestru onkologicznego e-KRN+, obejmującego:

- integrację systemu dziedzinnego/HIS z systemem e-KRN+ w zakresie zdarzeń medycznych związanych z diagnostyką i leczeniem pacjentów onkologicznych,
- instalację i konfigurację providera e-KRN na platformie integracyjnej,
- konfigurację harmonogramu wysyłki danych (CRON),
- testy integracyjne i odbiorowe oraz uruchomienie produkcyjne,
- szkolenie personelu i przekazanie dokumentacji powdrożeniowej.

2. Wymagania funkcjonalne

2.1. Integracja z e-KRN+ i zakres danych

1. System musi umożliwiać integrację systemu dziedzinnego z rejestrem onkologicznym e-KRN+ w zakresie przekazywania informacji o zdarzeniach medycznych związanych z:

- diagnostyką pacjenta onkologicznego,
 - leczeniem pacjenta onkologicznego.
2. System musi zapewniać przekazywanie danych w sposób zgodny z wymaganiami e-KRN+ (w szczególności w zakresie struktury i logiki przekazywanych zdarzeń).

2.2. Mechanizm komunikacji

1. Integracja z e-KRN+ musi być realizowana przy użyciu usług sieciowych (web services).
2. Moduł musi działać w oparciu o usługi sieciowe zgodnie ze specyfikacją e-KRN+.

2.3. Harmonogramowanie wysyłki (CRON)

1. System musi umożliwiać użytkownikowi/administratorowi zdefiniowanie własnego harmonogramu zadań (CRON) uruchamiającego proces wysyłki danych do e-KRN+.
2. Harmonogram musi być konfigurowalny i możliwy do modyfikacji (np. częstotliwość, okna czasowe, godziny pracy).

3. Integracje

3.1. Integracje wewnętrzne

1. Moduł musi wykorzystywać usługi integracyjne dostępne na platformie integracyjnej HIS.
2. W ramach realizacji zamówienia musi zostać zapewniona instalacja providera e-KRN umożliwiającego komunikację z systemem e-KRN+.

3.2. Integracje zewnętrzne

1. Rozwiązanie musi obejmować integrację z zewnętrznym systemem:
 - Krajowy Rejestr Nowotworów – e-KRN+.

4. Zależności między modułami i komponentami

1. Funkcjonalność wymaga systemu HIS AMMS oraz platformy integracyjnej HIS w wersjach zgodnych z wymaganiami minimalnymi.
2. Konfiguracja integracji realizowana jest z wykorzystaniem komponentów administracyjnych i integracyjnych (w szczególności modułu ADMIN_PANEL oraz platformy integracyjnej).

5. Kryteria odbioru produktu

Produkt zostanie uznany za zgodny z OPZ, jeżeli spełni łącznie następujące kryteria:

1. Moduł umożliwia integrację systemu dziedzicznego z e-KRN+ w zakresie przekazywania danych o zdarzeniach medycznych związanych z diagnostyką i leczeniem pacjentów onkologicznych.
2. Moduł realizuje komunikację w oparciu o usługi sieciowe zgodnie ze specyfikacją e-KRN+.
3. Użytkownik/administrator ma możliwość skonfigurowania własnego harmonogramu zadań (CRON) uruchamiającego wysyłkę danych.
4. Provider e-KRN jest zainstalowany i skonfigurowany, a komunikacja z e-KRN+ działa poprawnie.
5. Integracja przebiega zgodnie z wymaganiami organizacyjnymi i technicznymi Zamawiającego (sieć, bezpieczeństwo, dostępność).
6. Proces przekazywania danych został przetestowany – dane są poprawnie:
 - wysyłane z systemu,
 - odbierane i potwierdzane po stronie e-KRN+ (zgodnie z mechanizmem potwierdzeń).
7. Zrealizowano szkolenie personelu oraz przekazano dokumentację powdrożeniową.
8. Produkt uruchomiono w środowisku Zamawiającego na wymaganej wersji AMMS i platformy integracyjnej.

6. Wymagania do uruchomienia produktu

6.1. Warunki startowe

1. Minimalna wersja systemu HIS:
 - AMMS 6.00.05.00
2. Minimalna wersja Platformy Integracyjnej:
 - PI 6.00.05.00
3. Wymagane licencje:
 - licencja na moduł ADMIN_PANEL,
 - licencja/funkcjonalność: E-KRN – Integracja z systemem e-KRN+.

6.2. Wymagania techniczne

1. AMMS w wersji co najmniej 6.00.05.00.
2. Platforma Integracyjna (PI) w wersji co najmniej 6.00.05.00.
3. Zainstalowany provider e-KRN na serwerze integracyjnym.
4. Dostępność środowiska sieciowego umożliwiająca komunikację z usługami e-KRN+, w tym:
 - konfiguracja firewall,
 - otwarte wymagane porty,
 - obsługa certyfikatów (jeżeli wymagane).
5. Aktualna licencja ADMIN_PANEL z aktywną funkcjonalnością E-KRN.

6.3. Wymagania organizacyjne

1. Wyznaczenie administratora odpowiedzialnego za konfigurację i utrzymanie integracji.
2. Zapewnienie udziału personelu medycznego i/lub administracyjnego w szkoleniu.
3. Uzgodnienie harmonogramu wysyłki (CRON) z zespołem medycznym/IT.
4. Dostępność zespołu IT Zamawiającego podczas wdrożenia oraz testów akceptacyjnych.
5. Akceptacja procedury testów przekazywania danych do e-KRN+.

7. Zakres wdrożenia i konfiguracji

7.1. Działania przygotowawcze

Wykonawca zobowiązany jest do wykonania (lub wsparcia wykonania) czynności przygotowawczych przed uruchomieniem licencji produkcyjnej, co najmniej:

1. Instalacja Platformy Integracyjnej (jeżeli nie jest dostępna lub wymaga aktualizacji).
2. Instalacja providera e-KRN.
3. Ustawienie parametrów uruchomieniowych środowiska integracyjnego.
4. Uruchomienie i weryfikacja działania providera e-KRN+ w środowisku Zamawiającego.

7.2. Wdrożenie produkcyjne

W ramach wdrożenia produktu Wykonawca zobowiązany jest do:

1. Wgrania licencji (ADMIN_PANEL oraz funkcjonalność E-KRN).
2. Ustawienia parametrów konfiguracyjnych AMMS niezbędnych do poprawnej pracy integracji.
3. Przekodowania elementów leczenia na notatki – w zakresie wymaganym do prawidłowego mapowania/przekazywania danych (zgodnie z uzgodnioną metodyką i dokumentacją wdrożeniową).
4. Skonfigurowania harmonogramu CRON wysyłki danych.
5. Przeprowadzenia testów integracyjnych i testów akceptacyjnych.
6. Przeprowadzenia szkolenia personelu oraz konsultacji stanowiskowych.
7. Przekazania dokumentacji powdrożeniowej (konfiguracja, instrukcja obsługi, scenariusze testów/odbioru).

4.6. Karta uodpornień

1. Przedmiot zamówienia

Przedmiotem zamówienia jest dostarczenie, wdrożenie oraz udostępnienie funkcjonalności systemu informatycznego umożliwiającego prowadzenie Karty Uodpornień pacjenta, w tym rejestrację, przetwarzanie, prezentację oraz raportowanie danych dotyczących szczepień ochronnych, a także integrację z Elektroniczną Kartą Szczepień prowadzoną w systemie centralnym SIM (P1).

2. Zakres funkcjonalny systemu

2.1. Rejestracja i dostępność danych medycznych

1. System musi zapewniać możliwość rejestracji informacji o szczepieniach w danych medycznych pacjenta.
2. Dane dotyczące szczepień muszą być:
 - o trwale przypisane do pacjenta,
 - o dostępne i widoczne w kontekście każdego pobytu pacjenta w podmiocie leczniczym.

2.2. Karta Uodpornień – dokumentacja i wydruki

1. System musi umożliwiać wygenerowanie i wydruk dokumentu „Karta Uodpornienia” zgodnego z obowiązującym rozporządzeniem w sprawie szczepień obowiązkowych.
2. System może uwzględniać w Karcie Uodpornienia planowane szczepienia wynikające z aktualnego kalendarza szczepień, o ile kalendarz ten jednoznacznie określa listę szczepień dla poszczególnych grup wiekowych.
3. W przypadku dzieci urodzonych po dniu 1 października 2023 r.:
 - a. decyzję o rodzaju szczepień oraz przypisaniu do grupy wiekowej podejmuje lekarz, w zależności od wagi urodzeniowej oraz tygodnia urodzenia,
 - b. wydruk Karty Uodpornienia nie uwzględnia listy szczepień obowiązkowych.
4. System musi umożliwiać wybór schematu szczepień:
 - a. podstawowego,
 - b. rozszerzonego,dla dzieci urodzonych po dniu 1 października 2023 r.

2.3. Ewidencja szczepień

1. System musi umożliwiać rejestrację i ewidencję danych dotyczących szczepienia, obejmujących co najmniej:
 - a. datę kwalifikacji do szczepienia,
 - b. dane osoby kwalifikującej,
 - c. datę odroczenia szczepienia, jeżeli podczas kwalifikacji podjęto decyzję o odroczeniu,
 - d. numer dawki,
 - e. liczbę dawek wymaganych do optymalnego zaszczepienia,
 - f. dawkę wraz z jednostką,
 - g. dane dotyczące podanej szczepionki, w tym:
 - i. producenta,
 - ii. numeru serii,
 - iii. terminu ważności,
 - iv. liczby dawek w opakowaniu.

2. System musi wykorzystywać słowniki publikowane przez system SIM (P1), w zakresie co najmniej:
 - a. części ciała,
 - b. drogi podania,
 - c. źródła finansowania.
3. Zakres rejestrowanych danych musi być zgodny z zakresem danych przekazywanych do systemu SIM w ramach zdarzeń medycznych.

2.4. Odmowy szczepień

1. System musi umożliwiać oznaczenie odmowy wykonania szczepienia, wynikającego z listy szczepień obowiązkowych ujętych w Karcie Uodpornienia.

2.5. Obsługa wizyty i procedur medycznych

1. System musi umożliwiać:
 - a. dodawanie szczepień w ramach danych wizyty,
 - b. wprowadzanie szczegółów dotyczących podanego preparatu,
 - c. prezentację danych o szczepieniach zarejestrowanych w trakcie wizyty.
2. System musi umożliwiać przejście z poziomu danych wizyty do szczegółów zarejestrowanych szczepień.
3. System musi umożliwiać:
 - a. odnotowywanie szczepień w ramach danych wizyty,
 - b. odrębną ewidencję podanego preparatu oraz szczegółów wykonanej procedury medycznej.
4. System musi weryfikować kompletność danych dotyczących:
 - a. szczepienia,
 - b. podanego preparatu,
 - c. wykonanej procedury,przy czym musi istnieć możliwość przesunięcia walidacji podania leku i procedury na moment zatwierdzenia zakończenia wizyty.
5. System musi umożliwiać konfigurację automatycznego rejestrowania wykonanych procedur medycznych po zaewidencjonowaniu podania leku.

2.6. Integracja z systemem SIM (P1)

1. System musi zapewniać możliwość zapisu informacji o szczepieniu w Elektronicznej Karcie Szczepień prowadzonej w systemie SIM (P1).
2. System musi obsługiwać podpis odpowiednich zasobów zdarzeń medycznych przekazywanych do systemu SIM (P1).
3. System musi udostępniać listę wykonanych szczepień oraz umożliwiać zbiorczy podpis szczepień odnotowanych w systemie P1.

2.7. Raportowanie i zestawienia

1. System musi udostępniać możliwość wykonywania zestawień i raportów dotyczących zrealizowanych szczepień.

4.7. Import e-Deklaracji z systemu P1

1. Przedmiot zamówienia

Przedmiotem zamówienia jest dostarczenie i wdrożenie funkcjonalności systemu informatycznego klasy HIS, umożliwiającej import, obsługę oraz przetwarzanie e-Deklaracji POZ składanych przez pacjentów za pośrednictwem Internetowego Konta Pacjenta (IKP), a przechowywanych i obsługiwanych w systemie centralnym P1.

Funkcjonalność musi zapewniać poprawną integrację z systemem P1, umożliwiającą pobieranie, przeglądanie, akceptację lub odrzucanie e-Deklaracji oraz aktualizację danych pacjenta w systemie HIS.

2. Zakres funkcjonalny

2.1. Przegląd i obsługa e-Deklaracji

1. System musi umożliwiać przegląd e-Deklaracji POZ złożonych przez pacjentów w systemie IKP i udostępnionych w systemie P1.
2. System musi prezentować listę e-Deklaracji wraz z podstawowymi informacjami umożliwiającymi ich identyfikację, w szczególności:
 - a. dane pacjenta,
 - b. typ deklaracji,
 - c. data złożenia deklaracji,
 - d. status deklaracji.

2.2. Podgląd szczegółów e-Deklaracji

1. System musi umożliwiać podgląd szczegółów wybranej e-Deklaracji POZ w postaci dokumentu PDF, zgodnie z formatem udostępnianym przez system P1.
2. Podgląd dokumentu musi być dostępny bez konieczności eksportu danych poza system HIS.

2.3. Akceptacja i odrzucenie e-Deklaracji

1. System musi umożliwiać:
 - a. zaakceptowanie e-Deklaracji POZ w systemie P1,
 - b. odrzucenie e-Deklaracji POZ w systemie P1.
2. Operacje akceptacji lub odrzucenia e-Deklaracji muszą być realizowane z poziomu systemu HIS, z wykorzystaniem integracji z systemem P1.
3. System musi zapewniać aktualizację statusu e-Deklaracji po wykonaniu operacji akceptacji lub odrzucenia.

2.4. Import danych do systemu HIS

1. System musi umożliwiać pobranie danych e-Deklaracji złożonej w systemie P1 do systemu HIS.
2. Import danych musi obejmować co najmniej dane pacjenta oraz dane związane z treścią e-Deklaracji, w zakresie udostępnianym przez system P1.

2.5. Aktualizacja danych pacjenta

1. System musi umożliwiać aktualizację danych pacjenta w systemie HIS na podstawie danych zawartych w e-Deklaracji.
2. Aktualizacja danych pacjenta musi być realizowana w sposób kontrolowany, z zachowaniem spójności danych oraz zgodnie z obowiązującymi zasadami prowadzenia dokumentacji medycznej.

3. Wymagania integracyjne (minimalne)

1. Funkcjonalność importu e-Deklaracji musi być realizowana w oparciu o obowiązujące mechanizmy integracyjne systemu P1.
2. System musi zapewniać poprawną obsługę komunikacji, błędów oraz statusów wymiany danych z systemem P1.

4.8. Upgrade Banku Krwi, Serologii, oraz Integracja z systemem e-Krew

1. Przedmiot zamówienia

Przedmiotem zamówienia jest wykonanie upgrade'u (aktualizacji/modernizacji) oraz wdrożenie modułu Bank Krwi z Serologią (dalej: „System”) wraz z uruchomieniem i konfiguracją integracji z systemem centralnym e-Krew, a także zapewnieniem współpracy Systemu z działającym w Szpitalu systemem HIS/AMMS i EDM.

System ma wspierać kompleksowy proces leczenia krwią i jej składnikami, w szczególności: obsługę zamówień, rezerwacji i wydań, gospodarkę magazynową składnikami krwi, ewidencję przetoczeń i powikłań poprzetoczeniowych oraz obsługę badań serologicznych (grupa krwi, fenotyp, przeciwciała, próby zgodności). System musi być przeznaczony dla lekarzy, pielęgniarek, diagnostów laboratoryjnych oraz personelu Banku Krwi.

2. Zakres zamówienia

Zakres zamówienia obejmuje w szczególności:

1. Upgrade/uruchomienie Systemu Bank Krwi i Serologia w środowisku Zamawiającego.
2. Konfigurację Systemu, w tym słowników i parametrów niezbędnych do pracy produkcyjnej.
3. Integrację wewnętrzną z HIS/AMMS i EDM (w tym HL7, JMS, Web-Services) zgodnie z wymaganiami opisanymi w niniejszym OPZ.
4. Integrację zewnętrzną z e-Krew (zamówienia krwi/składników, badania konsultacyjne, przekazywanie informacji o powikłaniach – w zakresie udostępnionych usług).
5. Integrację z analizatorem (zlecenie/odbiór wyników) – pod warunkiem zapewnienia przez Zamawiającego możliwości technicznej komunikacji z urządzeniem.
6. Szkolenia użytkowników oraz administratorów.
7. Przygotowanie i przekazanie dokumentacji administracyjnej i konfiguracyjnej.

3. Wymagania funkcjonalne

3.1. Bank Krwi – ewidencja pacjentów

System musi umożliwiać co najmniej:

1. dostęp do podstawowych danych pacjenta: imię i nazwisko, data urodzenia, identyfikator (PESEL lub inny zgodny z przepisami), identyfikator szpitalny, adres, PESEL matki/opiekuna (jeżeli dotyczy);
2. ewidencję pobrań autologicznych wraz z wydrukiem etykiety; dla składnika autologicznego system musi blokować wydanie innemu pacjentowi niż dawca;
3. przegląd zamówień na krew i jej składniki dla pacjenta, pochodzących z różnych oddziałów – przy czym źródłem zamówień jest HIS/AMMS;
4. ewidencję rezerwacji krwi i jej składników dla pacjenta;
5. ewidencję wydań na oddział dla pacjenta wraz z odnotowaniem potwierdzenia przetoczenia lub powikłań poprzetoczeniowych (zgodnie z wymaganiami e-Krew);
6. ewidencję badań serologicznych pacjenta wykonanych w pracowni serologii;
7. ewidencję historii przeszczepień (dla pacjentów po przeszczepie);
8. ewidencję cech serologicznych pacjenta (grupa, fenotyp, przeciwciała) z możliwością dołączenia skanu wyniku z pliku (badania wykonane poza Szpitalem);

9. konfigurację uwag stałych pacjenta z możliwością wydruku na wynikach; uwagi muszą być widoczne w całym Systemie w kontekście pacjenta;
10. wyróżnianie pacjentów wg grup cech zdefiniowanych/nazwanych przez użytkownika;
11. obsługę pacjentów NN oraz automatyczną aktualizację danych pacjenta na podstawie danych z HIS/AMMS.

3.2. Bank Krwi – dostawy krwi i składników

System musi umożliwiać:

1. ewidencję dostaw krwi i składników wraz z cenami usług dodatkowych RCKiK oraz cenami składników zgodnymi z przepisami;
2. przyjmowanie składników na stan magazynowy poprzez skanowanie etykiet zgodnych ze standardem ISBT 128 – z możliwością skanowania kodów w dowolnej kolejności;
3. ewidencję rozmrażania osocza i krioprecypitatu oraz przyjęcia na magazyn rozmrożonych składników, wraz z możliwością wydruku etykiety dla rozmrożonego składnika (ISBT);
4. wydruk kwitu dostawy.

3.3. Bank Krwi – stany magazynowe i śledzenie składnika

System musi umożliwiać:

1. wyświetlanie listy składników na magazynie z podziałem na grupy (min. KKCZ, FFP, KKP, KRIO) oraz filtrowanie;
2. generowanie interaktywnego raportu stanów magazynowych (składnik/rodzaj/grupa krwi);
3. podgląd szczegółów składnika (m.in. numer donacji, numer podziału, kod składnika, data donacji, objętość, data ważności, dane dostawy) oraz pełną ewidencję zdarzeń: przesunięcia, wydania (oddział/pacjent/data/kwit/osoba), zwroty, utylizacje z powodami definiowanymi przez użytkownika;
4. graficzną oś czasu czynności wykonanych dla składnika;
5. listę rezerwacji składników krwi dla pacjenta;
6. listę badań w kontekście składnika (w tym wyniki prób krzyżowych);
7. obsługę więcej niż jednego magazynu oraz przesunięcia międzymagazynowe wraz z historią.

3.4. Bank Krwi – dokumenty magazynowe

System musi umożliwiać generowanie dokumentów w formacie PDF, co najmniej:

- dokument przyjęcia,
- kwit wydania wewnętrznego dla oddziału,
- dokument wydania zewnętrznego,
- protokół utylizacji/zniszczenia,
- dokument przesunięcia.

3.5. Bank Krwi – zamówienia wewnętrzne i realizacja

System musi umożliwiać:

1. obsługę zamówień na krew i składniki z wymianą informacji z HIS/AMMS w zakresie niezbędnym do prawidłowej realizacji;
2. ewidencję zamówień w trybach: zwykłe, pilne, na ratunek;
3. składanie zamówień manualnie i automatycznie (elektroniczne zamówienie z oddziału);
4. rezerwację składników dla pacjenta;
5. walidację zgodności ABO i RhD rezerwowanego składnika z zamówieniem;
6. walidację rezerwacji na ważność próby zgodności i ważność składnika;

7. automatyczne anulowanie niewykorzystanych rezerwacji KKCZ po przeterminowaniu próby zgodności;
8. utworzenie dokumentu wydania z Ośrodkiem Powstawania Kosztu oraz osobą wydającą i odbierającą;
9. automatyczne i manualne przekazywanie do HIS/AMMS informacji o wydanym składniku (w tym ceny oraz kody NFZ niezbędne do rozliczeń), aby umożliwić prawidłową ewidencję przetoczenia i wygenerowanie elektronicznej książki transfuzyjnej na oddziale.

3.6. Bank Krwi – zamówienia do RCKiK i e-Krew

System musi umożliwiać:

1. ewidencję zamówień do RCKiK (zbiorczych i indywidualnych);
2. elektroniczne wystanie zamówień do systemu centralnego e-Krew.

3.7. Bank Krwi – resztki, raporty i powikłania

System musi umożliwiać:

1. ewidencję resztek poprzetoczeniowych (dane składnika, data przyjęcia, data rozchodu/utyliczacji);
2. generowanie raportów w PDF i XLS, co najmniej:
 - składniki z kończącym się terminem ważności,
 - wydania wg oddziałów i pacjentów,
 - dostawy składników,
 - rozliczenie z RCKiK wg cennika,
 - książka przychodów i rozchodów,
 - zestawienie zużycia;
3. rejestrowanie powikłań poprzetoczeniowych i zdarzeń niepożądanych;
4. (wymaganie zalecane) elektroniczne przekazywanie informacji o powikłaniach/zdarzeniach do RCKiK za pośrednictwem e-Krew.

3.8. Bank Krwi – słowniki i administracja

System musi umożliwiać zarządzanie słownikami przez uprawnionych użytkowników, w tym:

- słownik kodów ostatecznych ISBT (zawartość dostarczana przez Wykonawcę przy wdrożeniu),
- słownik składników z mapowaniem kodów ISBT do grup preparatów,
- cennik preparatów (ceny, jednostka rozliczenia, kod świadczenia NFZ, import z pliku),
- słownik kontrahentów/organizacji (import struktury szpitala z pliku),
- słownik miejsc przechowywania (magazyny i miejsca np. lodówki),
- słownik personelu (synchronizacja z HIS/AMMS),
- słownik powodów utylizacji (inicjalnie zgodny z e-Krew).

System musi zapewniać obsługę administracyjną poprzez panel administratora.

4. Wymagania funkcjonalne – Serologia

4.1. Zlecenia na badania

System musi umożliwiać:

1. obsługę zleceń w trybach: normalny, pilny, pilna transfuzja z poziomu pacjenta;
2. rejestrację prób zgodności serologicznej i wyników (min. kategorie: zgodna, zgodna w próbie krzyżowej, serologicznie niezgodna/fenotypowo zgodna, niezgodna serologicznie, niezgodna);
3. rejestrację zleceń na badania serologiczne manualnie i automatycznie (integracja z HIS);

4. rejestrację zleceń na próby zgodności.

4.2. Wyniki i protokoły

System musi umożliwiać:

1. ewidencję protokołów wyników grup krwi i badań konsultacyjnych oraz wystawienie wyniku opisowego;
2. podgląd listy zleconych badań wg oddziału zlecającego (dane pacjenta i zlecenia);
3. modyfikację, podgląd i zatwierdzanie wyników przez uprawnionych użytkowników, z rejestrowaniem: fenotypów (w tym siły aglutynacji), przeciwciał, BTA, danych wykonującego i autoryzującego, daty/godziny pobrania próbki, numeru zewnętrznego badania oraz możliwością dołączenia skanu;
4. ewidencję protokołów prób zgodności (w tym dla noworodków);
5. wyszukiwanie badań wg kryteriów (kod/nazwa, pacjent, PESEL, status, numer);
6. ostrzeżenia o zmianie już zatwierdzonych wyników (grupa krwi, przeciwciała);
7. przegląd i wydruk listy wykonanych badań w zadanym zakresie numerów;
8. uzupełnianie badania i zatwierdzenie wyniku ostatecznego po uzyskaniu wyniku konsultacyjnego;
9. wyszukiwanie wg atrybutów (np. układ fenotypów, obecność przeciwciał);
10. sygnalizację niezgodności wyniku względem wcześniejszych wyników pacjenta;
11. automatyczne nadawanie numeru badania wg ustalonego formatu;
12. wydruk etykiety z numerem badania i kodem paskowym (PDF);
13. obsługę statusów zlecenia: nowe, zatwierdzone, wykonane, anulowane;
14. raport podsumowujący liczbę badań dla oddziału.

4.3. Wydruki i przekazywanie wyników do HIS/EDM

1. System musi umożliwiać wydruk wyników (grupy krwi, konsultacyjne) z fenotypami i przeciwciałami zgodnie z przepisami.
2. System musi umożliwiać wydruk prób zgodności dla dorosłych i noworodków (dla noworodków – możliwość odnotowania danych matki).
3. System musi umożliwiać przekazywanie do HIS/EDM informacji o potwierdzonych/podpisanych wynikach badań.

4.4. Kartoteka pacjentów dla Serologii

System musi umożliwiać:

1. ewidencję danych pacjenta (m.in. dwie wartości grupy krwi: źródło Serologia i źródło HIS, PESEL, płeć, identyfikator, data rejestracji, waga, telefon);
2. obsługę pacjentów NN z automatyczną aktualizacją danych z HIS;
3. manualne wprowadzanie pacjentów spoza Szpitala;
4. automatyczne zakładanie kartotek z danych z HIS;
5. przegląd historii pacjenta: zlecenia, badania, protokoły;
6. wyszukiwanie pacjentów po wielu kryteriach;
7. skanowanie i przechowywanie wyników zewnętrznych;
8. wyróżnianie pacjentów wg cech zdefiniowanych przez użytkownika;
9. ewidencję cech serologicznych z podpięciem skanów.

System musi umożliwiać ewidencję uwag stałych pacjenta, ostrzeżenia podczas wprowadzania danych, blokowanie uwag zdezaktualizowanych oraz śledzenie historii zmian.

4.5. Alerty, próbki, cenniki, słowniki i raporty

System powinien:

- sygnalizować wykrycie przeciwciał i konieczność doboru specjalnie dobranego składnika krwi.

System musi umożliwiać:

1. ewidencję pacjentów po przeszczepie szpiku (zmiana/po zmianie grupy krwi, wydruki, możliwość zmiany grupy);
2. automatyczną ewidencję próbek na podstawie komunikacji z HIS oraz manualną ewidencję próbek;
3. tworzenie i modyfikację cennika badań, automatyczne dopisywanie procedur do protokołu oraz przekazywanie do HIS informacji o procedurach i ich wartości;
4. definiowanie słowników (rodzaje badań/metody/pakiety, personel – synchronizacja z HIS, kontrahenci, sprzęt jednorazowy, aparatura);
5. raporty w PDF/XLS (ilości badań wg ośrodków kosztów/oddziałów/pacjentów oraz procedury);
6. wydruki (książka serologiczna grup krwi, książka prób zgodności, wyniki, lista zleceń).

5. Integracje i zależności

5.1. Integracje wewnętrzne z HIS/AMMS

System musi zapewniać integrację z HIS/AMMS, obejmującą co najmniej:

1. kontekstowe wywołanie Banku Krwi i Serologii (URL/token/Web-Service ContextParameterService);
2. komunikację HL7 dla:
 - zamówień na składniki krwi wraz z kartoteką pacjenta,
 - zleceń na badania serologiczne wraz z kartoteką pacjenta,
 - aktualizacji i scalania kartotek,
 - odsyłania realizacji zamówień,
 - odsyłania wyników badań (protokoły);
3. kolejkę JMS oraz Web-Services dla:
 - powikłań poprzetoczeniowych i zdarzeń niepożądanych,
 - synchronizacji słownika personelu.

Wymagana jest nadrzędność danych osobowych pacjenta po stronie HIS/AMMS.

5.2. Integracja z EDM/HIS (API)

System musi współpracować z EDM/HIS zgodnie ze specyfikacją EDM API v2.13 (producenta EDM/HIS) w zakresie:

- wysyłania podpisanych dokumentów,
- podglądu wyników badań grup krwi pacjenta zarejestrowanych w Serologii.

5.3. Integracje zewnętrzne

System musi zapewniać integrację z:

1. e-Krew – zamawianie krwi i składników w RCKiK, zlecenie badań konsultacyjnych oraz przekazywanie informacji o powikłaniach w zakresie dostępnych usług;
2. analizatorem – zlecenie badań i odbiór wyników (warunek: Zamawiający zapewni możliwość integracji z urządzeniem).

5.4. Zależności

1. Dla pełnej funkcjonalności wymagane jest działanie HIS/AMMS wraz z platformą integracyjną (procesy HL7, kolejka JMS).
2. System zależy od prawidłowo uruchomionego i skonfigurowanego Keycloak.
3. Rekomendowane jest zintegrowanie Keycloak z Active Directory Szpitala w zakresie użytkowników i haseł.

6. Wymagania niefunkcjonalne: dostęp, SSO, audyt, kopie

1. System musi być dostępny webowo z użyciem przeglądarki internetowej.
2. Bank Krwi i Serologia muszą zapewniać SSO pomiędzy modułami oraz brak ponownego logowania przy przejściu z HIS/AMMS po kliknięciu dedykowanej ikony (dla użytkowników o tych samych loginach w HIS i Systemie).
3. System musi umożliwiać integrację z Active Directory jako podstawowym źródłem użytkowników, z możliwością tworzenia użytkowników poza AD (np. technicznych).
4. Administratorzy muszą mieć możliwość przeglądu:
 - o listy użytkowników i ich uprawnień efektywnych,
 - o zdarzeń logowania,
 - o zdarzeń zmian konfiguracji logowania,
 - o utrwalonych zdarzeń w przeglądarce internetowej.
5. System musi logować zdarzenia działania (w tym błędy), odnotowywać modyfikacje danych biznesowych oraz umożliwiać wykonywanie kopii zapasowych danych w relacyjnej bazie danych.
6. System musi prezentować numer wersji oprogramowania w interfejsie webowym.
7. Wykonawca musi dostarczyć dokumentację administracyjną istotnych parametrów konfiguracyjnych.
8. Zarządzanie użytkownikami musi obejmować: listę uprawnień elementarnych, tworzenie grup, nadawanie uprawnień grupą lub elementarnie, dodawanie/modyfikację/usuwanie użytkowników, powiązanie użytkowników HIS z użytkownikami Systemu, integrację z AD.

7. Wymagania techniczne i środowiskowe

1. System musi być uruchamialny na architekturze Intel64/AMD64.
2. Serwer aplikacji i baza danych: Linux (Debian), Docker.
3. Stacje robocze: system operacyjny i przeglądarka zgodne z wymaganiami AMMS; Windows zgodny z AMMS.
4. Minimalna infrastruktura serwerowa: x86-64 Intel/AMD, 8 vCPU, 32 GB RAM, 1 TB HDD.
5. Wymagany skaner kodów kreskowych obsługujący ISBT 128.
6. Komunikacja HTTP musi być realizowana po HTTPS (SSL), z możliwością użycia certyfikatu dostarczonego przez Zamawiającego.
7. Środowisko musi znajdować się w sieci wewnętrznej Szpitala; użytkownicy łączą się siecią lokalną lub równoważną.
8. Serwer (VM) musi mieć dostęp sieciowy co najmniej do:
 - o repozytorium producenta (instalacja/aktualizacje),
 - o HIS/AMMS (wymiana danych),
 - o Internetu (aktualizacje systemu i bibliotek),
 - o systemów CeZ (integracja e-Krew).

8. Warunki uruchomienia i licencjonowanie

1. Minimalna wersja AMMS: 6.10.00.62.
2. Wymagany pakiet licencji: AMMS – Bank Krwi, Serologia i Integracja z e-Krew.
3. Dla klientów posiadających wcześniej rozwiązania: wymagany upgrade Banku Krwi, Serologii i integracji z e-Krew.
4. Klucze licencyjne:
 - o NBK_BANKKRWI
 - o NBK_SEROLOGIA

- NBK_EKREW

9. Wymagania organizacyjne i wdrożeniowe

9.1. Działania przygotowawcze

Zamawiający/Wykonawca (zgodnie z podziałem odpowiedzialności w umowie) zapewni m.in.:

- zgłoszenie do właściwego RCKiK w celu uzyskania dostępu do e-Krew,
- przygotowanie serwera Linux/Docker zgodnie z wymaganiami,
- zapewnienie łączności serwera Systemu z AMMS,
- instalację serwera licencji,
- zapewnienie wymaganej wersji AMMS w produkcji,
- konfigurację EDM (system i użytkownik dla Serologii),
- definicję procesów nadawczo-odbiorczych oraz weryfikację HL7 i JMS,
- konsultacje z dostawcą analizatora w zakresie dostępu do integracji.

9.2. Prace wdrożeniowe – po stronie HIS/AMMS

W ramach prac po stronie HIS/AMMS przewiduje się w szczególności:

- parametryzację systemów zewnętrznych dla Nowego Banku Krwi i Serologii,
- definicję JOS dla pracowni serologii i JOSów zlecających/przyjmujących/wykonujących,
- konfigurację elementów leczenia (przetoczenia, badania) i słowników składników,
- konfigurację EDM i procesów integracyjnych,
- instalację/konfigurację serwera licencji (jeśli wymagane),
- szkolenia dla personelu oddziałowego (zamówienia krwi, zlecenia badań, ewidencja przetoczeń).

9.3. Prace wdrożeniowe – po stronie serwera Systemu (Linux)

Wykonawca zapewni m.in.:

- instalację Systemu na wskazanym serwerze,
- konfigurację integracji z AMMS (zamówienia, badania, dane pacjentów, odsyłanie wyników i wydań),
- inicjalne zasilenie słownika personelu,
- konfigurację słowników i parametrów (w tym baza składników ISBT),
- instalację sterownika integracji z analizatorem (pod warunkiem dostępu),
- uruchomienie integracji e-Krew (zamówienia, badania konsultacyjne) – po uzyskaniu uprawnień RCKiK,
- szkolenia zdalne: Bank Krwi i Serologia oraz administratorzy IT (uprawnienia, backup, aktualizacje).

10. Kryteria odbioru (testy akceptacyjne)

Produkt zostanie uznany za zgodny funkcjonalnie i gotowy do pracy produkcyjnej, jeśli co najmniej:

1. Zostanie wykonane kontekstowe przejście z HIS do Banku Krwi i Serologii bez ponownego logowania.
2. Zamówienie na składnik krwi z HIS zostanie zarejestrowane i wyświetlone w Banku Krwi dla pacjenta: z PESEL, NN i obcokrajowca.
3. Zamówienie pilne i normalne zostanie zrealizowane przez rezerwację skanerem, a wydanie zostanie poprawnie zarejestrowane w HIS przy właściwym pacjencie.
4. Dostawa składników zostanie przyjęta skanerem i zarejestrowana na wskazanym magazynie, a dokument przyjęcia zostanie wygenerowany.
5. Zamówienie zbiorcze do RCKiK zostanie wprowadzone, a raport PDF odpowiadający zamówieniu zostanie wygenerowany.

6. Utylizacja składnika zostanie wprowadzona, zatwierdzona i zostanie wygenerowany raport utylizacji PDF.
7. Zwrot składnika zostanie odnotowany, zatwierdzony, a składnik wróci na stan magazynowy.
8. Zlecenie badania grupy krwi z HIS zostanie zarejestrowane w Serologii wraz z założeniem kartoteki (PESEL/NN/obcokrajowiec).
9. Badanie próby krzyżowej zostanie obsłużone, wynik zostanie przesłany do HIS oraz zostanie wydrukowany wynik próby zgodności.
10. Próbką zostanie wprowadzona skanerem wraz z datą dostarczenia i będzie poprawnie widoczna w podglądzie.
11. Zostanie obsłużony proces badania grupy krwi (wynik potwierdzony) wraz z przekazaniem wyniku do HIS.
12. Będzie możliwe dopisanie badań konsultacyjnych do protokołu, poprawna prezentacja danych w protokole oraz na wydruku.

4.9. Integracja z analizatorem serologicznym

1. Przedmiot zamówienia

Przedmiotem zamówienia jest dostawa, uruchomienie oraz konfiguracja interfejsu integracyjnego zapewniającego współpracę systemu Zamawiającego (modułu Serologii / LIS lub równoważnego) z posiadanym przez Zamawiającego analizatorem serologicznym DIAHEM IH500, w zakresie:

- przekazywania do analizatora danych demograficznych pacjenta oraz zleconych badań,
- odbioru z analizatora wyników badań wraz z protokołami i zapisania ich w systemie Zamawiającego.

Integracja ma umożliwiać automatyzację procesu zlecenia i rejestrowania wyników badań serologicznych wykonywanych na analizatorze.

2. Zakres integracji (wymagania funkcjonalne)

2.1. Wysyłanie danych do analizatora

1. Interfejs musi umożliwiać wysyłanie do analizatora DIAHEM IH500 danych demograficznych pacjenta, obejmujących co najmniej:
 - imię i nazwisko,
 - identyfikator pacjenta w systemie Zamawiającego,
 - PESEL (lub inny identyfikator zgodny z przepisami, jeżeli PESEL nie występuje),
 - datę urodzenia,
 - płeć.
2. Interfejs musi umożliwiać wysyłanie zleconych badań do analizatora, w szczególności wraz z identyfikatorem zlecenia/badania oraz powiązaniem z pacjentem.
3. Interfejs musi zapewniać, że dane pacjenta i zlecenia są przekazywane w sposób umożliwiający ich jednoznaczną identyfikację w analizatorze oraz późniejsze powiązanie wyników z właściwym pacjentem i zleceniem w systemie Zamawiającego.

2.2. Odbiór wyników z analizatora

1. Interfejs musi umożliwiać automatyczny odbiór wyników badań wykonanych na analizatorze DIAHEM IH500.
2. Odbierane dane muszą obejmować wyniki wraz z protokołem/protokołami badań przekazywanymi przez analizator (w zakresie udostępnianym przez urządzenie).
3. System musi umożliwiać zapis odebranych wyników do właściwego zlecenia i pacjenta w systemie Zamawiającego.

2.3. Obsługa spójności i statusów

1. Interfejs musi zapewniać obsługę co najmniej następujących scenariuszy:
 - o brak zgodności danych pacjenta lub zlecenia (np. brak identyfikatora w systemie),
 - o zdublowane wyniki / ponowna wysyłka tego samego wyniku,
 - o przerwanie komunikacji i ponowna synchronizacja po przywróceniu łączności.
2. Interfejs powinien umożliwiać śledzenie statusu wymiany danych (wysłane / przyjęte / błąd) dla zleceń przekazanych do analizatora oraz wyników odebranych z analizatora.

3. Wymagania techniczne (minimalne)

1. Integracja musi działać z analizatorem DIAHEM IH500 posiadanym przez Zamawiającego.
2. Interfejs musi wykorzystywać protokół komunikacyjny dostępny dla tego urządzenia (np. wg dokumentacji producenta analizatora) oraz umożliwiać konfigurację parametrów komunikacyjnych.
3. Po stronie Wykonawcy wymagane jest uruchomienie i konfiguracja integracji w środowisku Zamawiającego, w tym zapewnienie poprawnego mapowania badań (kody badań) pomiędzy systemem Zamawiającego a analizatorem.

Warunek: Zamawiający zapewni fizyczny i sieciowy dostęp do analizatora oraz niezbędne informacje konfiguracyjne/protokolarne udostępniane przez producenta lub serwis urządzenia.

4. Wymagania dotyczące testów i odbioru

Integracja zostanie uznana za odebraną, jeżeli zostaną spełnione łącznie następujące warunki (kryteria odbioru minimalne):

1. Z systemu Zamawiającego zostaną wysłane do analizatora DIAHEM IH500 dane pacjenta oraz zlecone badania dla co najmniej 3 przypadków: pacjent z PESEL, pacjent NN / bez PESEL, pacjent obcokrajowiec (identyfikator alternatywny).
2. Analizator przyjmie zlecenie i wykona badania, a wyniki zostaną automatycznie odebrane przez interfejs.
3. Otrzymane wyniki wraz z protokołem zostaną poprawnie przypisane do właściwego pacjenta i właściwego zlecenia w systemie Zamawiającego.
4. W przypadku symulacji błędu komunikacji (np. czasowe rozłączenie) interfejs zapewni ponowienie transmisji/odbioru oraz brak utraty danych.

5. Dokumentacja i utrzymanie

1. Wykonawca dostarczy dokumentację powdrożeniową obejmującą:
 - o opis konfiguracji integracji,
 - o mapowanie badań (kody system ↔ kody analizatora),
 - o opis logów i sposobu diagnostyki problemów komunikacyjnych.
2. Interfejs musi zapewniać logowanie zdarzeń integracyjnych (wysyłki/odbior/błędy) umożliwiające analizę incydentów.

4.10. WDSZ - Integracja z systemem digitalizacji dokumentacji

1. Przedmiot zamówienia

Przedmiotem zamówienia jest integracja systemu WDSZ (Wewnętrzny/Dedykowany System Zarządzania dokumentacją) z systemem digitalizacji dokumentacji medycznej oraz repozytorium Elektronicznej Dokumentacji Medycznej (EDM), realizowana w oparciu o udostępnione interfejsy programistyczne (API).

Celem integracji jest zapewnienie spójnego, bezpiecznego i automatycznego przepływu danych pomiędzy systemem medycznym, systemem skanowania dokumentów oraz repozytorium EDM.

2. Zakres integracji

Integracja realizowana będzie w modelu komunikacji system–system poprzez API, obejmującym:

2.1. Dane udostępniane przez system medyczny

System medyczny udostępnia poprzez API następujące dane:

- Dane dotyczące pobytu pacjenta:
 - identyfikator pobytu,
 - numer pobytu;
- Dane personelu medycznego wykorzystywane do:
 - identyfikacji osoby skanującej dokument,
 - identyfikacji osoby autoryzującej kopię elektroniczną dokumentu;
- Dane pacjenta:
 - numer PESEL,
 - identyfikator pacjenta w systemie medycznym,
 - imię,
 - nazwisko.

2.2. Dane przekazywane przez system digitalizacji do repozytorium EDM

System digitalizacji dokumentacji przekazuje do repozytorium EDM:

- Elektroniczny obraz zeskanowanego dokumentu, w postaci pliku cyfrowego;
- Atrybuty dokumentu, w tym:
 - identyfikator pracownika autoryzującego skan;
- Dane indeksowe dokumentu, obejmujące:
 - identyfikator pacjenta,
 - identyfikator pobytu.

3. Wymagania funkcjonalne

W ramach realizacji przedmiotu zamówienia Wykonawca zapewni:

1. Poprawną i dwukierunkową komunikację pomiędzy systemem WDSZ, systemem medycznym oraz systemem digitalizacji dokumentów.
2. Automatyczne przypisywanie zeskanowanej dokumentacji do właściwego pacjenta i pobytu na podstawie danych indeksowych.
3. Możliwość jednoznacznej identyfikacji osoby skanującej oraz autoryzującej dokument.
4. Zapewnienie integralności i kompletności danych przesyłanych pomiędzy systemami.
5. Obsługę błędów integracyjnych oraz mechanizmów ponawiania transmisji danych.

4. Wymagania techniczne

1. Integracja musi być realizowana w oparciu o udostępnione API, zgodnie z dokumentacją techniczną Zamawiającego.
2. Komunikacja pomiędzy systemami powinna być zabezpieczona (np. szyfrowanie transmisji, autoryzacja dostępu).
3. Rozwiązanie musi być zgodne z obowiązującymi przepisami prawa, w szczególności:
 - ustawą o systemie informacji w ochronie zdrowia,
 - przepisami RODO,
 - przepisami dotyczącymi EDM.

5. Wymagania organizacyjne

Wykonawca zobowiązany jest do:

1. Przeprowadzenia testów integracyjnych przed uruchomieniem produkcyjnym.
2. Wsparcia Zamawiającego w procesie uruchomienia integracji.
3. Przekazania dokumentacji powdrożeniowej obejmującej opis integracji i wykorzystywanych interfejsów.

4.11. WDSZ - Integracja z ICPen

1. Przedmiot zamówienia

Przedmiotem zamówienia jest integracja systemu WDSZ z rozwiązaniem ICPen, umożliwiającą obsługę dokumentów medycznych wypełnianych odręcznie przy użyciu elektronicznego długopisu, z zachowaniem pełnej integracji z systemem HIS.

Celem integracji jest zapewnienie ciągłości procesu tworzenia, wypełniania, walidacji oraz zapisu dokumentacji medycznej w systemie HIS, z wykorzystaniem elektronicznego długopisu oraz obsługi dokumentów w postaci elektronicznej.

2. Zakres integracji

Integracja obejmuje współpracę pomiędzy systemem HIS, systemem WDSZ oraz rozwiązaniem ICPen w zakresie:

- generowania dokumentów gotowych do odręcznego wypełnienia,
- obsługi elektronicznego długopisu,
- prezentacji dokumentów w formacie PDF,
- zapisu danych odręcznych w bazie danych systemu HIS.

3. Wymagania funkcjonalne

3.1. Generowanie i druk dokumentów

1. System musi umożliwiać integrację z systemem HIS, pozwalającą na wydruk dokumentu z poziomu HIS, przeznaczonego do odręcznego wypełnienia za pomocą elektronicznego długopisu.
2. Na generowanym dokumencie musi istnieć możliwość nadrukowania dowolnych danych dostępnych w szablonach pism systemu HIS, w szczególności:
 - danych osobowych pacjenta,
 - danych dotyczących pobytu,
 - danych jednostki organizacyjnej, w której przebywa pacjent.

3.2. Obsługa dokumentów PDF

1. Integracja powinna umożliwiać podgląd wypełnionego dokumentu w postaci pliku PDF bezpośrednio w systemie HIS.
2. System HIS musi umożliwiać podgląd dokumentu PDF przed jego wystaniem do dalszego przetwarzania.

3.3. Obsługa elektronicznego długopisu i walidacja danych

1. System musi umożliwiać przesłanie:
 - dokumentu wydrukowanego z HIS,
 - dokumentu wypełnionego odręcznie przy użyciu elektronicznego długopisu do aplikacji skanującej dane z elektronicznego długopisu.
2. Po wykonaniu wstępnej walidacji dokument powinien zostać przesłany do systemu HIS.
3. System musi umożliwiać zapis w bazie danych systemu HIS danych wypełnionych pismem odręcznym dla dedykowanych dokumentów.

3.4. Elektroniczne wypełnianie formularzy

1. Integracja powinna umożliwiać przesyłanie formularzy z HIS do systemu umożliwiającego elektroniczne wypełnianie dokumentacji.
2. Przekazanie formularza musi odbywać się wraz z informacją o wyborze urzędnika, na którym dokument będzie wypełniany.
3. System HIS przed wystaniem formularza musi umożliwiać wybór urzędnika elektronicznego ze słownika.

3.5. Konfiguracja urządzeń i szablonów

1. System HIS musi umożliwiać:
 - o konfigurację słownika listy urządzeń zewnętrznych wykorzystywanych do podpisu elektronicznego,
 - o zarządzanie listą dostępnych urządzeń w sposób administracyjny.
2. System HIS musi umożliwiać zdefiniowanie szablonów pism, które mogą być:
 - o wypełniane odręcznie za pomocą elektronicznego długopisu,
 - o wypełniane elektronicznie w ramach integracji z ICPen.

4. Wymagania niefunkcjonalne

1. System musi oferować elastyczną konfigurację integracji, umożliwiającą jej dostosowanie do indywidualnych potrzeb Zamawiającego.
2. Integracja powinna zapewniać:
 - o integralność danych,
 - o jednoznaczne przypisanie dokumentów do pacjenta i pobytu,
 - o zgodność z obowiązującymi przepisami prawa, w szczególności dotyczącymi dokumentacji medycznej i ochrony danych osobowych.
3. Komunikacja pomiędzy systemami powinna być zabezpieczona przed nieautoryzowanym dostępem.

5. Wymagania wdrożeniowe

Wykonawca zobowiązany jest do:

1. Przeprowadzenia testów integracyjnych przed uruchomieniem produkcyjnym.
2. Zapewnienia wsparcia w procesie uruchomienia rozwiązania.
3. Dostarczenia dokumentacji powdrożeniowej obejmującej opis integracji oraz konfiguracji systemu.

5. Licencja Oracle lub równoważna – 1 sztuka

Przedmiotem zamówienia jest dostawa licencji Oracle Database Standard Edition 2 dla Oracle Database 19c lub równoważnej (dalej: „System bazodanowy”) wraz z zapewnieniem prawa do korzystania z aktualizacji i wsparcia producenta w minimalnym zakresie określonym w niniejszym

Wymagania:

1. Wykonawca dostarczy 1 szt. licencji Systemu bazodanowego.
2. Licencje muszą umożliwiać uruchomienie i eksploatację Systemu bazodanowego w środowisku Zamawiającego w sposób zgodny z wymaganiami wskazanymi w niniejszym OPZ.
3. Oferowany silnik bazy danych musi być dostępny co najmniej dla platform systemów operacyjnych Windows oraz Linux.

4. Oferowany silnik bazy danych dla systemu HIS musi posiadać możliwość rozbudowy do wersji wspierającej synchroniczną replikację danych w dwóch niezależnych centrach danych.
5. Oferowany silnik bazy danych musi posiadać komercyjne wsparcie producenta; nie dopuszcza się zastosowania rozwiązań typu RDBMS open source.
6. Silnik bazy danych musi posiadać możliwość realizacji kopii bezpieczeństwa w trakcie działania (hot backup).
7. Silnik bazy danych musi umożliwiać wykonywanie kopii bezpieczeństwa:
 - a. automatycznie (o określonej porze),
 - b. na żądanie operatora
8. Silnik bazy danych musi umożliwiać odtwarzanie bazy danych z kopii archiwalnej, w tym sprzed awarii.
9. Silnik bazy danych musi umożliwiać eksport i import danych w formacie tekstowym z uwzględnieniem polskiego standardu znaków.
10. System musi wspierać
 - a. wiele ustawień narodowych oraz wiele zestawów znaków (w tym Unicode),
 - b. migrację zestawu znaków bazy danych do Unicode,
 - c. redefiniowanie ustawień narodowych (symbole walut, format dat, porządek sortowania) z użyciem narzędzi graficznych.
11. System musi zapewniać wsparcie dla architektury trójwarstwowej, w tym:
 - a. możliwość uruchomienia wielu sesji bazy danych przy wykorzystaniu jednego połączenia z serwera aplikacyjnego do serwera bazy danych,
 - b. możliwość otworzenia wielu aktywnych zbiorów rezultatów w jednej sesji bazy danych.
12. System musi wspierać protokoły i standardy:
 - a. XA,
 - b. JDBC 3.0,
 - c. zgodność ze standardem ANSI/ISO SQL 2003 lub nowszym.
13. System musi umożliwiać wpływ na optymalizację zapytań SQL poprzez:
 - a. parametry konfiguracyjne pracy serwera,
 - b. wskazówki (hints) w instrukcjach SQL.
14. System nie może wprowadzać formalnych ograniczeń co do:
 - a. liczby tabel i indeksów,
 - b. rozmiaru tabel i indeksów (liczby wierszy).
15. Silnik bazy danych musi wspierać procedury i funkcje składowane w języku proceduralnym, blokowym, z obsługą wyjątków i ich propagacją do bloku nadrzędnego lub jednostki wywołującej.
16. Procedury i funkcje składowane muszą umożliwiać:
 - a. parametry proste oraz złożone typy definiowane przez użytkownika,
 - b. zwracanie zbiorów danych możliwych do użycia jako źródło danych w SQL (we frazie FROM),
 - c. wykonywanie instrukcji SQL (DML, DDL, zapytania),
 - d. jednoczesne otwarcie wielu kursorów pobierających paczki danych,
 - e. obsługę mechanizmów transakcyjnych (commit/rollback).
17. System musi umożliwiać kompilację procedur składowanych do postaci kodu binarnego (biblioteki dzielonej).
18. System musi umożliwiać deklarowanie wyzwalaczy (triggerów):
 - a. na poziomie instrukcji DML,
 - b. na poziomie wiersza,
 - c. na poziomie zdarzeń bazy danych (m.in. logowanie użytkownika, start/stop serwera, próba wykonania DDL, specyficzny błąd),
19. System musi zapewniać możliwość obsługi DML na niemodyfikowalnych widokach.

20. W przypadku błędu w wyzwalaczu dla instrukcji DML, wykonywana instrukcja DML musi zostać automatycznie wycofana, a stan transakcji ma odpowiadać stanowi sprzed rozpoczęcia tej instrukcji.
21. System musi posiadać wbudowaną obsługę wyrażeń regularnych zgodną ze standardem POSIX, dostępną z poziomu SQL oraz procedur/funkcji składowanych.
22. Administrator musi mieć możliwość wyboru danych monitorowanych w logach systemu z dokładnością do poszczególnych kolumn w tabelach danych; zarządzanie logami może odbywać się z poziomu narzędzi do zarządzania bazami danych (dopuszcza się narzędzie na poziomie silnika bazy danych).
23. Hasła użytkowników muszą być przechowywane w bazie danych w postaci niejawnej (zaszyfrowanej).
24. System musi umożliwiać autoryzowanie użytkowników bazodanowych w oparciu o rejestr użytkowników założony w bazie danych.
25. System musi umożliwiać polityki haseł, w tym co najmniej:
 - a. wymuszanie złożoności hasła,
 - b. czas życia hasła,
 - c. historię haseł,
 - d. blokowanie konta przez administratora,
 - e. automatyczne blokowanie konta po przekroczeniu limitu nieudanych logowań.
26. System musi umożliwiać nadawanie uprawnień:
 - a. systemowych (np. tworzenie sesji, tworzenie obiektów),
 - b. do obiektów aplikacyjnych (np. SELECT/INSERT/UPDATE/DELETE, EXECUTE),
 - c. z użyciem mechanizmu ról/grup, przy czym użytkownik może mieć aktywny dowolny podzbiór nadanych ról.
27. System musi umożliwiać wykonywanie i katalogowanie kopii bezpieczeństwa bezpośrednio przez serwer bazy danych.
28. System musi umożliwiać zautomatyzowane usuwanie zbędnych kopii przy zachowaniu polityki nadmiarowości (retencji).
29. System musi umożliwiać integrację z powszechnie stosowanymi systemami backupu (np. Legato, Veritas, Tivoli, OmniBack, ArcServe lub równoważnymi).
30. Wykonywanie kopii musi być możliwe w trybie:
 - a. offline,
 - b. online (hot backup).
31. Odtwarzanie musi umożliwiać:
 - a. odzyskanie stanu danych z chwili awarii,
 - b. odtworzenie do punktu w czasie (point-in-time recovery),
 - c. odtwarzanie całej bazy lub pojedynczych plików danych.
32. W przypadku odtwarzania pojedynczych plików danych, pozostałe pliki bazy danych mogą być dostępne dla użytkowników.
33. Oprogramowanie musi być dostępne na współczesne 64-bitowe platformy Unix, w tym co najmniej:
 - a. HP-UX (PA-RISC i Itanium),
 - b. Solaris (SPARC i Intel/AMD),
 - c. IBM AIX,oraz na:
 - d. Intel/AMD Linux 32-bit i 64-bit,
 - e. MS Windows 32-bit i 64-bit,przy zachowaniu identycznej funkcjonalności serwera bazy danych na ww. platformach.
34. Wymagana jest niezależność platformy systemowej dla oprogramowania klienckiego/serwera aplikacyjnego od platformy systemowej bazy danych.
35. Wymagana jest możliwość migracji struktur bazy danych i danych pomiędzy ww. platformami bez konieczności rekompilacji aplikacji lub migracji środowiska aplikacyjnego.

36. System musi zapewniać możliwość zagnieżdżania transakcji, tj. uruchomienia niezależnej transakcji wewnątrz transakcji nadrzędnej, w tym w scenariuszach audytowych (np. rejestr operacji w tabeli dziennika niezależnie od zatwierdzenia lub wycofania transakcji nadrzędnej).
37. Wykonawca zapewni wsparcie producenta obejmujące co najmniej prawo do otrzymywania bezpłatnych aktualizacji przez minimum 36 miesięcy.

Część II – Upgrade posiadanego systemu PACS/RIS wraz z integracją z PUI

1. Upgrade posiadanego systemu PACS/RIS wraz z integracją z PUI

1. Przedmiot zamówienia

1. Przedmiotem zamówienia jest rozbudowa i upgrade posiadanego przez Zamawiającego systemu PACS/RIS poprzez:
 1. wykonanie upgrade'u posiadanego systemu RIS/PACS wraz z wdrożeniem dodatkowych funkcjonalności,
 2. rozszerzenie systemu o moduł opisywania badań radiologicznych wspomagany przez LLM wraz z czasową licencją transkrypcji opisów na okres 36 miesięcy (limit 10 000 badań rocznie),
 3. rozszerzenie integracji PACS/RIS o połączenie z Platformą Usług Inteligentnych (PUI) w standardach HL7 / FHIR, w tym pełny obieg danych obrazowych DICOM oraz wyników analiz,
 4. zapewnienie gwarancji i wsparcia przez 36 miesięcy dla integracji z PUI oraz zmian wprowadzonych w systemie w ramach integracji.
2. Zamówienie obejmuje w szczególności: dostawę/licencjonowanie oprogramowania, prace wdrożeniowe, migrację danych, konfigurację integracji, testy, szkolenia, dokumentację powdrożeniową oraz serwis.

2. Zakres realizacji (minimalny)

Wykonawca zobowiązany jest do realizacji co najmniej następujących elementów:

2.1. Upgrade RIS/PACS

- Upgrade posiadanego systemu RIS/PACS do wersji umożliwiającej realizację wymagań funkcjonalnych i нефunkcjonalnych opisanych w OPZ.
- Wdrożenie obejmuje instalację, uruchomienie oraz przekazanie do użytkownika.

2.2. Moduł opisywania badań radiologicznych z LLM + transkrypcja (36 miesięcy)

- Dostawa i uruchomienie modułu opisywania badań wraz z mechanizmem dyktowania i generowania opisu przez LLM.
- Udzielenie licencji czasowej na 36 miesięcy, umożliwiającej wykonanie 10 000 opisów rocznie (łącznie 30 000 opisów w okresie 36 miesięcy), liczone od podpisania protokołu odbioru.

2.3. Integracja z HIS oraz integracja z PUI

- Zapewnienie pełnej integracji RIS/VNA/PACS z systemem HIS po HL7/FHIR.
- Zapewnienie integracji z PUI w standardach HL7/FHIR, obejmującej:
 - wysyłanie obrazów DICOM do PUI,
 - wysyłanie kompletnych metadanych DICOM,
 - odbiór wyników analiz, danych przetworzonych i obrazów z oznaczeniami patologii,
 - prezentację wyników i ich włączenie do procesu diagnostycznego oraz do RIS.

2.4. Migracja danych

- Migracja danych RIS do nowego środowiska.
- Migracja danych PACS do VNA/RIS (archiwum obrazowe) z zachowaniem integralności danych.

2.5. Szkolenia

- Przeprowadzenie szkoleń dla personelu medycznego i technicznego (dopuszczalne szkolenia online).

2.6. Gwarancja i wsparcie

- 36 miesięcy gwarancji/serwisu i nadzoru autorskiego dla integracji PUI oraz zmian wprowadzonych w systemie w tym zakresie.

3. Wymagania ogólne bezpieczeństwa i rozliczalności

1. System musi zapewniać mechanizmy autoryzacji i skuteczne zabezpieczenia przed nieautoryzowanym dostępem na poziomie aplikacji klienckiej oraz serwera bazy danych.
2. System musi zapewniać pełną rozliczalność działań użytkowników poprzez rejestrowanie i ewidencjonowanie wszystkich operacji (w tym prób dostępu) wykonywanych zarówno z poziomu aplikacji, jak i narzędzi serwera bazy danych (logi/dzienniki zdarzeń).
3. Całość komunikacji pomiędzy serwerami i stacjami roboczymi musi być szyfrowana co najmniej protokołem TLS.

4. Wymagania architektury i utrzymania (konteneryzacja, aktualizacje, administracja)

1. Rozwiązanie musi być w pełni separowane od systemu operacyjnego, a każdy moduł systemu musi być skonteneryzowany w technologii Docker, w celu zapewnienia wysokiego poziomu bezpieczeństwa zgodnie z NIST SP 800-190 – tak, aby kompromitacja jednego serwisu nie umożliwiała przejęcia kontroli nad pozostałymi.
2. Administrator musi mieć możliwość samodzielnej instalacji systemu VNA/RIS.
3. System musi umożliwiać swobodną aktualizację oprogramowania poprzez wybór nowej wersji i automatyczną aktualizację bez potrzeby wiedzy specjalistycznej.
4. System musi umożliwiać samodzielne instalowanie nowych modułów.
5. System musi zapewniać panel administracyjny WWW umożliwiający:
 - podgląd logów każdego kontenera,
 - uruchamianie i zatrzymywanie każdego kontenera.

5. Wymagania redundancji i kopii zapasowych

1. Rozwiązanie musi zapewniać pełną redundancję bazy danych oraz wykonywanie co najmniej raz dziennie kopii przyrostowej.
2. Użytkownik musi mieć możliwość samodzielnego uruchomienia kopiowania bazy danych i obrazów do bezpiecznego systemu chmurowego.
3. Rozwiązanie musi zapewniać pełną redundancję plików obrazowych w trybie „antymalware” – kopia na drugim serwerze musi być chroniona przed zaszyfrowaniem w przypadku zaszyfrowania kopii na pierwszym serwerze.

6. Wymagania producenta i spójności rozwiązania

1. Oprogramowanie VNA/RIS/PACS oraz integracja PUI muszą pochodzić od jednego producenta.

7. Wymagania dot. interfejsu i funkcjonalności RIS (WEB/PL/moduły)

1. Oprogramowanie musi działać w przeglądarkach: Chrome, Safari, Edge, Firefox.
2. Oprogramowanie musi działać w języku polskim.
3. System musi zawierać moduły: Rejestracja, Terminarz, Opisywanie badań, Technika, Raporty, Zarządzanie pacjentami, Zarządzanie badaniami.
4. System musi obsługiwać wiele jednostek organizacyjnych oraz przypisywanie użytkownika do jednostki.

5. System musi umożliwiać tworzenie wielu gabinetów dla każdej jednostki organizacyjnej.

7.1. Moduł Rejestracja – minimalne funkcje

System musi umożliwiać m.in.:

- wprowadzenie danych pacjenta: imię, nazwisko, data urodzenia, PESEL, paszport, nr dowodu,
- rejestrację w imieniu opiekuna/rodzica,
- telefon, e-mail,
- adres w oparciu o słownik ogólnokrajowy,
- nr karty diagnostycznej/kartoteki głównej,
- automatyczną weryfikację AP-Kolce,
- daty skierowania i dostarczenia,
- zlecenie wewnętrzne/zewnętrzne,
- oznaczanie: CITO, DILO, VIP, badanie kliniczne,
- płatnik: pacjent/ubezpieczyciel/NFZ/niedopłata,
- wybór badania/badań z badaniem głównym,
- ustawienie czy badanie ma posiadać opis,
- ICD9,
- dane dodatkowe: waga, wzrost, kreatynina, GFR, glukoza,
- informację o ciałach metalowych.

7.2. Moduł Terminarz – minimalne funkcje

System musi umożliwiać m.in.:

- rejestrację do wielu jednostek/gabinetów jednocześnie,
- wyszukiwanie pierwszego wolnego terminu po rodzaju badania z podaniem 3 najbliższych,
- terminarz w slotach czasowych,
- rezerwację slotu, potwierdzenie, edycję, usuwanie,
- rejestrację z e-skierowania i PIN,
- przenoszenie na inny dzień,
- historię rezerwacji,
- wsparcie call center i notatki dla kolejnej zmiany.

7.3. Moduł Technika – minimalne funkcje

System musi umożliwiać m.in.:

- podgląd poprzednich badań web do przygotowania,
- wprowadzanie detali procedury (osoby, wklucie, znieczulenie, dyżur),
- dane techniczne (fazy/projekcje/protokół/DLP/DAP/CTDI/dawka), kontrast, kratki,
- dodanie dodatkowej procedury,
- skanowanie dokumentów do badania,
- wskazanie osoby autoryzującej,
- uwagi do radiologa.

7.4. Moduł Opisywania badań – minimalne funkcje

System musi umożliwiać m.in.:

- listę badań do opisu i konfigurowalne kolumny,
- udostępnianie badań do opisu (wewnątrz/na zewnątrz) na e-mail,
- prezentowanie badań z innych placówek (konsultacje/opisy),
- zasilanie listy roboczej z RIS/HIS/dowolnego PACS,
- podłączenie dowolnego PACS i automatyczne tworzenie zleceń opisu na podstawie danych PACS,
- teleradiologię z domu, w tym:
 - pobranie oprogramowania teleradiologii i automatyczny transfer badań,

- informowanie o nowej wersji i aktualizacji,
- ładowanie badań <10 s dla badań 400 sliców w MPR z użyciem serwera szpitalnego,
- brak przechowywania DICOM po stronie klienta (bezpieczeństwo).

8. Moduł opisywania z AI/LLM i transkrypcją – wymagania szczegółowe

1. Rozwiązanie działa w przeglądarce WWW i nie wymaga instalacji na stacji użytkownika.
2. Umożliwia jednym kliknięciem otwarcie badania w oprogramowaniu firm typu Siemens/Osiris.
3. Obsługuje cyfrowe podpisy opisów certyfikatem ZUS, w tym:
 - samodzielne wgranie certyfikatu przez użytkownika,
 - prezentację wyniku przed podpisem,
 - możliwość bezpiecznego zapisania hasła do certyfikatu.
4. Opis badania zapisywany jest w RIS.
5. Rozwiązanie współpracuje z dowolnym mikrofonem kierunkowym i zapewnia automatyczną transkrypcję mowy do tekstu.
6. Integracja z modułem opisowym Zamawiającego musi zapewniać:
 - automatyczną aktywację dyktowania po wejściu w tryb opisu,
 - wprowadzanie dyktowanego tekstu do pola „brudnopis” z podglądem na bieżąco,
 - po zakończeniu dyktowania procedurę przeniesienia do „czystego opisu”,
 - wybór protokołu opisowego i generowanie kompletnego opisu przez LLM.
7. Dopasowanie do stylu radiologa:
 - możliwość odczytu poprzednich opisów danego lekarza z RIS i tworzenie wzorca stylu.
8. Automatyczna poprawa jakości tekstu:
 - korekta literówek,
 - korekta błędów w wypowiedzi do słownika medycznego,
 - usuwanie fragmentów konwersacyjnych niezwiązanych z badaniem.
9. Moduł administracyjny musi umożliwiać:
 - włączanie/wyłączanie dyktowania dla użytkowników,
 - statystyki użycia i liczby podyktowanych/wykonanych/opisanych badań,
 - statystyki czasu opisu (średni/min/max/mediana).

9. Wymagania dot. zarządzania pacjentami, badaniami i raportami

Zarządzanie pacjentem: lista pacjentów, edycja danych, łączenie pacjentów, przejście do listy badań.

Zarządzanie badaniami: lista badań zgodnie z uprawnieniami, wydawanie wyników, szczegóły, edycja, dodanie nowego badania do wykonanego, dołączanie skanów, anulowanie, oznaczenie wykonania, wydruk informacji.

Raporty: min. 100 raportów, dostęp wg uprawnień, harmonogramowanie, tworzenie własnych raportów, centralne repozytorium raportów do współdzielenia.

10. Wymagania VNA/PACS – MDR, DICOM, kompresja, MWL, warstwy storage

1. Całość zaoferowanego modułu (VNA) musi być dostarczona jako wyrób medyczny klasy IIb zgodnie z MDR (UE) 2017/745 i posiadać ważny certyfikat MDR.
2. System musi archiwizować wszystkie dane obrazowe z urządzeń diagnostycznych w formacie DICOM z zastosowaniem kompresji bezstratnej (np. JPEG2000 Lossless) bez utraty informacji, zarówno w archiwum on-line, jak i kopii zapasowej.

3. System musi umożliwiać określenie rodzaju kompresji per modalność (brak kompresji / JPEG2000 bezstratna).
4. System musi wspierać listę roboczą MWL (DICOM Modality WorkList) oraz konfigurację per aparat, z filtrami min.: data zlecenia, oddział kierujący, pracownia, AETitle.
5. Dane obrazowe muszą być składowane na macierzach ONLINE (SSD), z automatycznym przenoszeniem na NEARLINE po czasie lub po zajęciu objętości.
6. System musi mieć wbudowane mechanizmy HL7/FHIR i być w pełni zintegrowany z RIS.
7. System musi wspierać wymagane klasy SOP SCU/SCP oraz Transfer Syntax wskazane w wymaganiach Zamawiającego (zgodnie z listą w OPZ – stanowi wymaganie minimalne).
8. System musi umożliwiać nagrywanie płyt CD/DVD na wskazanych stacjach roboczych, z wyborem badań, dołączeniem opisu (w tym SR i adnotacji) oraz przeglądarką DICOM na nośniku.
9. System musi tworzyć logi dla wszystkich usług PACS min. w zakresie: import, autorouting, admin, MWL, HL7, kopie DICOM, dystrybucja.
10. System musi umożliwiać wyszukiwanie badań archiwalnych wg kryteriów pacjenta/badania/administracyjnych oraz zarządzanie AETitle.
11. System musi umożliwiać DICOM C-STORE/C-MOVE do innych węzłów, w tym wysyłki grupowe na wiele węzłów w jednym zadaniu.
12. System musi umożliwiać modyfikację danych pacjenta i badania w archiwum (zmiany w bazie danych, a DICOM aktualizowany przy eksporcie/wysyłce) co najmniej w zakresie wymaganym w OPZ.

11. Monitoring

1. System musi być monitorowany przez otwarte rozwiązanie typu Zabbix lub Prometheus.
2. Monitoring minimalnie obejmuje: CPU/RAM/GPU, IOPS, RAID, sieć, stan serwisów VNA/RIS/dystrybucji, stan backupu.

12. Integracja z PUI – wymagania szczegółowe

1. Podłączenie systemu do serwisu PUI nastąpi do 60 dni od ogłoszenia gotowości CEZ; Zamawiający współpracuje z Wykonawcą w zakresie przekazania niezbędnych informacji.
2. System musi automatycznie przysyłać badania do PUI z kompletnymi metadanymi DICOM (m.in. grubość serii, protokoły, pixel spacing, kontrast i fazy).
3. System musi automatycznie identyfikować i transmitować wybrane serie badań na podstawie nazwy, grubości warstw i protokołu badania.
4. Zamawiający musi mieć możliwość decydowania i kontrolowania, które dane są przysyłane do PUI.
5. Integracja musi obejmować:
 - wysyłanie DICOM do PUI,
 - odbiór wyników analiz i obrazów z oznaczeniami patologii,
 - zapewnienie spójnej prezentacji wyników w przeglądarce radiologicznej i integracji z RIS.
6. System musi zawierać mechanizmy zapobiegające błędnemu przypisaniu obrazów przy przenoszeniu badań między pacjentami (integralność danych pacjenta).
7. System musi posiadać mechanizm kontroli jakości udostępniania wyników pacjentom (CD/DVD/portal pacjenta) dopiero po akceptacji radiologa – pacjent widzi tylko zaakceptowane wyniki AI.
8. Wymagana jest konfigurowalna integracja z platformami teleradiologicznymi z możliwością precyzyjnego określania elementów badań i wyników AI udostępnianych do konsultacji.

9. System musi zapewnić automatyczną ekstrakcję informacji z obrazów zawierających oznaczenia patologii naniesione przez PUI oraz możliwość porównania z opisami radiologów.
10. System musi zapewniać wydajną komunikację przy równoległym przeglądaniu dużej ilości wyników, obsługę wielu węzłów DICOM oraz szybkie ładowanie obrazów w przeglądarce HTML5.
11. Wymagana jest przeglądarka HTML5 do plików DICOM.

13. Odbiory, testy i dokumentacja (minimum)

1. Wykonawca przeprowadzi testy funkcjonalne i integracyjne co najmniej w zakresie:
 - poprawności przepływów RIS–HIS, RIS–PACS/VNA, PACS/VNA–PUI–RIS,
 - poprawności MWL,
 - poprawności odbioru wyników AI i ich prezentacji,
 - kontroli jakości udostępniania wyników (akceptacja radiologa),
 - weryfikacji logowania i rozliczalności działań.
2. Wykonawca prześle dokumentację powdrożeniową obejmującą co najmniej:
 - opis architektury i konteneryzacji,
 - instrukcje backup/restore i DR,
 - instrukcję aktualizacji i instalacji modułów,
 - opis integracji HL7/FHIR i integracji PUI (mapowania, komunikaty, kolejki, retry, logowanie),
 - instrukcje administracyjne i użytkowe.

14. Serwis i gwarancja

1. Wykonawca udzieli 36 miesięcy gwarancji wraz ze świadczeniem serwisu i nadzoru autorskiego dla integracji PUI oraz zmian w systemie.
2. Zgłoszenia serwisowe obsługiwane przez dedykowany system zgłoszeń Wykonawcy.
3. Maksymalne czasy usunięcia błędów:
 - błędy krytyczne – 3 dni robocze,
 - błędy uciążliwe – 30 dni roboczych.
4. Wsparcie:
 - call center: 8:00–16:00,
 - dla błędów krytycznych: 24/7 (wymóg: zgłoszenie w systemie + potwierdzenie telefoniczne),
 - możliwość zgłoszeń 24/7 w systemie.

Część III – Infrastruktura IT i cyberbezpieczeństwo

1. Serwer TYP 1 – 1 sztuka

Przedmiotem zamówienia jest dostawa fabrycznie nowego serwera przeznaczonego do realizacji kopii zapasowych, wraz z wymaganym oprogramowaniem, licencjami, akcesoriami, dokumentacją oraz gwarancją, spełniającego minimalne wymagania techniczne i funkcjonalne określone w niniejszym OPZ.

Wymagania:

1. Obudowa i konstrukcja

1. Serwer w obudowie typu Rack, o wysokości maksymalnie 2U, umożliwiającej instalację minimum 8 dysków 3,5”.
2. Serwer musi być dostarczony wraz z:
 - o kompletem wysuwanych szyn montażowych umożliwiających montaż w szafie rack oraz wysuwanie serwera do celów serwisowych,
 - o przednim panelem zamykanym na klucz, zabezpieczającym dyski przed nieuprawnionym wyjęciem.

2. Płyta główna i procesory

1. Płyta główna umożliwiająca instalację do dwóch procesorów.
2. Chipset dedykowany przez producenta procesora do pracy w serwerach dwuprocessorowych.
3. Zainstalowane dwa procesory:
 - o minimum 16 rdzeni każdy,
 - o taktowanie bazowe minimum 2,8 GHz,
 - o umożliwiające osiągnięcie w teście SPECrate2017_fp_base wyniku dla dwóch procesorów minimum 420 pkt.
4. Wynik testu SPECrate2017_fp_base dostępny na żądanie zamawiającego.

3. Pamięć operacyjna RAM

1. Zainstalowana pamięć RAM:
 - o minimum 512 GB RAM,
 - o typ DDR5 RDIMM,
 - o szybkość minimum 5600 MT/s,
 - o moduły o pojemności min. 32 GB.
2. Płyta główna musi posiadać minimum 32 sloty pamięci RAM.
3. Obsługa i aktywne wsparcie mechanizmów zabezpieczających pamięć:
 - o Memory Mirroring,
 - o ECC,
 - o Patrol Scrubbing,
 - o SDDC,
 - o Memory Thermal Throttling,
 - o ADDDC-SR,
 - o PPR,
 - o Memory SMBus Hang Recovery.

4. Grafika i porty wbudowane

1. Zintegrowana karta graficzna obsługująca rozdzielczość minimum 1920×1200.
2. Wbudowane porty:
 - o minimum 4 porty USB, w tym:
 - co najmniej 1 × USB 3.0 na przednim panelu,
 - 2 × USB 3.0 na tylnym panelu,
 - 1 × USB na płycie głównej,
 - o 1 × port VGA na tylnym panelu.

3. Wskazane porty nie mogą być realizowane za pomocą adapterów, przejściówek ani kart rozszerzeń.
5. Magistrale i sloty rozszerzeń
 1. Minimum 3 aktywne sloty PCI-E 5.0, w tym co najmniej:
 - 1 × slot PCI-E x16.
 2. Możliwość rozbudowy serwera o min 5 dodatkowych slotów PCI-E.
6. Interfejsy sieciowe i komunikacyjne
 1. Zainstalowane i w pełni funkcjonalne interfejsy:
 - minimum 1 × RJ-45 Ethernet (port zarządzający),
 - minimum 4 × 10 Gb/s Ethernet SFP+ wraz z wkładkami SFP+ Multimode,
 - minimum 2 × FC 16 Gb/s wraz z wkładkami SR do podłączenia biblioteki taśmowej.
7. Pamięć masowa
 1. Zainstalowane dyski systemowe:
 - 2 × SSD M.2 Read-Intensive Hot-Plug,
 - pojemność minimum 480 GB każdy,
 - Dyski M.2 muszą być skonfigurowane w sprzętowy RAID1,
 - dyski nie mogą zajmować kieszeni 3,5”.
 2. Zainstalowane dyski danych:
 - 8 × HDD SATA,
 - pojemność minimum 16 TB każdy.
8. Kontroler RAID dla dysków danych
 1. Sprzętowy kontroler RAID umożliwiający konfigurację poziomów:
 - RAID 0, 1, 5, 6, 10, 50, 60.
 2. Kontroler wyposażony w:
 - minimum 4 GB pamięci cache,
 - podtrzymanie bateryjne.
9. Chłodzenie i zasilanie
 1. Wentylatory:
 - wymiana Hot-Swap,
 - konfiguracja nadmiarowa,
 - liczba wentylatorów zapewniająca poprawne chłodzenie maksymalnej konfiguracji serwera.
 2. Zasilanie:
 - 2 identyczne zasilacze,
 - moc minimum 1600 W każdy,
 - klasa sprawności Titanium,
 - praca redundantna Hot-Swap,
 - możliwość wymiany bez przerywania pracy i bez spadku wydajności.
 3. W komplecie kable zasilające o długości minimum 2 m.
10. Bezpieczeństwo sprzętowe
 1. Fabryczny czujnik otwarcia obudowy.
 2. Moduł TPM 2.0.
11. Panel diagnostyczny (LCD)

Serwer musi umożliwiać wyposażenie w przedni panel diagnostyczny LCD, umożliwiający m.in.:

 - wyświetlanie numeru seryjnego, wersji BIOS i firmware,
 - podgląd statusów i logów RAM, CPU, dysków, wentylatorów, czujników temperatury i zasilaczy,
 - reset konta administratora,
 - podgląd temperatury wlotu powietrza oraz procesorów w czasie rzeczywistym,
 - konfigurację ustawień sieciowych modułu zarządzania.
12. Zdalne zarządzanie
 1. Niezależna karta zarządzająca z dedykowanym portem 1 GbE RJ-45.

2. Funkcjonalności:

- monitoring sprzętu i temperatur,
- monitoring zużycia energii,
- zbieranie logów sprzętowych,
- wirtualna konsola (KVM),
- wirtualne nośniki,
- identyfikacja fizyczna serwera (LED),
- powiadomienia e-mail i SNMP,
- obsługa IPMI, SSH, Redfish,
- screenshot BSOD,
- role użytkowników,
- aktualizacja BIOS, firmware, zasilaczy i LCD,
- możliwość instalacji modułu Wi-Fi.

13. Oprogramowanie zarządzające

Wraz z serwerem musi zostać dostarczone oprogramowanie producenta serwera umożliwiające centralne zarządzanie wieloma serwerami (klaster), dostępne przez przeglądarkę WWW (HTML), obejmujące m.in.:

- zarządzanie zasilaniem i konsolą,
- tworzenie szablonów instalacyjnych OS,
- profile konfiguracji BIOS/RAID/CPU/RAM,
- zdalne montowanie ISO,
- aktualizację BIOS i sterowników,
- zbieranie i wizualizację danych o zużyciu energii.

14. System operacyjny

1. Dostarczenie Windows Server 2025 Standard umożliwiającego uruchomienie dwóch maszyn wirtualnych, z uwzględnieniem liczby rdzeni serwera lub równoważny.

2. Licencja:

- bezterminowa,
- z oficjalnego kanału dystrybucji na rynek polski,

3. Opis równoważności licencji oprogramowania:

- Oprogramowanie serwerowe musi umożliwić uruchomienie oprogramowania dziedzinowego użytkowanego aktualnie w urzędzie oraz pełną współpracę z ActiveDirectory. Licencja zostanie wykorzystana do uruchomienia oprogramowania na serwerze zakupionym w ramach niniejszego postępowania.
- Dostarczone licencje powinny pochodzić z oficjalnego kanału dystrybucyjnego producenta na rynek polski.
- Licencja bez ograniczeń czasowych.
- Instalacja i użytkowanie aplikacji 32- i 64-bitowych na dostarczonym serwerowym systemie operacyjnym;
- Obsługa 64 procesorów fizycznych oraz co najmniej 64 procesorów logicznych (wirtualnych);
- Wielkość obsługiwanej pamięci RAM w ramach jednej instancji systemu operacyjnego – przynajmniej 4TB;
- Obsługa dostępu wielościeżkowego do zasobów LAN poprzez karty Gigabit Ethernet i szybsze, w trybie równoważenia obciążenia łączy (load balancing) i redundancji łączy (failover) – natywnie lub z wykorzystaniem sterowników producenta sprzętu;
- Praca w roli klienta domeny Microsoft Active Directory;
- Zawarta możliwość uruchomienia roli kontrolera domeny Microsoft Active Directory;
- Zawarta możliwość uruchomienia roli serwera DHCP, w tym funkcji klastrowania serwera DHCP (możliwość uruchomienia dwóch serwerów DHCP operujących jednocześnie na tej samej puli oferowanych adresów IP);
- Zawarta możliwość uruchomienia roli serwera DNS;

- Możliwość uruchomienia serwera DNS z możliwością integracji z kontrolerem domeny;
- Zawarta możliwość uruchomienia roli klienta i serwera czasu (NTP);
- Zawarta możliwość uruchomienia roli serwera plików z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory;
- Zawarta możliwość uruchomienia roli serwera wydruku z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory;
- Zawarta możliwość uruchomienia roli serwera stron WWW;
- Zawarta funkcjonalność szyfrowania dysków;
- Dostępny hypervisor umożliwiający uruchamianie wirtualnych systemów w ramach zasobów sprzętowych serwera;
- W ramach licencji zawarte prawo do wirtualizacji dwóch systemów na zasobach sprzętowych serwera;
- W ramach licencji zawarte prawo do pobierania poprawek systemu operacyjnego;
- Wszystkie wymienione powyżej parametry, role, funkcje, itp. systemu operacyjnego objęte są dostarczoną licencją (licencjami) i zawarte w dostarczonej wersji oprogramowania (nie wymagają ponoszenia przez Zamawiającego dodatkowych kosztów);
- Możliwość dokonywania aktualizacji i poprawek systemu przez Internet z możliwością wyboru instalowanych poprawek;
- Możliwość dokonywania uaktualnień sterowników urządzeń przez Internet – witrynę producenta systemu;
- Wbudowana zaporę internetową (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsoli do zarządzania ustawieniami zapory i regułami ip v4 i v6;
- Obsługa zdalnego pulpitu;
- Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu;
- Obsługa PowerShell 4.0;
- Obsługa WiFi i Bluetooth;
- Możliwość współdzielenia zasobów GPU między hostami.

15. Normy, certyfikaty i zgodność

1. Zgodność z normami:

- ISO 9001,
 - ISO 14001,
 - ISO 27001,
 - ISO 50001
- lub normami równoważnymi.

2. Deklaracja CE.

3. Serwer musi znajdować się na liście Windows Server Catalog ze statusem *Certified for Windows Server 2025*.

4. Dokumentacja w języku polskim lub angielskim.

5. Sprzęt i oprogramowanie z oficjalnego kanału dystrybucyjnego.

16. Gwarancja i serwis

1. Serwer fabrycznie nowy, wyprodukowany nie wcześniej niż 6 miesięcy przed dostawą.
2. Gwarancja minimum 36 miesięcy, tryb On-Site, czas reakcji Next Business Day.
3. Realizacja gwarancji przez producenta lub autoryzowanego partnera.
4. Disk retention – uszkodzone dyski pozostają u Zamawiającego.
5. Serwis zgodny z ISO 9001 lub równoważnym.
6. Dostęp do:
 - aktualizacji firmware,
 - bazy wiedzy,

- centrum wsparcia technicznego,
- zgłoszeń serwisowych hardware/software.

2. Serwer TYP 2 – 1 sztuka

Przedmiotem zamówienia jest dostawa fabrycznie nowego serwera przeznaczonego do odtwarzania kopii zapasowych z wykorzystaniem wirtualizacji, wraz z wymaganymi akcesoriami montażowymi, oprogramowaniem, licencjami, dokumentacją oraz gwarancją i serwisem producenta.

Wymagania:

1. Obudowa i montaż

1. Serwer w obudowie typu Rack, o wysokości maksymalnie 1U.
2. Serwer musi zostać dostarczony wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie RACK oraz wysuwanie serwera do celów serwisowych.

2. Płyta główna, chipset, procesory i wydajność

1. Płyta główna umożliwiająca instalację do dwóch procesorów.
2. Chipset dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych.
3. Zainstalowane dwa procesory, każdy:
 - min. 16-rdzeniowy,
 - o taktowaniu bazowym min. 2,8 GHz,
 - umożliwiające osiągnięcie w teście SPECrate2017_fp_base wyniku dla dwóch procesorów min. 420 pkt.
4. Wynik testu SPECrate2017_fp_base potwierdzający spełnienie wymogu dostępny na żądanie zamawiającego.

3. Pamięć operacyjna RAM

1. Zainstalowana pamięć RAM min. 512 GB, w technologii DDR5 RDIMM 5600 MT/s, w modułach po min. 32 GB.
2. Płyta główna musi posiadać min. 32 sloty przeznaczone do instalacji pamięci RAM.
3. Wymagane mechanizmy zabezpieczenia pamięci:
 - Memory mirroring,
 - ECC,
 - Patrol scrubbing,
 - SDDC,
 - Memory thermal throttling,
 - ADDDC-SR,
 - PPR,
 - Memory SMBus hang recovery.

4. Grafika i porty wbudowane

1. Zintegrowana karta graficzna umożliwiająca rozdzielczość min. 1920×1200.
2. Wbudowane porty:
 - 4 porty USB, w tym:
 - co najmniej 1 port USB na przednim panelu obudowy,
 - 2 porty USB 3.0 na tylnym panelu obudowy,
 - 1 port USB na płycie głównej.
 - 1 port VGA na tylnym panelu obudowy.
 - Porty USB oraz VGA nie mogą być realizowane przy użyciu adapterów, przejściówek ani kart rozszerzeń.

5. Sloty rozszerzeń

1. Minimum 2 aktywne sloty PCI-E 5.0 x16.

6. Interfejsy sieciowe i SAN

1. Zainstalowane i w pełni funkcjonalne interfejsy:

- min. 1 × RJ-45 Ethernet management port,
- min. 4 × 10 Gb/s Ethernet SFP+ wraz z wkładkami SFP+ Multimode,
- min. 2 × FC 16 Gb/s wraz z wkładkami SR do podłączenia biblioteki taśmowej.

7. Pamięć masowa – dyski systemowe i RAID

1. Zainstalowane 2 dyski serwerowe SSD M.2 Read-Intensive Hot-Plug o pojemności min. 480 GB każdy.
2. Dyski M.2 muszą być skonfigurowane w sprzętowy RAID1.
3. Dyski nie mogą zajmować kieszeni na dyski 2,5”.

8. Chłodzenie

1. Wentylatory wspierające wymianę Hot-Swap, zamontowane nadmiarowo.
2. Ilość zainstalowanych wentylatorów musi zapewniać wydajne chłodzenie dla maksymalnej konfiguracji serwera (CPU, RAM, PCI-E, dyski, zasilacze).

9. Zasilanie

1. Dwa identyczne zasilacze o mocy min. 1600 W, klasy Titanium, pracujące redundantnie.
2. Zasilacze muszą umożliwiać wyłączenie i wyjęcie dowolnego z nich bez przerywania pracy serwera oraz bez ograniczania wydajności.
3. W komplecie należy dostarczyć kable zasilające o długości min. 2 m.

10. Bezpieczeństwo sprzętowe

1. Wbudowany czujnik otwarcia obudowy jako fabryczne rozwiązanie producenta.
2. Moduł TPM 2.0.

11. Panel diagnostyczny (LCD)

1. Serwer musi umożliwiać wyposażenie w przedni panel diagnostyczny (LCD) umożliwiający:
 - wyświetlenie podstawowych informacji o serwerze (numer seryjny, wersje firmware/BIOS),
 - wyświetlanie stanu i logów dla RAM, CPU, pamięci masowej, wentylatorów, czujników temperatury i zasilaczy,
 - przywracanie konta administratora,
 - podgląd temperatury wlotu powietrza w czasie rzeczywistym,
 - podgląd temperatury procesorów w czasie rzeczywistym,
 - konfigurację ustawień sieciowych modułu zarządzania.

12. Zdalne zarządzanie (BMC)

1. Karta zarządzająca niezależna od systemu operacyjnego, posiadająca dedykowany port 1 GbE RJ-45 (1000 Mbps).
2. Wymagane funkcje:
 - monitoring stanu serwera i komponentów (temperatury, wentylatory itp.),
 - monitoring w czasie rzeczywistym poboru mocy,
 - zbieranie logów błędów sprzętowych,
 - wirtualna konsola z dostępem do myszy i klawiatury,
 - montowanie wirtualnych napędów/nośników,
 - zdalna identyfikacja serwera (sygnalizator optyczny),
 - powiadomienia e-mail i SNMP,
 - wsparcie dla IPMI, SSH, Redfish,
 - wsparcie funkcji screenshot BSOD dla systemów Windows,
 - nadawanie ról użytkownikom,
 - aktualizacje: BMC/BIOS/zasilacze/LCD,
 - możliwość instalacji modułu Wi-Fi do połączenia z modułem zarządzania.

13. Oprogramowanie zarządzające producenta

1. Wraz z serwerem należy dostarczyć oprogramowanie producenta serwera umożliwiające zdalne zarządzanie serwerami jako grupą (klastrem), z GUI dostępnym z poziomu przeglądarki WWW (HTML), obejmujące co najmniej:

- zasilanie (ON/OFF/Restart), logi, status sprzętu, dostęp do pełnej konsoli graficznej,
- tworzenie szablonów instalacyjnych systemów operacyjnych,
- tworzenie profili serwerów (BIOS/CPU/RAM/RAID) do szybkiego wdrożenia identycznych konfiguracji,
- zdalne montowanie obrazów ISO i uruchamianie serwera z ISO,
- aktualizacje sterowników i BIOS,
- zbieranie statystyk zużycia energii dla wszystkich serwerów z prezentacją historyczną (wykresy).

14. System operacyjny i licencje

1. Wraz z serwerem należy dostarczyć Windows Server 2025 Standard zapewniający prawo uruchomienia dwóch maszyn wirtualnych, z uwzględnieniem liczby rdzeni oferowanego serwera lub równoważny.
2. Wymagania równoważności licencji/oprogramowania – oprogramowanie musi spełniać co najmniej wymagania:
 - Oprogramowanie serwerowe musi umożliwić uruchomienie oprogramowania dziedzicznego użytkowanego aktualnie przez Zamawiającego oraz pełną współpracę z ActiveDirectory. Licencja zostanie wykorzystana do uruchomienia oprogramowania na serwerze zakupionym w ramach niniejszego postępowania.
 - Dostarczone licencje powinny pochodzić z oficjalnego kanału dystrybucyjnego producenta na rynek polski.
 - Licencja bez ograniczeń czasowych.
 - Instalacja i użytkowanie aplikacji 32- i 64-bitowych na dostarczonym serwerowym systemie operacyjnym;
 - Obsługa 64 procesorów fizycznych oraz co najmniej 64 procesorów logicznych (wirtualnych);
 - Wielkość obsługiwanej pamięci RAM w ramach jednej instancji systemu operacyjnego – przynajmniej 4TB;
 - Obsługa dostępu wielościeżkowego do zasobów LAN poprzez karty Gigabit Ethernet i szybsze, w trybie równoważenia obciążenia łącza (load balancing) i redundancji łącza (failover) – natywnie lub z wykorzystaniem sterowników producenta sprzętu;
 - Praca w roli klienta domeny Microsoft Active Directory;
 - Zawarta możliwość uruchomienia roli kontrolera domeny Microsoft Active Directory;
 - Zawarta możliwość uruchomienia roli serwera DHCP, w tym funkcji klastrowania serwera DHCP (możliwość uruchomienia dwóch serwerów DHCP operujących jednocześnie na tej samej puli oferowanych adresów IP);
 - Zawarta możliwość uruchomienia roli serwera DNS;
 - Możliwość uruchomienia serwera DNS z możliwością integracji z kontrolerem domeny;
 - Zawarta możliwość uruchomienia roli klienta i serwera czasu (NTP);
 - Zawarta możliwość uruchomienia roli serwera plików z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory;
 - Zawarta możliwość uruchomienia roli serwera wydruku z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory;
 - Zawarta możliwość uruchomienia roli serwera stron WWW;
 - Zawarta funkcjonalność szyfrowania dysków;
 - Dostępny hypervisor umożliwiający uruchamianie wirtualnych systemów w ramach zasobów sprzętowych serwera;
 - W ramach licencji zawarte prawo do wirtualizacji dwóch systemów na zasobach sprzętowych serwera;
 - W ramach licencji zawarte prawo do pobierania poprawek systemu operacyjnego;
 - Wszystkie wymienione powyżej parametry, role, funkcje, itp. systemu operacyjnego objęte są dostarczoną licencją (licencjami) i zawarte w dostarczonej wersji

oprogramowania (nie wymagają ponoszenia przez Zamawiającego dodatkowych kosztów);

- Możliwość dokonywania aktualizacji i poprawek systemu przez Internet z możliwością wyboru instalowanych poprawek;
- Możliwość dokonywania uaktualnień sterowników urządzeń przez Internet – witrynę producenta systemu;
- Wbudowana zaporę internetową (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsoli do zarządzania ustawieniami zapory i regułami ip v4 i v6;
- Obsługa zdalnego pulpitu;
- Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu;
- Obsługa PowerShell 4.0;
- Obsługa WiFi i Bluetooth;
- Możliwość współdzielenia zasobów GPU między hostami.

3. Licencje:

- muszą pochodzić z oficjalnego kanału dystrybucyjnego producenta na rynek polski,
- muszą być bezterminowe.

15. Normy, certyfikaty, zgodność i dokumentacja

1. Wykonawca zapewni zgodność producenta/organizacji serwisowej (lub równoważność) z normami: ISO 9001, ISO 14001, ISO 27001, ISO 50001.
2. Serwer musi posiadać deklarację zgodności CE.
3. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows Server 2025” – dokument potwierdzający należy dołączyć do oferty.
4. Zamawiający wymaga dokumentacji w języku polskim lub angielskim.
5. Urządzenia i oprogramowanie muszą pochodzić z oficjalnego kanału dystrybucyjnego producenta; na wezwanie Zamawiającego Wykonawca dostarczy oświadczenie producenta potwierdzające fabryczną nowość i pochodzenie.

16. Gwarancja i serwis

1. Serwer fabrycznie nowy, wyprodukowany nie wcześniej niż 6 miesięcy przed datą dostawy, objęty serwisem producenta na terenie RP.
2. Gwarancja minimum 36 miesięcy, w trybie On-Site, z czasem reakcji nie później niż Next Business Day od zgłoszenia.
3. Dopuszcza się realizację gwarancji przez autoryzowanego partnera serwisowego producenta.
4. Usługi gwarancyjne świadczone przez producenta lub autoryzowany serwis z ISO 9001 (lub równoważnym) albo podmiot autoryzowany posiadający ISO 9001 (lub równoważny).
5. Na wezwanie Zamawiającego Wykonawca dostarczy:
 - oświadczenie producenta o zaoferowaniu wymaganego poziomu SLA,
 - oświadczenie producenta potwierdzające, że elementy serwera są produktami producenta serwera lub są przez niego certyfikowane oraz że całość jest objęta gwarancją producenta.
6. Gwarancja musi zapewniać:
 - możliwość pobierania najnowszego firmware,
 - dostęp do bazy wiedzy producenta,
 - dostęp do centrum pomocy technicznej producenta lub autoryzowanego serwisu,
 - możliwość otwierania zgłoszeń serwisowych dot. hardware/software oraz otrzymywania poprawek i aktualizacji.

3. Rozbudowa serwerów – 1 komplet

Przedmiotem zamówienia jest rozbudowa posiadanych serwerów xFusion 2288H V6 oraz 1288H V6 kości pamięci RAM 32GB DDR4 RDIMM-3200000KHz-1.2V-ECC-2Rank(2G*8bit) w ilości 56 szt.

4. Rozbudowa macierzy – 1 komplet

Przedmiotem zamówienia jest rozbudowa posiadanej macierzy blokowo-plikowej Huawei OceanStor 2600 V5 (PN: 02355HKU) o poniższe elementy:

32 szt. dysków HDD SAS 2,4 TB

16 szt. dysków SSD SAS 3,84 TB

4 szt. kart z 4 portami 25G SFP28

5. Rozbudowa serwerów NAS – 1 komplet

Przedmiotem zamówienia jest rozbudowa posiadanych serwerów NAS QNAP TS-h2477XU-RP-3700X-32G o dyski HDD SATA 18TB dedykowane do serwerów NAS w ilości 24 szt.

6. Deduplikator – 1 sztuka

Przedmiotem zamówienia jest deduplikator do zadań backupowych.

Wymagania:

1. Obudowa do montażu w szafie rack 19” za pomocą dostarczonych dedykowanych elementów. Oferowany deduplikator nie może przekroczyć rozmiaru 2U. Oferowana obudowa musi umożliwiać instalację min 12 dysków 3.5”.
2. Deduplikator musi być wyposażony w minimum 2 kontrolery pracujące w trybie active-passive lub active-active. Deduplikator nie może posiadać pojedynczego punktu awarii, który powodowałby brak dostępu do danych. W przypadku awarii kontrolera wszystkie procesy musi przejąć drugi kontroler.
3. Oferowany model deduplikatora musi osiągać w maksymalnej konfiguracji zagregowaną wydajność backupu co najmniej 5 TB/h (dane podawane przez producenta). Dodatkowo wymagana zagregowana wydajność backupu przy zastosowaniu deduplikacji na źródle co najmniej 15 TB/h (dane podawane przez producenta).
4. Surowa przestrzeń dyskowa (RAW) stworzona w oparciu o dyski NL SAS musi wynosić min. 160 TB. Dyski muszą być skonfigurowane w RAID 6 z min. 1 dyskiem hot-spare lub przestrzenią hot-spare równą pojemności min. 1 dysku. Dodatkowo wymagane jest zastosowanie co najmniej 4 dysków SSD SAS o łącznej pojemności RAW min. 15 TB jako cache pod zapis backupu.
5. Dane przechowywane w obrębie podsystemu dyskowego urządzenia muszą być chronione za pomocą technologii RAID 6 lub równoważnej tolerującej jednoczesną awarię 2 dysków bez utraty danych.
6. Wymagana możliwość rozbudowy przestrzeni użytkowej poprzez instalację dysków i półek dyskowych oraz dodanie licencji (jeśli będzie wymagana) do min 300 TB.
7. Co najmniej 256GB pamięci cache na cały deduplikator (dwa kontrolery). Pamięć cache musi być zabezpieczona przed utratą danych w przypadku awarii zasilania.
8. Urządzenie musi posiadać minimum:
 - a. 8 portów RJ45 Ethernet 1 Gb/s oraz 4 porty SFP+ Ethernet 10 Gb/s z możliwością obsługi każdym portem Ethernet protokołów CIFS, NFS.
 - b. Wszystkie porty SFP+ wyposażone we wkładki optyczne MM LC 10 Gb/s.
9. Wymagana możliwość agregowania portów (bond port).
10. Wymagane wsparcie dla NFS, CIFS.

11. Zarządzanie deduplikatorem (wszystkimi kontrolerami) z poziomu pojedynczego interfejsu graficznego. Wymagane jest stałe monitorowanie stanu deduplikatora w tym monitorowanie wydajności obiektów takich jak:
 - a. cały deduplikator
 - b. kontrolery
 - c. CPU
 - d. porty front-end
 - e. porty logiczne
 - f. dyski
 - g. file systemyJeżeli do obsługi tych funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane na tym etapie postępowania.
12. Wymagane jest stałe monitorowanie stanu deduplikatora pod kątem parametrów takich jak:
 - a. operacje wejścia/wyjścia IOPS
 - b. przepustowość (KB/s lub MB/s)
 - c. czas odpowiedzi (latency)
 - d. średnie użycie (w % dla CPU)Jeżeli do obsługi tych funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane na tym etapie postępowania.
13. Wymagana możliwość dostępu do historycznych danych wydajnościowych z poziomu GUI urządzenia do co najmniej 2 lat wstecz lub jako równoważne dostarczenie fizycznego serwera z oprogramowaniem umożliwiającym zbieranie i przeglądanie danych historycznych. Jeżeli do obsługi tej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane na tym etapie postępowania.
14. Wymagany dostęp do informacji o wykorzystanej fizycznej przestrzeni oraz aktualnym współczynniku redukcji danych. Jeżeli do obsługi tej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane na tym etapie postępowania.
15. Wymagane wsparcie dla Multi-factor authentication. Jeżeli do obsługi tej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane na tym etapie postępowania.
16. Wymagana możliwość definiowania polityk logowania. Jeżeli do obsługi tej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane na tym etapie postępowania.
17. Urządzenie musi deduplikować dane inline przed zapisem na nośnik dyskowy. Technologia deduplikacji musi wykorzystywać algorytm bazujący na zmiennym bloku. Algorytm ten musi samoczynnie i automatycznie dopasowywać się do otrzymywanego strumienia danych. Proces deduplikacji musi odbywać się inline – w pamięci urządzenia, przed zapisem danych na nośnik dyskowy. Dane muszą być poddane także procesowi kompresji. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
18. Wymagana także obsługa deduplikacji na źródle, co pozwala ograniczyć zużycie sieci. Dostarczenie tej funkcjonalności jest wymagane na tym etapie postępowania.
19. Musi być oficjalne wsparcie producenta dla oferowanego deduplikatora maksymalnego stopnia redukcji danych co najmniej 65:1.
20. Wymagana możliwość skonfigurowania tzw. quote ograniczającej wystawione zasoby plikowe. Wymagana możliwość ograniczenia użytkownikom przestrzeni z której mogą korzystać lub liczby plików jakie mogą być przechowywane na udostępnionej przestrzeni. Dostarczenie tej funkcjonalności jest wymagane na tym etapie postępowania.
21. Wymagana możliwość ograniczenia dostępu do udostępnionych udziałów CIFS/NFS poprzez zdefiniowanie adresów IP lub ich przedziałów, które będą miały do nich dostęp. Dostarczenie tej funkcjonalności jest wymagane na tym etapie postępowania.

22. Tworzenie na żądanie tzw. migawkowej kopii danych (ang. snapshot) file system'ów w ramach deduplikatora do wykorzystania w celu np. wykonywania kopii zapasowych. Wymagana jest możliwość utworzenia harmonogramu snapshotów, które będą zabezpieczone przed modyfikacją oraz usunięciem przez wybrany okres czasu bez odpowiednich uprawnień celem przywrócenia danych w przypadku ataku ransomware. Musi być możliwość odtworzenia danych z dowolnej kopii (snapshot) wykonanej w ramach harmonogramu. Odtworzenie danych z jednej kopii nie może uniemożliwiać odtworzenia danych z innej kopii z innego punktu w czasie. Dostarczenie tej funkcjonalności jest wymagane na tym etapie postępowania na całą przestrzeń dyskową i na maksymalną liczbę snapshotów obsługiwanych przez oferowany model deduplikatora.
23. Wymagana możliwość zablokowania plików przed modyfikacją lub usunięciem (WORM) na poziomie całego file system'u. Dostarczenie licencji na tą funkcjonalność jest wymagane na tym etapie postępowania.
24. Urządzenie musi umożliwiać replikację danych do drugiego urządzenia w ramach tej samej rodziny oferowanego deduplikatora. Replikacja musi się odbywać w trybie asynchronicznym. Wymagana możliwość ograniczenia ilości przesyłanych danych poprzez ich deduplikację oraz kompresję. Dostarczenie tej funkcjonalności nie jest wymagane na tym etapie postępowania.
25. Deduplikator musi umożliwiać konfigurację harmonogramu replikacji poprzez określenie interwału (np. replikacja co 60min) lub konkretnych okien czasowych (np. w każdą sobotę o godz 20:00). Dostarczenie tej funkcjonalności nie jest wymagane na tym etapie postępowania.
26. Urządzenie musi wspierać co najmniej następujące aplikacje do backupu: Commvault, Veritas NetBackup, Veeam Backup&Replication.
27. Deduplikator musi posiadać możliwość upgrade'u firmware-u kontrolerów bez przerywania dostępu do danych.
28. Urządzenie przystosowane do napraw w miejscu instalacji oraz wymiany elementów bez konieczności jego wyłączenia.
29. Urządzenie musi umożliwiać zdalne zarządzanie.
30. Urządzenie musi być fabrycznie nowe, wyprodukowane nie wcześniej niż 6 miesięcy przed datą dostarczenia do Zamawiającego i musi być objęte serwisem producenta lub autoryzowanego partnera serwisowego na terenie RP.
31. Urządzenie musi być zakupione w oficjalnym kanale dystrybucyjnym producenta. Na wezwanie Zamawiającego należy dostarczyć oświadczenie producenta oferowanego deduplikatora, potwierdzające pochodzenie urządzenia z oficjalnego kanału dystrybucyjnego producenta.
32. Wymagana gwarancja na 36 miesięcy w trybie 9x5 NBD. Na wezwanie Zamawiającego należy dostarczyć oświadczenie producenta z potwierdzeniem zaoferowanego poziomu gwarancji.
33. W przypadku awarii, uszkodzone dyski pozostają u Zamawiającego tj. Zamawiający wymaga dostarczenia disk retention.

7. Biblioteka taśmowa – 1 sztuka

Przedmiotem zamówienia jest biblioteka taśmowa LTO-9

Wymagania:

1. Możliwość montażu w szafie RACK 19". Biblioteka musi być dostarczona ze wszystkimi komponentami niezbędnymi do prawidłowej instalacji w szafie rack.
2. Wbudowany wyświetlacz LCD sygnalizujący stan pracy urządzenia.
3. Wysokość dostarczanego urządzenia nie może być większa niż 3U.
4. Obsługiwane typy napędów taśmowych: LTO-8, LTO-9, LTO-10 zarówno w wersji HH jak i FH z interfejsami SAS i FC
5. Zainstalowany minimum 1 napęd LTO-9 wyposażony w złącze FC. Urządzenie musi mieć możliwość instalowania w tej samej obudowie i w tym samym czasie napędów LTO-8 oraz 10. generacji także z interfejsem SAS oraz wspierać technologię LTFS (Linear Tape File System)

umożliwiająca kopiowanie danych na taśmę bez konieczności użycia oprogramowania do backupu kompatybilną z systemami Linux, MAC OS i Microsoft. Prędkość zapisu pojedynczego napędu bez kompresji – minimum 300 MB/sek. Zainstalowany napęd musi posiadać funkcję zarządzania energią, mieć możliwość dynamicznego i płynnego dopasowania prędkości do napływających danych (speed matching), oferować funkcję SkipSync zapewniającą dużą szybkość zapisu małych plików bez konieczności zatrzymywania i przewijania kasyety oraz stosować szyfrowanie danych metodą AES 256-bit zgodną ze standardem FIPS 140-2. Napęd musi wspierać technologię zapisu WORM.

6. Minimum 40 aktywnych kieszeni na taśmy (urządzenie powinno być dostarczone z kompletem magazynków). Jeżeli licencjonowana jest liczba slotów - wymagane aktywowanie wszystkich dostępnych slotów. Wymagana ilość mail slot (I/E): min. 5.
7. Za pomocą panelu kontrolnego znajdującego się na froncie urządzenia, linii poleceń (Command Line Interface) oraz zdalnie przez sieć poprzez przeglądarkę internetową (web GUI) za pomocą interfejsu 1GbE. Oprogramowanie zarządzające musi umożliwiać integrację kont użytkowników biblioteki z serwerem LDAP oraz zapewniać wsparcie dla SSL. Wymagane wsparcie technologii KMIP, SNMP i IPv6 oraz możliwość definiowania minimum 4 poziomów zarządzania urządzeniem. Urządzenie musi mieć możliwość zabezpieczania swojej konfiguracji na podłączony, poprzez slot USB, PenDrive. Operacja powinna być możliwa zarówno poprzez web GUI jak i poprzez panel kontrolny urządzenia
8. Urządzenie musi być wyposażone w minimum 2 interfejsy sieciowe 1GbE, 2 porty USB służące do podłączenia urządzeń testowych i umożliwiające aktualizację firmware napędu oraz robota, dwa porty rozszerzenia, interfejs ADI ze wsparciem ścieżki kontrolnej napędu (control path drives)
9. Urządzenie musi być wyposażone w redundantne zasilacze umożliwiające automatyczne przejęcie pracy przez drugi zasilacz, jeżeli pierwszy uległ uszkodzeniu. Zasilacze powinny pracować w trybie „HotSwap” (wymiana podczas pracy urządzenia)
10. Możliwość wymiany napędów, zasilaczy, modułu portów zarządzania u użytkownika bez konieczności demontażu urządzenia z szafy przemysłowej oraz bez konieczności zdejmowania pokrywy głównej. Możliwość wyjmowania magazynków z urządzenia nawet przy braku zasilania. Pełne wsparcie technologii Air Gap (izolacja powietrzna). Zarówno napędy jak i zasilacze oraz moduł portów zarządzania powinny być wyposażone w lamki kontrolne, informujące o stanie technicznym i widoczne na tylnej stronie biblioteki. Możliwość zdalnego wysuwania magazynków, restartowania biblioteki, definiowania ilości aktywnych slotów w zakresie od 1 do 40 oraz wyłączenia zasilania napędów.
11. Biblioteka musi umożliwiać podział na min. 21 bibliotek logicznych (partycjonowanie). Jeżeli funkcjonalność wymaga licencji należy taką licencję dostarczyć wraz z urządzeniem.
12. możliwość rozbudowy do min. 44 napędów LTO w celu zwiększenia transferu danych
 - a. możliwość rozbudowy do min. 620 slotów w celu zwiększenia pojemności
 - b. urządzenie powinno mieć możliwość łączenia ze sobą kolejnych modułów z możliwością automatycznego przekładania nośników między modułami, przy czym układ robotyki dla przenoszenia kaset z taśmami LTO musi operować wyłącznie wewnątrz biblioteki. Jeżeli do rozbudowy konieczna są jakiekolwiek licencje (np. licencje na sloty, napędy) należy takie dostarczyć wraz z urządzeniem – dostarczone licencje muszą obsługiwać maksymalną liczbę napędów i slotów
13. Urządzenie musi być standardowo wyposażone w czytnik kodów kreskowych, kable zasilające, zestaw odpowiednich kabli o długości min. 5m koniecznych do podłączenia napędu do odpowiedniego kontrolera serwera umożliwiającego komunikację z urządzeniem. Wraz z urządzeniem należy dostarczyć zestaw minimum 32 kompatybilnych nośników danych LTO-9 RW o pojemności do 45TB oraz minimum 10 kompatybilnych nośników danych LTO-9 WORM o pojemności do 45TB wraz z nośnikiem czyszczącym (wszystkie nośniki wyposażone w indywidualne naklejki z kodami kreskowymi), przy czym dostarczone nośniki muszą być

kompatybilne i dedykowane do współpracy z oferowanym urządzeniem, co należy poświadczyć odpowiednim oświadczeniem producenta urządzenia.

14. 36 miesięcy naprawy w miejscu instalacji sprzętu z czasem reakcji na zgłoszenia do max. 4 godzin. Czas przyjmowania zgłoszeń serwisowych w trybie 5x9. Naprawa uszkodzonego komponentu lub urządzenia najpóźniej do 48 godzin od zgłoszenia. Gwarantowana możliwość rozszerzenia oferowanego serwisu do 84 miesięcy. Zgłaszanie awarii wyłącznie poprzez ogólnopolską linię telefoniczną producenta lub autoryzowany serwis producenta posiadający certyfikaty ISO9001 na usługi serwisowe (certyfikaty dołączyć do oferty) – kontakt z serwisem wyłącznie w języku polskim.
15. Pisemne oświadczenie wystawione przez producenta i dostarczone wraz z ofertą o oferowanej gwarancji świadczonej realizowanej przez producenta lub jego autoryzowany serwis posiadający ISO9001 na usługi serwisowe wraz z potwierdzeniem możliwości przedłużenia gwarancji do 84 miesięcy. W oświadczeniu wymagane jest podanie wszystkich danych kontaktowych z serwisem (mail, telefon, adres) oraz potwierdzenie wykupienia przez wykonawcę wymienionych usług serwisowych u producenta.
16. Wymaga się, aby wdrożenie i konfigurację urządzenia przeprowadziła osoba posiadająca certyfikat techniczny producenta urządzenia wystawiony w roku wdrożenia systemu.
17. Biblioteka musi być wyprodukowana zgodnie z następującymi normami: CE, RoHS, WEEE, ISO9001, ISO14001, ISO27001, ISO50001 lub równoważnymi.

8. Oprogramowanie do backupu i archiwizacji – 1 komplet

8.1. Oprogramowanie do backupu VM – 1 komplet

Przedmiotem zamówienia jest dostawa oprogramowania do tworzenia kopii zapasowych oraz przywracania danych dla maszyn wirtualnych. W ramach zamówienia przewiduje się zakup licencji wieczystych na oprogramowanie umożliwiające kompleksowe zarządzanie procesem backupu oraz przywracania danych dla 50 maszyn wirtualnych ze wsparciem technicznym na minimum 36 miesięcy. Oprogramowanie ma zapewniać niezawodność, skalowalność oraz pełną integrację z istniejącą infrastrukturą wirtualną zamawiającego. Jeśli przy danym punkcie wymogu występuje informacja „jako opcja” oznacza to iż zaproponowany system posiada daną funkcjonalność, a jej uruchomienie może wymagać zakupu dodatkowych licencji – Zamawiający nie oczekuje oferty na nią a jedynie chce mieć możliwość w przyszłości rozbudowy o tę funkcjonalność.

Wymagania:

1. Rozwiązanie musi reprezentować architekturę trójwarstwową (serwer zarządzający, serwer medialny oraz klient), taka architektura pozwoli na elastyczną skalowalność rozwiązania bez względu na dynamikę przyrostu danych.
2. Oprogramowanie nie może preferować platformy sprzętowej, nie może być profilowane pod konkretnego dostawcę sprzętu serwerowego oraz pamięci masowych. Niedopuszczalne jest aby funkcjonalności związane z zabezpieczaniem danych były w jakikolwiek sposób związane czy zależne od konkretnego typu czy producenta urządzenia.
3. Licencje muszą pozwalać na stworzenie dla serwera zarządzającego rozwiązania wysokodostępного z częstotliwością replikacji bazy katalogowej nie dłuższym niż 15 minut (RPO nie większe niż 15 min dla uruchomienia zapasowego serwera zarządzającego). Jeśli do stworzenia takowego rozwiązania potrzebne są licencje replikacyjne, klastrowe, współdzielona przestrzeń dyskowa to muszą zostać zaoferowane. Licencje muszą pozwalać na skonfigurowanie serwerów zarządzających oraz ich replikację dla co najmniej trzech lokalizacji, gdzie pierwsza jest lokalizacja produkcyjną, druga i trzecia są typu standby dla serwera zarządzającego.

4. Jako opcja musi istnieć możliwość zainstalowania serwera zarządzającego na systemie operacyjnym Linux z zachowaniem możliwości replikacji bazy katalogowej i tworzeniem serwerów typu standby.
5. Możliwość jako opcja testowania (walidacja) odtwarzania serwera zarządzającego w chmurze producenta w celu weryfikacji możliwości DR w przypadku jego awarii
6. Proces przełączenia serwera zarządzającego musi umożliwiać:
 - a. Przełączenie automatyczne inicjalizowane przez administratora
 - b. Przełączenie automatyczne (bezobsługowe) w przypadku wykrycia awarii (w przypadku awarii serwera zarządzającego system automatycznie wykrywa awarie i przełącza działanie systemu na serwer zapasowy – standby, bez jakiegokolwiek interwencji administratora)
7. Przełączenie serwera zarządzającego musi odbywać się w pełni automatycznie poprzez administratora, który decyduje kiedy ma ono nastąpić, przełączanie serwera zarządzającego musi być możliwe pomiędzy różnymi typami infrastruktury:
 - a. serwer fizyczny -> serwer fizyczny
 - b. serwer fizyczny -> serwer wirtualny (onpremis)
 - c. serwer fizyczny -> serwer wirtualny (AWS, Azure, Google)
 - d. serwer wirtualny (onpremis) -> serwer fizyczny
 - e. serwer wirtualny (onpremis) -> serwer wirtualny (onpremis)
 - f. serwer wirtualny (onpremis) -> serwer wirtualny (AWS, Azure, Google)
8. Mechanizm przełączania serwera zarządzającego musi pozwalać (minimum) na wybór trybu:
 - a. Test failover (testowanie mechanizmu przełączania)
 - b. Failover (produkcyjne przełączenie działania na serwer standby)
 - c. Maintenance failover (przełączenie w celu np. aktualizacji oprogramowania)
9. Rozwiązanie musi zapewnić interfejs graficzny do zarządzania i instalacji.
10. Oprogramowanie musi umożliwiać zdalne instalowanie i odinstalowywanie klienta systemu z centralnego serwera dla systemów Windows, Linux i Unix – musi być to możliwe z jednego serwera pełniącego rolę cache dla wszystkich binarii klienckich
11. System musi zapewniać funkcjonalność odtwarzania po awarii konfiguracji serwera zarządzającego tworzeniem kopii bezpieczeństwa i archiwów.
12. System musi posiadać możliwość nieodwracalnego kasowania danych – funkcjonalność ta musi być częścią oprogramowania i musi pozwalać na wyczyszczenie przestrzeni dyskowych (zamazanie) tak aby narzędziami niskiego poziomu nie było możliwości odzyskania tych danych.
13. Administrator systemu musi mieć możliwość wybrania (minimum) plików z danej kopii backupowej i ich skasowania, tak aby nie było możliwości ich późniejszego odtworzenia z tej kopii.
14. Dla dowolnego transferu danych z klienta musi istnieć możliwość definiowania/ograniczania pasma dla transferu danych – funkcjonalność ta musi być dostępna także przy włączonej deduplikacji na kliencie
System musi pozwalać na składowanie danych na taśmach celem przechowywania długoterminowego. Składowane dane na taśmach muszą być w formie nie zdeduplikowanej (nawodnione) po to by była możliwość odtwarzania ich bezpośrednio, a więc bez konieczności pośrednictwa dysków, buforów czy importu
15. System musi pozwalać na zarządzanie całością działania systemu (backup, archiwizacja, backup laptopów) z jednej konsoli administracyjnej oraz także z konsoli webowej
16. Agenci systemu muszą posiadać funkcjonalność komunikowania się poprzez jeden port TCP/IP, celem zabezpieczenia komunikacji z środowisk typu DMZ
17. Automatyczne tunelowanie komunikacji TCP/IP pomiędzy agentami systemu – jeśli agent systemu wykryje ograniczenia w komunikacji, wtenczas automatycznie zestawia połączenie tunelowe wykorzystujące tylko jeden port TCP/IP

18. System musi umożliwiać nie tylko szyfrowanie danych (kopii backupowych) ale także całej komunikacji pomiędzy komponentami systemu (minimum pomiędzy agentem backupowym a serwerem składającym i zarządzającym kopiami).
19. System musi umożliwiać konfigurację, którymi kartami sieciowymi ma przebiegać komunikacja i transfer danych, wybór interface musi odbywać się co najmniej poprzez nazwę domeny, subnet, zakres IP
System musi pozwalać na współdzielenie napędów taśmowych w środowisku sieci SAN
20. System musi umożliwić przechowywanie jedynie unikalnych bloków danych tzw. deduplikacja. Funkcjonalność ta musi działać na poziomie blokowym i być wykonywana online podczas procesu tworzenia kopii danych. Deduplikacja musi być realizowana poprzez oprogramowanie systemu na dowolnym sprzęcie czy to w warstwie serwera systemu czy klienta. Pojedynczy serwer systemu musi umożliwiać przechowywanie danych po deduplikacji minimum do 500 TB (rozbudowa do tej wielkości może nastąpić tylko poprzez dodanie dodatkowej przestrzeni do składowania danych poprzez dodanie dysków, półki dyskowej a nie przez wymianę urządzenia).
21. Włączenie funkcjonalności deduplikacji na kliencie musi być możliwe dla różnych systemów operacyjnych: Windows, Linux, Unix i Macintosh
22. Logiczna Globalna deduplikacja – system musi oferować deduplikację globalną co oznacza iż niezależnie z jakich klientów dane będą deduplikowane (serwery fizyczne, hosty wirtualne, bazy i aplikację) – deduplikacja musi opierać się na jednej logicznej centralnej bazie deduplikacyjnej
23. Włączenie funkcjonalności deduplikacji nie może generować wymogu instalacji dodatkowych modułów programowych po stronie klienckiej lub serwera systemu. Niedopuszczalne jest łączenie systemu z dodatkowym oprogramowaniem czy sprzętem (appliance) dla uzyskania funkcjonalności deduplikacji danych.
24. Deduplikacja blokowa musi obejmować dane nie tylko backupowane ale i archiwizowane, przy czym wielkość bloku nie może być większa niż 128KB.
25. System musi zapewniać wspólny stopień deduplikacji (jedna baza deduplikacyjna) dla danych czy to z backupu czy archiwizacji.
26. System musi umożliwiać wykonywanie kopii w post procesie do drugiej lokalizacji przesyłając jedynie unikalne bloki danych (dla dowolnych danych: czy to z procesu backupu czy archiwizacji). A więc replikacja danych do innej lokalizacji musi być wykonywana na danych po deduplikacji i funkcjonalność ta musi być realizowana i zarządzana z poziomu systemu.
27. Proces przesyłania danych (replikacji) na inny serwer systemu celem tworzenia dodatkowej kopii danych nie może być zależny od warstwy sprzętowej, a więc dowolny producent serwera, dowolny producent macierzy/półki dyskowej.
28. System musi składować dane po deduplikacji (kopie backupowe) na storage obiektowym zgodnym z S3 czy to w środowisku onpremis czy cloud, musi wspierać technologię WORM na tych typach storage, transfer danych musi odbywać się z wykorzystaniem deduplikacji i muszą być wysyłane tylko unikalne bloki danych. Nie dopuszczalne jest aby tworzenie kolejnej kopii danych na storage obiektowym wymagało nawodnienia danych – transfer musi odbywać się tylko unikalnych bloków danych.
29. System musi pozwalać na instalację bazy deduplikacyjnej w układzie wysokiej dostępności (minimum na dwóch serwerach) w taki sposób aby awaria pojedynczego serwera nie powodowała utraty możliwości backupu z deduplikacją i odtwarzania wcześniejszych kopii danych.
30. System musi pozwalać na odtwarzanie zdeduplikowanych danych nawet w momencie, gdy baza deduplikacyjna jest niedostępna. Proces odtwarzania (nawadniania) zdeduplikowanych danych nie korzysta z bazy deduplikacyjnej.
31. Na jednym serwerze systemu (na jednej instancji systemu operacyjnego) może być zainstalowane minimum dwie bazy deduplikacyjne pozwalające zwiększyć skalowalność systemu.
32. System musi zapewniać dostęp zintegrowany z usługą katalogową, minimum Active Directory, a więc tak zwany „single sign on” – pojedyncze logowanie: użytkownik po zalogowaniu do domeny

AD, nie potrzebuje wykonywać następnego logowania aby zarządzać systemem poprzez konsolę administracyjną.

33. Możliwość uruchomienia logowania wieloskładnikowego (SAML) dla dostępu do konsoli administracyjnej.
34. System musi być odporny na tzw. „atak na wzorzec czasu”: to znaczy iż przy radykalnej zmianie czasu na serwerze zarządzającym System musi automatycznie zatrzymać co najmniej proces kasowania (ekspiracji) kopii backupowych generując odpowiednie alerty do czasu potwierdzenia tej zmiany przez administratora.
35. System musi zapewniać elastyczne delegowanie uprawnień oraz audytowanie działań użytkowników. Z tym, że delegowanie uprawnień musi pozwalać na przydział uprawnień per serwer czy grupa serwerów, przydział uprawnień musi pozwalać na definiowanie uprawnień dla grup użytkowników z domeny AD.
36. Komunikacja pomiędzy agentem a serwerem systemu musi opierać się na certyfikatach.
37. System musi posiadać funkcjonalność blokowania danych do odczytu dla administratora, to znaczy, że administrator systemu nawet mając pełne uprawnienia nie może odtworzyć danych, jeśli nie jest ich właścicielem, funkcjonalność ta musi być dostępna nie tylko dla danych z laptopów/desktopów ale i dla serwerów (także dla danych plikowych i bazodanowych).
38. System musi pozwalać na skonfigurowanie mechanizmu podwójnej autentyfikacji administratora – do uruchomienia konsoli administracyjnej systemu potrzebne jest nie tylko logowanie, ale i dodatkowy tymczasowy kod wysyłany do administratora np. poprzez mail.
39. Szyfrowanie danych musi pozwalać na wybór algorytmu (minimum dwa algorytmy: Blowfish, AES) także dla danych deduplikowanych na kliencie systemu.
40. Możliwość szyfrowania musi pozwalać na elastyczny wybór miejsca szyfrowania: szyfrowanie danych na kliencie, szyfrowanie danych na serwerze backupowym i szyfrowanie tylko transmisji pomiędzy klientem backupowym a serwerem.
41. System musi wspierać mechanizm szyfrowania danych na napędach taśmowych LTO.
42. System musi pozwalać na integrację z zewnętrznymi repozytoriami do przechowywania kluczy szyfrującym zgodnymi z KMIP – minimum dla:
 - a. AWS CloudHSM
 - b. Fortanix Data Security Manager
 - c. HashiCorp Vault
 - d. IBM Security Key Lifecycle Manager (SKLM)
 - e. Safenet
 - f. StorMagic SvKMS
 - g. Thales CipherTrust Manager
 - h. Vormetric
 - i. Amazon Web Services (AWS) key management service
 - j. Microsoft Azure Key Vault
43. System musi umożliwiać składowanie kopii bazy katalogowej w chmurze producenta oprogramowania, funkcjonalność ta musi być w cenie produktu i pozwalać na automatyczne składowanie kopii bazy.
44. System musi mieć wbudowane mechanizmy zabezpieczające przed złośliwym oprogramowaniem (Ransomware), minimum to:
 - a. Dedykowany dashboard będący częścią konsoli administracyjnej systemu do identyfikacji i zarządzania zagrożeniami, pozwalający administratorowi na działania proaktywne lub reaktywne w momencie wykrycia zagrożenia.
 - b. Monitorowanie nietypowych zachowań systemu backupowego obejmującego obszary:
 - i. Czyszczenia bazy deduplikacyjnej (DDB)
 - ii. Zdarzeń w Systemie (events)
 - iii. Ilości nieudanych zadań
 - iv. Ilości zadań czekających
 - v. Ilości zadań zakończonych sukcesem

- vi. Konsoli monitorującej zadania
 - vii. Czasu trwania zadań
 - c. Zabezpieczenie ścieżek dostępu do danych składowanych (kopii backupowych) na dyskach – tylko procesy systemu mogą zapisywać i modyfikować dane.
 - d. Monitorowanie (jako opcja) nietypowych aktywności na serwerach plikowych.
 - e. Monitorowanie nietypowych aktywności na serwerach za pomocą metody: Honeypot (plików pułapek/wabików) – system cyklicznie i automatycznie sprawdza czy pliki pułapki nie były modyfikowane.
 - f. Monitorowanie (jako opcja) możliwego zagrożenia dotyczącego zaszyfrowania plików na serwerach.
 - g. Monitorowanie (jako opcja) różnych typów plików i weryfikowanie czy typ pliku jest zgodny i czytelny z nagłówkiem tego pliku (detekcja uszkodzeń plików czy ich zaszyfrowania).
 - h. Monitorowanie klientów Systemu i alertowanie o tych którzy tracą komunikację z Systemem.
 - i. Air Gap (izolowanie i segmentowanie składowanych kopii backupowych) – musi polegać na wbudowanym automatycznym mechanizmie wyłączania komunikacji pomiędzy pozostałymi komponentami systemu backupowego. Tak więc komunikacja z wybranym segmentem środowiska backupowego odbywa się tylko w określonym przedziale czasowym dla potrzeb replikacji kopii backupowych, natomiast przez pozostały czas żadne procesy systemu backupowego nie mają możliwości komunikacji z tym środowiskiem.
 - j. Możliwość definiowania serwerów komunikacyjnych (tzw. bram/gateway) przez które wykonywana jest komunikacja pomiędzy modułami systemu backupowego, w szczególności pomiędzy serwerem zarządzającym a serwerem medii czy serwerem z dowolnym agentem backupowym.
 - k. Możliwość definiowania kierunku inicjalizowania komunikacji sieciowej pomiędzy komponentami systemu backupowego.
 - l. Mechanizm WORM - możliwość zablokowania zmiany retencji (czas przechowywania kopii backupowych) na krótszą dla kopii backupowych składowanych na dowolnych typach nośników w tym na dyskach i taśmach.
 - m. Wsparcie dla mechanizmu WORM dla macierzy obiektowych.
 - n. MFA (Multi Factor Authentication) - uwierzytelnianie wieloskładnikowe.
 - o. MPA (Multi Person Autorisation) – dwuosobowa autoryzacja działań (w przypadku wykonywania przez administratora systemu działania, które spowoduje skasowanie danych inna/dodatkowa osoba musi potwierdzić lub odrzucić takie działanie).
45. Identyfikacja złośliwego oprogramowania i zapobieganie ponownej infekcji dla backupów plikowych (Threat Scan) jako opcja, która skanuje pliki kopii zapasowych wykorzystując różne techniki: File Entropy, SIM Hash, Signature o funkcjonalnościach minimum:
- a. Częstotliwość aktualizacji silnika skanującego nie mniejsza niż co 24 godziny wykonywana automatycznie.
 - b. Manualny lub automatyczny wybór kopii backupowych zasobów plikowych do skanowania.
 - c. Wykrywanie zagrożeń typu malware.
 - d. Analiza zbackupowanych plików pod kątem zaszyfrowania.
 - e. Automatyczne blokowanie zainfekowanych plików z kopii backupowych przed odtwarzaniem.
 - f. Możliwość detekcji i odtwarzania danych historycznych nie zainfekowanych.
 - g. Raportowanie i zarządzanie komponentem poprzez konsolę administracyjną systemu backupowego.
 - h. Skanowanie danych z pierwszej (podstawowej) lub drugiej kopii backupowej.

46. Identyfikacja złośliwego oprogramowania i zapobieganie ponownej infekcji dla backupów stacji roboczych (Threat Scan) jako opcja, która skanuje pliki kopii zapasowych wykorzystując różne techniki: File Entropy, SIM Hash, Signature o funkcjonalnościach minimum:
- Częstotliwość aktualizacji silnika skanującego nie mniejsza niż co 24 godziny wykonywana automatycznie.
 - Manualny lub automatyczny wybór kopii backupowych zasobów plikowych do skanowania.
 - Wykrywanie zagrożeń typu malware.
 - Analiza zbackupowanych plików pod kątem zaszyfrowania.
 - Automatyczne blokowanie zainfekowanych plików z kopii backupowych przed odtwarzaniem.
 - Możliwość detekcji i odtwarzania danych historycznych nie zainfekowanych
 - Raportowanie i zarządzanie komponentem poprzez konsolę administracyjną systemu backupowego.
 - Skanowanie danych z pierwszej (podstawowej) lub drugiej kopii backupowej.
47. Identyfikacja złośliwego oprogramowania i zapobieganie ponownej infekcji dla kopii backupowych maszyn wirtualnych (Threat Scan) jako opcja, która skanuje zawartość dysków zbackupowanych maszyn wirtualnych różne techniki: File Entropy, SIM Hash, Signature o funkcjonalnościach minimum:
- Częstotliwość aktualizacji silnika skanującego nie mniejsza niż co 24 godziny wykonywana automatycznie.
 - Manualny lub automatyczny wybór maszyny wirtualnej z kopii backupowej.
 - Skanowanie musi odbywać na odtworzonej maszynie wirtualnej.
 - Raportowanie i zarządzanie komponentem poprzez konsolę administracyjną systemu backupowego.
 - Skanowanie danych z pierwszej (podstawowej) lub drugiej kopii backupowej.
48. Wszelkie działania w systemie, także działania użytkowników końcowych muszą być logowane i przechowywane.
49. Integracja z systemami SOAR.
50. System musi posiadać zaawansowane mechanizmy exportu i analizy logów poprzez Syslog server.
51. System musi posiadać rozbudowany system raportowania dla administratorów, minimalny zestaw dostępnych raportów to:
- Raport zmian/wzrostu środowiska systemu.
 - Raport wykorzystania licencji.
 - Raport wykonanych zadań backupowych.
 - Raporty obciążenia serwerów backupowych – minimum monitorowanie użycia CPU i pamięci RAM.
52. System musi mieć możliwość automatycznego wysyłania dowolnych raportów do wybranych użytkowników poprzez mail.
53. System musi mieć możliwość automatycznego zapisywania raportów w formacie minimum: PDF, HTML i CSV.
54. Notyfikacje alertów muszą być wysyłane minimum poprzez mail.
55. System musi zapewniać funkcjonalność wznowiania zadań backupowych.
56. System musi zapewniać funkcjonalność równoległego wykonywania kopii danych backupowanych – inline copy (tego samego zestawu danych pojedynczego klienta) na minimum dwa docelowe urządzenia przechowywania danych.
57. System musi zapewniać funkcjonalność wykonywania zadania backupu wieloma równoległymi strumieniami – tzw. multistreaming. Polega ona na tym iż agent systemu równolegle czyta różne obszary danych i bez pośredniczenia dysków automatycznie wysyła je do serwera, który zapisuje te dane albo na dyski albo na nośniki taśmowe. Funkcjonalność ta musi być dostępna dla dowolnych typów danych: backup plikowy, bazodanowy.

58. Funkcjonalność multistreamingu musi być dostępna dla deduplikacji bez względu czy następuje na kliencie czy na serwerze systemu.
59. System musi zapewniać funkcjonalność multipleksowania kilku strumieni danych na nośniku taśmowym – tzw. multiplexing. Wydajny zapis wielu strumieni danych na taśmy bez pośrednictwa dysków.
60. Rozwiązanie musi posiadać możliwość wykonywania backupu pełnego, przyrostowego, różnicowego oraz syntetycznego.
61. System musi posiadać funkcję szyfrowania i kompresji danych transmitowanych przez LAN, możliwość wykorzystania szyfrowania i kompresji musi być dostępna w dowolnej kombinacji.
62. System ma realizować procesy backupu oraz odzyskiwania danych, procesy te muszą być uruchamiane ręcznie i poprzez wbudowany kalendarz, możliwość definiowania zadań poprzez wbudowany w system kalendarz musi być możliwa nie tylko dla zadań backupowych ale także dla zadań odtwarzania danych a więc restore.
63. System musi posiadać (jako opcja) zintegrowane w systemie mechanizmy indeksowania pełnokontekstowego i wyszukiwania danych. Indeksowaniu powinny podlegać dane zbackupowane i zarchiwizowane już znajdujące się w systemie.
64. System musi realizować funkcjonalność weryfikacji wykonanych kopii.
65. System powinien umożliwiać wykorzystanie funkcjonalności Bare Metal Restore dla odtwarzania systemu po awarii, wsparcie musi być dostępne dla systemów:
 - a. Windows
 - b. Linux: Debian/Oracle Linux/RHEL/CentOs/SuSe/Ubuntu
66. System powinien umożliwiać składowanie kopii backupowych na storage obiektowym w chmurze, minimum: Azure, Amazon, Google Cloud, jeśli do włączenia tej funkcjonalności potrzebne są jakieś dodatkowe komponenty to muszą być zaoferowane.
67. System musi umożliwiać odtwarzanie danych plikowych pomiędzy systemami operacyjnymi np. odtwarzanie danych plikowych Linux na systemie Windows.
68. Możliwość backupu i odtwarzania (jako opcja) dedykowanym agentem dokumentów i maili dla Office 365 z:
 - a. SharePoint Online
 - b. Exchange Online
 - c. OneDrive
 - d. Teams
 - e. Ruch pocztowy SMTP
69. Możliwość (jako opcja) pełnokontekstowego indeksowania i wyszukiwania treści (eDiscovery i Compliance Search) z danych backupowanych z:
 - a. Skrzynek pocztowych (Exchange onpremis)
 - b. Skrzynek journalingowych (Exchange onpremis)
 - c. Ruchu pocztowego SMTP
 - d. Exchange Online
 - e. Serwerów plikowych
 - f. Laptopów i desktopów
 - g. OneDrive for Business
 - h. SharePoint Online
70. System (jako opcja) musi pozwalać na wyszukiwanie danych wrażliwych (np. numery PESEL) i pozwalać osobie uprawnionej nie tylko na raportowanie takich zdarzeń ale także umożliwiać kasowanie plików nie tylko z systemów produkcyjnych ale i z kopii backupowej.
71. Możliwość zwiększenia bezpieczeństwa systemu poprzez integrację z CyberArk pozwalającą na przechowywanie kont i haseł także dla aplikacji w środowisku CyberArk a nie w środowisku backupowych. Integracja musi pozwalać na rotacyjną zmianę haseł i ich synchronizację w środowisku.
72. Musi istnieć możliwość wskazania klucza szyfrującego (Bring Your Own Key – BYOK), który będzie wykorzystywany do szyfrowania kopii backupowych.

73. Automatyzacja – zarządzanie systemem poprzez API, Terraform, Ansible i PowerShell.
74. Workflow – dedykowany komponent do tworzenia i uruchamiania procesów obejmujących działania w obszarze backupu, odtwarzania oraz pozwalający na wykonywanie poleceń czy skryptów z systemów zewnętrznych.
75. Podstawowe komponenty systemu jak: serwer zarządzający, serwery składujące i deduplikujące dane muszą wspierać system operacyjny Linux, a więc musi istnieć możliwość bezpośredniego zainstalowania na systemie Linux tych komponentów bez jakiegokolwiek warstwy virtualizacyjnej.
76. System (jako opcja) musi posiadać zaawansowaną funkcjonalność analizy zasobów plikowych minimum o funkcjonalnościach:
- Detekcja powtarzających się zasobów
 - Raportowanie praw dostępu do plików
 - Raportowanie i analiza dostępu do zasobów i ich modyfikacji
 - Możliwość kasowania plików z zasobów produkcyjnych
77. System (jako opcja) musi pozwalać na wyszukiwanie danych wrażliwych (np. numery PESEL) i pozwalać osobie uprawnionej nie tylko na raportowanie takich zdarzeń ale także umożliwiać kasowanie plików nie tylko z systemów produkcyjnych ale i z kopii backupowej.
78. System musi wspierać backup całych maszyn wirtualnych/kontenerów dla czołowych rozwiązań virtualizacyjnych, kontenerowych i chmurowych:
- Alibaba Cloud
 - Amazon
 - Citrix Xen
 - Google Cloud Platform
 - Huawei FusionCompute
 - Microsoft Azure
 - Microsoft Azure Stack Hub
 - Microsoft Azure Stack HCI
 - Microsoft Hyper-V
 - Kubernetes
 - Nutanix Acropolis Hypervisor (AHV)
 - OpenStack
 - Oracle Cloud Classic
 - Oracle Cloud Infrastructure
 - Oracle VM
 - Red Hat OpenShift
 - Red Hat Virtualization
 - vCloud Director
 - VMware
- To znaczy musi posiadać dedykowany komponent do backupu minimum całej maszyny wirtualnej/kontenera/aplikacji/wolumenu bez konieczności instalowania agenta wewnątrz np. maszyny z możliwością granularnego odtwarzania pojedynczych plików.
79. Dla maszyn wirtualnych musi być możliwość zainstalowania agenta plikowego i bazodanowego dla zabezpieczenia zasobów z wewnątrz maszyny wirtualnej – funkcjonalność ta musi być zawarta dla wszystkich wymaganych virtualizatorów i być w cenie rozwiązania.
80. Przy odtwarzaniu danych środowisk kontenerowych musi istnieć możliwość selekcji zasobów podlegającym odtworzeniu.
81. Dla backupu i odtwarzania środowisk wirtualnych opartych o VMware musi być możliwość wyboru różnych transportów: SAN, Hot-add, NBD, SSL, NAS - gdzie transport NAS pozwala na bezpośredni odczyt i zapis danych maszyny wirtualnej z urządzenia NAS.
82. System musi zapewniać automatyczne wykrywanie i dodawanie do polityki backupu nowych maszyn wirtualnych.

83. System musi umożliwiać odzyskanie i uruchomienie maszyn wirtualnych z kopii zapasowej bez oczekiwania na pełne przywrócenie maszyny wirtualnej minimum dla Vmware i Hyper-V.
84. System musi umożliwiać konwertowanie maszyn wirtualnych pomiędzy wirtualizatorami, minimum:
- a. Vmware do: Hyper-V, Azure, Amazon, Google Cloud Platform, Openstack, Oracle Cloud Infrastructure
 - b. Hyper-V do: Azure, Amazon, Vmware
 - c. Amazon do: Azure, Vmware
 - d. Azure do: Amazon, Hyper-V, Vmware
- Co oznacza, iż w przypadku odtwarzania zbackupowanej maszyny wirtualnej istnieje możliwość wybrania innego wirtualizatora jako miejsce odtwarzania i uruchomienia odtworzonej maszyny wirtualnej.
85. System musi wspierać mechanizm CBT (change block tracking) minimum dla Vmware i Hyper-V.
86. System musi umożliwiać konwersję zbackupowanego serwera Windows i Linux do maszyny wirtualnej w środowisku:
- a. Hyper-V
 - b. Vmware
87. Możliwość (jako opcja) synchronizacji maszyn wirtualnych Vmware do środowiska Amazon, Azure, Hyper-V, Vmware celem budowy rozwiązania DR (Disaster Recovery) z funkcjonalnościami:
- a. Failover (planowane i niezaplanowane/awaryjne)
 - b. Failback
88. System (jako opcja) musi oferować rozbudowę o funkcjonalność przeszukiwania i analizy zasobów plikowych dla maszyn wirtualnych (minimum Vmware) całość działań związanych musi odbywać się na kopiach backupowych maszyn wirtualnych a nie na środowisku produkcyjnym.
89. System musi oferować integrację z mechanizmami deduplikacyjnymi urządzeń typu appliance minimalne wsparcie to Catalyst i urządzenie StoreOnce. Integracja z StoreOnce musi być dostępna nie tylko dla Windows ale także dla Linux i wspierać tzw. client direct (transfer danych bezpośrednio na urządzenia deduplikacyjne a tylko metadane wysyłane do systemu backupowego).
90. System musi oferować integrację z mechanizmami deduplikacyjnymi urządzeń typu appliance minimalne wsparcie to DDBoost i urządzenie StoreOnData Domain. Integracja z Data Domain musi być dostępna nie tylko dla Windows ale także dla Linux i wspierać tzw. client direct (transfer danych bezpośrednio na urządzenia deduplikacyjne a tylko metadane wysyłane do systemu backupowego).
91. Niedopuszczalne jest aby licencjonowanie było zależne od ilości składowanych danych (kopii backupowych) na dowolnych nośnikach (np. dysk, taśma VTL...) czy to z deduplikacją czy bez.
92. Niedopuszczalne jest aby licencjonowanie było zależne od ilości komponentów środowiska backupowego, które będą wykorzystywane w procesie backupu czy odtwarzania danych.
93. Niedopuszczalne jest aby licencjonowanie zależne było od ilości serwerów fizycznych czy ich mocy (ilości procesorów) niezależnie czy dane są z nich backupowane bezpośrednio czy tworzą platformę wirtualizacyjną, która jest backupowana.
94. Zaoferowane licencje nie mogą ograniczać wielkości przestrzeni do składowania danych czy replik ich do innych lokalizacji. Jakakolwiek rozbudowa przestrzeni dyskowej czy to w siedzibie podstawowej czy innej nie może wymagać zakupu jakichkolwiek licencji dla systemu.
95. Oferowana licencja oraz architektura systemu musi pozwalać na backup danych na:
- a. nielimitowana ilość bibliotek taśmowych i napędów fizycznych
 - b. nielimitowaną przestrzeń w rozwiązaniach chmurowych (minimum: AWS, Azure, Google)

96. W przypadku wielu lokalizacji licencja musi pozwalać na nielimitowaną replikację danych po deduplikacji pomiędzy lokalizacjami.
97. Zaoferowane licencje nie mogą mieć żadnych ograniczeń czasowych (muszą być wieczyste) dla wszystkich wymaganych funkcjonalności backupowych.
98. Zaoferowane oprogramowanie musi być licencjonowane per ilość maszyn wirtualnych podlegających backupowi niezależnie czy będą wykorzystywani agenci plikowi czy bazodanowi zainstalowani wewnątrz maszyny.
99. Do dostarczonych licencji jest wymagane 36 miesięczne wsparcie producenta lub autoryzowanego partnera serwisowego (pierwsza i druga linia wsparcia świadczona w języku polskim) zapewniające wsparcie techniczne w trybie 8x5 oraz dostęp do bezpłatnych ewentualnych poprawek i uaktualnień.
100. Zaoferowane licencje na system muszą zapewnić backup danych z środowiska maszyn wirtualnych o ilości min. 50 sztuk.
101. Oprogramowanie musi być zakupione w oficjalnym kanale dystrybucyjnym producenta. Na wezwanie Zamawiającego Wykonawca musi dostarczyć oświadczenie producenta oferowanego oprogramowania, potwierdzające pochodzenie oprogramowania z oficjalnego kanału dystrybucyjnego producenta.
102. Zamawiający wymaga licencji wieczystych z gwarancją i serwisem na okres minimum 36 miesięcy, z możliwością przedłużenia. Serwis powinien obejmować wsparcie techniczne, usuwanie usterek oraz aktualizacje oprogramowania.

8.2. Archiwizacja poczty elektronicznej – 1 komplet

Przedmiotem zamówienia jest dostawa oprogramowania do archiwizacji poczty elektronicznej na 1200 skrzynek pocztowych. Zamówienie obejmuje dostawę licencji wieczystej ze wsparciem technicznym na minimum 36 miesięcy.

Wymagania:

1. Serwer systemu archiwizującego pocztę elektroniczną musi mieć możliwość zainstalowania na systemach operacyjnych rodziny Microsoft Windows, co najmniej na:
 - a. Windows 10
 - b. Windows 11
 - c. Windows Server 2025
 - d. Windows Server 2022
 - e. Windows Server 2019
 - f. Windows Server 2016
2. System musi posiadać wbudowany serwer http
3. System musi posiadać wbudowany serwer IMAP
4. System musi posiadać wbudowaną bazę danych, taką, żeby nie było potrzeby instalacji lub podłączania baz danych zewnętrznych dostawców
5. Dostęp administracyjny musi odbywać się poprzez:
 - a. Konsolę webową, do której dostęp odbywa się wyłącznie poprzez bezpieczne połączenie HTTPS
 - b. Aplikację desktopową, która dodatkowo musi umożliwiać logowanie zintegrowane z logowaniem Windowsowym
6. Dostęp użytkownika musi odbywać się poprzez:
 - a. Konsolę webową, do której dostęp odbywa się poprzez zwykłe połączenie HTTP lub bezpieczne połączenie HTTPS
 - b. Aplikację desktopową, która dodatkowo musi umożliwiać logowanie zintegrowane z logowaniem Windowsowym
 - c. Add-in do programu Outlook
 - d. Protokół IMAP polegający na podłączeniu do archiwum z dowolnego klienta pocztowego

- e. Poprzez aplikację webową umożliwiającą dostęp do archiwum z poziomu interfejsu usług Microsoft 365.
- 7. System musi umożliwiać ręczne definiowanie użytkowników oraz administratorów
- 8. System musi posiadać funkcjonalność integracji listy użytkowników z usługami katalogowymi, co najmniej:
 - a. Active Directory
 - b. Google Workspace
 - c. IceWarp
 - d. Kerio Connect
 - e. LDAP Generic
 - f. Mdaemon
 - g. Microsoft 365 (autoryzacja OAuth 2.0)
 - h. Office 365, w tym obsługiwany przez Vianet
- 9. Administrator musi mieć możliwość wyboru, które grupy użytkowników zostaną zsynchronizowane (jeśli usługa katalogowa posiada taką funkcjonalność)
- 10. System musi umożliwić administratorowi na zdefiniowanie uprawnień domyślnych dla nowo synchronizowanych i dodawanych użytkowników
- 11. System musi umożliwić administratorowi zmianę uprawnień dla już zsynchronizowanych i dodanych użytkowników
- 12. System musi posiadać funkcjonalność umożliwiającą włączenie logowania dwuetapowego (MFA) dla użytkowników korzystających z aplikacji.
- 13. System musi pozwalać na podgląd archiwów użytkowników, co najmniej w kwestii:
 - a. Ilości wiadomości w archiwum
 - b. Rozmiaru całkowitego archiwum podanego w MB
 - c. Rozmiaru całkowitego archiwum podanego w %
- 14. System musi umożliwiać automatyczne tworzenie osobnych magazynów przechowujących wiadomości e-mail, z dodatkową możliwością ograniczenia ich do określonej wielkości podanej w GB
- 15. Administrator musi mieć możliwość zdefiniowania położenia magazynu lokalnie, lub zdalnie jako ścieżka UNC lub dysk wirtualny
- 16. System musi mieć wbudowaną możliwość indeksowania wiadomości oraz załączników, nie mniej niż txt, csv, doc, dot, ppt, pps, xls, docx, dotx, pptx, xlsx, odt, ods, odp, pdf
- 17. System musi pozwalać na włączenie lub wyłączenie administratorom dostępu do archiwów innych użytkowników
- 18. System musi pozwalać na zdefiniowanie zasad przechowywania e-maili, które będą dotyczyć okresu czasu, po którym konkretny e-mail będzie mógł zostać usunięty. Zdefiniowane zasady mogą dotyczyć:
 - a. Wszystkich e-maili
 - b. Tylko wiadomości spełniających konkretne kryteria, co najmniej:
 - i. Tematu wiadomości
 - ii. Treści wiadomości
 - iii. Zawartości załączników
 - iv. Nazwy załącznika
 - v. Od kogo została wysłana wiadomość
 - vi. Do kogo została wysłana wiadomość
- 19. System musi posiadać funkcjonalność, która umożliwi na tymczasowe wyłączenie możliwości usuwania wiadomości z archiwów, niezależnie od ustawień zdefiniowanych w zasadach przechowywania
- 20. System musi posiadać funkcjonalność, która umożliwi stworzenie konta audytora, mającego domyślnie prawo do odczytu wszystkich archiwów użytkowników

21. System musi posiadać wbudowany dziennik audytu, który będzie zapisywał wszystkie czynności oraz zmiany dokonywane przez użytkowników w systemie. Dziennik ten musi posiadać okno szczegółów, zawierające informacje o danej akcji, co najmniej:
 - a. Datę i czas wykonania akcji
 - b. Użytkownika, który podjął akcję
 - c. Typ akcji, która została podjęta
 - d. Adres IP, z którego akcja została podjęta
 - e. Typ agenta na którym podjęto akcję
22. System musi posiadać wbudowany wiersz poleceń, który pozwoli na konfigurację ustawień, gdy nie jesteśmy tego w stanie zrobić z poziomu interfejsu graficznego
23. System musi posiadać sekcję zadań, które możemy planować z wyprzedzeniem. Zadania te mogą być wykonywane jednokrotnie lub cyklicznie. Zadania te muszą się odnosić co najmniej do:
 - a. Tworzenia kopii zapasowych
 - b. Sprawdzania integralności danych
 - c. Uruchamiania profili archiwizacji i eksportu
 - d. Synchronizowania bazy użytkowników z usługami katalogowymi
 - e. Wysyłania raportu o stanie systemu
24. Administrator musi mieć możliwość zdefiniowania własnego, niestandardowego zadania w oparciu o API
25. System musi umożliwiać podgląd oraz zarządzanie licencjami
26. System musi umożliwiać zdefiniowanie ustawień SMTP w celu wysyłania raportów
27. System musi umożliwiać podgląd aktywnych sesji użytkowników
28. System powinien posiadać funkcjonalność automatycznego sprawdzania, pobierania oraz instalowania najnowszych wersji systemu
29. System musi umożliwiać tworzenie profili archiwizacji poczty elektronicznej, globalnie przez administratora oraz lokalnie przez użytkownika.
30. Każdy profil archiwizacji musi mieć możliwość ręcznego jego wykonania na żądanie
31. Archiwizacja e-maili musi odbywać się w tle i nie może wpływać na jakość pracy użytkownika
32. Tworząc profil archiwizacji, musimy mieć możliwość wyboru źródła, z którego będziemy te wiadomości archiwizować. Źródłami muszą być co najmniej:
 - a. Serwery poczty elektronicznej, nie mniej niż:
 - i. Microsoft 365
 - ii. Microsoft Exchange
 - iii. Google Workspace
 - iv. Gmail
 - v. MDaemon Email Server
 - vi. Kerio Connect
 - vii. IceWarp Mail Server
 - viii. Dedykowane proxy lub gateway dostarczony przez producenta
 - ix. Innego serwera poczty za pomocą IMAP lub POP3
 - b. Klienci poczty elektronicznej, nie mniej niż:
 - i. Microsoft Outlook
 - ii. Windows Live Mail
 - iii. Mozilla Thunderbird
 - iv. Mozilla SeaMonkey
 - c. Pliki wiadomości, nie mniej niż:
 - i. Pliki EML oraz MSG
 - ii. Plik PST Microsoft Outlook
 - iii. Plik MBOX
33. System musi umożliwiać tworzenie profili eksportu poczty elektronicznej, globalnie przez administratora oraz lokalnie przez użytkownika.

34. Każdy profil eksportu musi mieć możliwość ręcznego jego wykonania na żądanie
35. Eksport e-maili musi odbywać się w tle i nie może wpływać na jakość pracy użytkownika
36. Tworząc profil eksportu, musimy mieć możliwość wyboru miejsca docelowego, na które będziemy te wiadomości wysyłać. Miejscami docelowymi, muszą być co najmniej:
- Serwery poczty elektronicznej, nie mniej niż:
 - Microsoft 365 Skrzynka pocztowa
 - Skrzynka Exchange
 - Google Workspace
 - Gmail
 - Skrzynka IMAP
 - Klienci poczty elektronicznej, nie mniej niż:
 - Microsoft Outlook
 - Mozilla Thunderbird
 - Mozilla SeaMonkey
 - Pliki wiadomości, nie mniej niż:
 - Pliki płaskie
 - Plik PST Microsoft Outlook
37. System musi umożliwiać wyszukiwanie archiwizowanych e-maili w oparciu co najmniej o filtry takie jak:
- Temat
 - Nadawca
 - Odbiorca
 - Treść wiadomości
 - Nazwa plików załączników
 - Zawartość załączników
 - Wsparcie do licencji powinno być realizowane w języku polskim
38. Licencja oprogramowania powinna być bezterminowa wraz ze wsparciem oraz aktualizacjami na okres minimum 36 miesięcy
39. Licencja powinna pozwolić na archiwizację 1200 skrzynek pocztowych
40. Licencja nie powinna wprowadzać ograniczeń, co do ilości i wielkości archiwizowanych wiadomości email
41. Wsparcie do licencji powinno być realizowane w języku polskim.
42. W ramach tego zadania należy również zainstalować i uruchomić nowy system poczty elektronicznej na 1200 kont na licencji Open Source o poniższych wymaganiach:
- System musi zapewnić:
 - Obsługę standardowych protokołów e-mail: SMTP, IMAP, POP3.
 - Nowoczesne i responsywne GUI webmail (Modern Responsive UI).
 - Obsługę załączników i zaawansowane wyszukiwanie wiadomości.
 - Zarządzanie kontaktami, listami dystrybucyjnymi oraz książką adresową Global Address List (GAL).
 - Zarządzanie kalendarzem, zadaniami i planowanie spotkań.
 - Współdzielenie kalendarzy i zasobów.
 - System musi umożliwiać:
 - Integrację z klientami IMAP/POP (np. Thunderbird, Apple Mail).
 - Obsługę Outlook Connector dla klientów MS Outlook.
 - System musi zapewnić:
 - Webową konsolę administracyjną oraz interfejs CLI do zaawansowanego zarządzania.
 - Obsługę wielu domen oraz zarządzanie domenami.
 - System musi posiadać:
 - Wbudowaną ochronę antyspam i antywirus.
 - Uwierzytelnianie dwuskładnikowe (2FA).

- iii. S/MIME do podpisów cyfrowych i szyfrowania wiadomości.
- iv. Obsługę standardów bezpieczeństwa protokołów (TLS/SSL).
- v. Polityki haseł, blokady kont, listy blokowane, filtry antyphishingowe.
- e. Oprogramowanie powinno oferować:
 - i. Backup poczty realizowany na poziomie systemowym (VM / filesystem)
 - ii. Integrację z obiektowymi repozytoriami storage.
- f. Organizacja musi otrzymać:
 - i. Dokumentację techniczną, instrukcje i materiały szkoleniowe dla administratorów.
- g. System musi działać w środowisku serwerowym Linux (x86_64).
- h. Kompatybilny z istniejącym systemem DNS, certyfikatami SSL/TLS, serwerami MX i infrastrukturą mailflow.
- i. Zgodność z obowiązującymi przepisami ochrony danych osobowych (np. RODO) przy przechowywaniu i przetwarzaniu wiadomości.
- j. System poczty musi umożliwiać:
 - i. Obsługę min. 1200 skrzynek z zapewnieniem odpowiedniej przepustowości i SLA dostępności.
 - ii. Możliwość odbudowy usług w oparciu o backup.
 - iii. Monitorowanie zasobów i statystyk pracy usług.
- k. W ramach dostawy wykonawca zobowiązany jest przeprowadzić:
 - i. Szkolenie techniczne dla administratorów (min. 8 godzin szkoleniowych).
 - ii. Migrację obecnych kont pocztowych i wiadomości przechowywanych na serwerze Postfix (wersja 2.11.0) z bazą danych MySQL.
 - iii. Dokumentację wdrożeniową i operacyjną.
- l. System ma obejmować:
 - i. Dostawę licencji na serwer + użytkowników.
 - ii. Instalację i konfigurację środowiska produkcyjnego.
 - iii. Integrację z usługami DNS, systemami bezpieczeństwa i politykami organizacji.
 - iv. Backup & Restore, polityki retencji poczty.

9. Oprogramowanie antywirusowe i EDR/XDR – 1 komplet

Przedmiotem zamówienia jest dostawa, wdrożenie i konfiguracja oprogramowania antywirusowego i EDR/XDR. Oprogramowanie będzie musiało spełniać wymogi operacyjne i technologiczne Zamawiającego, zapewniając pełną integrację z istniejącą infrastrukturą oraz optymalizację działań związanych z cyberbezpieczeństwem. Zamówienie obejmuje dostawę licencji na 600 stanowisk na okres 36 miesięcy.

Wymagania:

1. Administracja zdalna w chmurze:
 - a. Konsola centralnego zarządzania musi być dostępna w wersji lokalnej (on-prem) oraz w wersji chmurowej (SaaS).
 - b. Rozwiązanie musi umożliwiać dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW.
 - c. Rozwiązanie musi być zabezpieczone za pośrednictwem protokołu SSL/TLS.
 - d. Rozwiązanie musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji.
 - e. Rozwiązanie musi posiadać dedykowaną aplikację pochodzącą od tego samego producenta co konsola zarządzająca, umożliwiającą co najmniej:
 - i. Pośredniczenie w komunikacji pomiędzy stacją zarządzaną i serwerem centralnego zarządzania,

- ii. Pośredniczenie w komunikacji pomiędzy stacją zarządzaną a serwerami aktualizacjami producenta,
 - iii. Buforowanie ruchu HTTPS.
 - f. Rozwiązanie musi posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy.
 - g. Rozwiązanie musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej. Uwierzytelnianie dwuskładnikowe musi być realizowane co najmniej przy pomocy następujących aplikacji mobilnych dla systemów iOS oraz Android: Google Authenticator, Microsoft Authenticator, Authy, Aplikacji pochodzącej od tego samego producenta konsoli centralnego zarządzania.
 - h. Rozwiązanie musi posiadać minimum 80 szablonów raportów, przygotowanych przez producenta.
 - i. Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów. Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby zostać umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera.
 - j. Rozwiązanie musi posiadać możliwość uruchomienia zadań automatycznie, przynajmniej z wyzwalaczem: wyrażenie CRON, codziennie, cotygodniowo, comiesięcznie, corocznie, po wystąpieniu nowego zdarzenia oraz po automatycznym umieszczeniu agenta w grupie dynamicznej.
 - k. Konsola centralnego zarządzania musi być dostępna co najmniej w językach polskim oraz angielskim. Język konsoli centralnego zarządzania musi być możliwy do zmiany bez przeinstalowania ani ponownego uruchomienia procesu systemu centralnego zarządzania
 - l. Rozwiązanie musi mieć możliwość tagowania obiektów.
 - m. Rozwiązanie musi posiadać możliwość eksportu danych do zewnętrznych systemów, w tym co najmniej Syslog. 13.1. Eksport danych musi być możliwy w co najmniej następujących formatach: JSON, LEEF, CEF.
2. Ochrona stacji roboczych - Windows:
- a. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11).
 - b. Rozwiązanie musi być dostępne co najmniej w języku polskim oraz angielskim.
 - c. Rozwiązanie musi zapewniać wykrywanie i usuwanie zagrożeń co najmniej typu: wirus, trojan, robak, adware, spyware, dialer, phishing, backdoor.
 - d. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
 - e. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami aktywnymi oraz ukrywającymi się.
 - f. Rozwiązanie musi posiadać ochronę przed podłączeniem hosta do sieci botnet.
 - g. Rozwiązanie musi posiadać funkcjonalność automatycznego przywracania plików po ich zaszyfrowaniu przez oprogramowanie typu ransomware.
 - h. Technologia ta musi być autorskim rozwiązaniem producenta rozwiązania ochrony stacji roboczych.
 - i. Technologia umożliwiająca przywrócenie plików po ich zaszyfrowaniu nie może wykorzystywać mechanizmu VSS (Volume Shadow Copy Service).
 - j. Technologia, która tworzy kopię zapasową plików musi działać w czasie rzeczywistym i zabezpieczać pliki przed modyfikacją przez podejrzane procesy.
 - k. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
 - l. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.

- m. Rozwiązanie musi zapewniać skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem co najmniej: całego dysku, wybranych katalogów, pojedynczych plików, plików spakowanych oraz skompresowanych, dysków sieciowych, dysków przenośnych.
- n. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej: wybranych plików, wybranych procesów, wybranych lokalizacji, wybranych rozszerzeń, nazwy wykrycia, sumy kontrolnej (SHA1).
- o. Rozwiązanie musi integrować się z Intel Threat Detection Technology.
- p. Rozwiązanie musi posiadać system wczesnego ostrzegania oparty na chmurze pochodzący od tego samego producenta oprogramowania antywirusowego, który umożliwia co najmniej:
 - i. Sprawdzenie reputacji działających procesów i plików co najmniej z poziomu interfejsu programu oraz menu kontekstowego.
 - ii. Konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników.
 - iii. Konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy.
- q. Rozwiązanie musi zapewniać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie” (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).
- r. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów co najmniej HTTPS, POP3S, IMAPS.
- s. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyką ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
- t. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników oraz grup urządzeń na stacji w oparciu o co najmniej:
 - i. typ urządzenia: pamięci masowe, optyczne pamięci masowe, pamięci masowe Firewire, urządzenia do tworzenia obrazów, drukarki USB, urządzenia Bluetooth, czytniki kart inteligentnych, modemy, porty LPT/COM, urządzenia przenośne.
 - ii. parametry urządzenia: numer seryjny, producent, model.
 - iii. typ dostępu: brak możliwości zapisu, pełen dostęp, ostrzeżenie użytkownika, brak dostępu.
- u. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:
 - i. tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
 - ii. tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
 - iii. tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
 - iv. tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach,
 - v. tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.

- v. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji:
 - i. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa.
 - ii. Musi istnieć możliwość wygenerowania raportu na temat stacji przy pomocy dedykowanej aplikacji typu standalone pochodzącej od tego samego producenta co oprogramowanie do zabezpieczenia stacji roboczej.
 - iii. Raport musi posiadać co najmniej: Listę zainstalowanych aplikacji, Listę usług systemowych, Informacje o systemie operacyjnym i sprzęcie, Listę aktywnych procesów i połączeń sieciowych, Harmonogram systemu operacyjnego, Szczegóły pliku hosts, Informacje o sterownikach.
- w. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci operacyjnej, z którego korzystają co najmniej następujące funkcje systemu: antywirus, zapora osobista, sandbox, antyspyware, metody heurystyczne.
- x. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń atakujących, jeszcze przed uruchomieniem systemu operacyjnego.
- y. Rozwiązanie musi posiadać ochronę antyspamową realizowaną przez dedykowaną wtyczkę:
 - i. Wtyczka ta musi być dostępna jako plugin dla klienta pocztowego Microsoft Outlook.
 - ii. Ochrona musi być realizowana w oparciu o co najmniej: globalna czarna lista RBL, czarna lista użytkownika, biała lista użytkownika, na którą automatycznie muszą zostać dodane adres email z książki adresowej klienta Microsoft Outlook.
- z. Rozwiązanie musi posiadać wbudowany system IDS, który musi posiadać co najmniej następujące funkcjonalności:
 - i. Ochrona przed anomaliami sieciowymi, w tym co najmniej: Skanowanie portów TCP oraz UDP, Wykrywanie duplikacji adresu IP, Atak zatrutowania ARP, Nieprawidłowa długość pakietu TCP oraz UDP.
 - ii. Ochrona przed atakami typu brute-force dla co najmniej usług oraz protokołów: RDP, SMB, My SQL, MS SQL.
 - iii. Możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.
- aa. Rozwiązanie musi posiadać moduł zapory osobistej, która pochodzi od tego samego producenta rozwiązania antywirusowego:
 - i. Zapora osobista musi działać w oparciu o reguły i musi posiadać co najmniej 60 wbudowanych reguł, stworzonych przez producenta.
 - ii. Zapora osobista musi posiadać co najmniej cztery tryby pracy:
 - A. tryb automatyczny – rozwiązanie blokuje ruch przychodzący i zezwala tylko na połączenia wychodzące,
 - B. tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,
 - C. tryb oparty na regułach – rozwiązanie blokuje ruch przychodzący i wychodzący,
 - D. tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość skonfigurowania czasu działania trybu.
- bb. Rozwiązanie musi posiadać moduł bezpiecznej przeglądarki, pochodzący od producenta tego samego rozwiązania antywirusowego:

- i. Bezpieczna przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika.
 - ii. Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki.
 - iii. W przypadku połączenia aplikacji zdalnej (w tym przynajmniej aplikacja TeamViewer) kolor ramki musi ulec zmianie oraz musi pojawić się alert informujący o zdalnym połączeniu.
 - cc. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych pochodzący od tego samego producenta:
 - i. Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 160 kategorii i podkategorii.
 - ii. Rozwiązanie musi umożliwiać stworzenie własnego komunikatu na zablokowanych stronach w oparciu o co najmniej: Treść komunikatu, Obraz.
3. Ochrona stacji roboczych – MacOS:
- a. Rozwiązanie musi posiadać pełne wsparcie dla systemów macOS 11 (Big Sur) oraz nowszych.
 - b. Rozwiązanie musi być dostępne co najmniej w języku polskim oraz angielskim.
 - c. Rozwiązanie musi zapewniać wykrywanie i usuwanie zagrożeń co najmniej typu: wirus, trojan, robak, adware, spyware, dialer, phishing, backdoor.
 - d. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
 - e. Rozwiązanie musi posiadać możliwość skanowanie w czasie rzeczywistym otwieranych, tworzonych i wykonywanych plików.
 - f. Rozwiązanie musi chronić pliki co najmniej za pomocą: sygnatur wirusów, reputacji chmurowej. Rozwiązanie musi umożliwiać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP "w locie" (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).
 - g. Rozwiązanie musi posiadać system wczesnego ostrzegania oparty na chmurze pochodzący od tego samego producenta oprogramowania antywirusowego, który umożliwia co najmniej:
 - i. Sprawdzenie reputacji działających aplikacji i plików co najmniej z poziomu interfejsu programu.
 - ii. Konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników.
 - iii. Konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy.
 - h. Rozwiązanie musi zapewniać skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem co najmniej: całego dysku, wybranych katalogów, pojedynczych plików, plików spakowanych oraz skompresowanych, dysków sieciowych, dysków przenośnych.
 - i. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej: wybranych plików, wybranych procesów, wybranych lokalizacji, wybranych rozszerzeń, nazwy wykrycia, sumy kontrolnej (SHA1).
 - j. Rozwiązanie musi posiadać moduł zapory osobistej, która pochodzi od tego samego producenta rozwiązania antywirusowego:
 - i. Zapora osobista musi działać w oparciu o reguły i musi posiadać co najmniej 30 wbudowanych reguł, stworzonych przez producenta.
 - ii. Zapora osobista musi posiadać co najmniej dwa tryby pracy:

- A. tryb automatyczny – rozwiązanie blokuje ruch przychodzący i zezwala tylko na połączenia wychodzące,
 - B. tryb oparty na regułach – rozwiązanie blokuje ruch przychodzący i wychodzący,
- 4. Ochrona stacji roboczych – Linux:
 - a. Rozwiązanie musi wspierać co najmniej następujące systemy operacyjne: Ubuntu Desktop, Red Hat Enterprise Linux, Linux Mint.
 - b. Rozwiązanie musi obsługiwać co najmniej następujące środowiska pulpitu: Cinnamon, GNOME, KDE, MATE, XFCE.
 - c. Rozwiązanie musi zapewniać wykrywanie i usuwanie zagrożeń co najmniej typu: wirus, trojan, robak, adware, spyware, dialer, phishing, backdoor.
 - d. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
 - e. Rozwiązanie musi posiadać możliwość skanowanie w czasie rzeczywistym otwieranych, tworzonych i wykonywanych plików.
 - f. Rozwiązanie musi posiadać system wczesnego ostrzegania oparty na chmurze pochodzący od tego samego producenta oprogramowania antywirusowego, który umożliwia co najmniej:
 - i. Konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników.
 - ii. Konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy.
 - g. Rozwiązanie musi zapewniać skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem co najmniej: całego dysku, wybranych katalogów, pojedynczych plików, plików spakowanych oraz skompresowanych, dysków sieciowych, dysków przenośnych.
 - h. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej: wybranych plików, wybranych procesów, wybranych lokalizacji, wybranych rozszerzeń,
 - i. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników oraz grup urządzeń na stacji w oparciu o co najmniej:
 - i. typ urządzenia: pamięci masowe, optyczne pamięci masowe,
 - ii. parametry urządzenia: numer seryjny, producent, model.
 - iii. typ dostępu: brak możliwości zapisu, pełen dostęp, brak dostępu.
- 5. Ochrona serwera – Windows Server:
 - a. Rozwiązanie musi wspierać systemy w tym co najmniej: Microsoft Windows Server 2012 R2, Microsoft Windows Server 2016, Microsoft Windows Server 2019, Microsoft Windows Server 2022, Microsoft Windows Server 2025.
 - b. Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.
 - c. Rozwiązanie musi zapewniać wykrywanie i usuwanie zagrożeń co najmniej typu: wirus, trojan, robak, adware, spyware, dialer, phishing, backdoor.
 - d. Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS.
 - e. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.

- f. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji.
- g. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.
- h. Rozwiązanie musi posiadać system wczesnego ostrzegania oparty na chmurze pochodzący od tego samego producenta oprogramowania antywirusowego, który umożliwia co najmniej:
 - i. Sprawdzenie reputacji działających procesów i plików co najmniej z poziomu interfejsu programu oraz menu kontekstowego.
 - ii. Konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników.
 - iii. Konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy.
- i. Rozwiązanie musi zapewniać skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem co najmniej: całego dysku, wybranych katalogów, pojedynczych plików, plików spakowanych oraz skompresowanych, dysków sieciowych, dysków przenośnych.
- j. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej: wybranych plików, wybranych procesów, wybranych lokalizacji, wybranych rozszerzeń, nazwy wykrycia, sumy kontrolnej (SHA1).
- k. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.
- l. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:
 - i. tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
 - ii. tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
 - iii. tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
 - iv. tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach,
 - v. tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.
- m. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji:
 - i. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa.
 - ii. Musi istnieć możliwość wygenerowania raportu na temat stacji przy pomocy dedykowanej aplikacji typu standalone pochodzącej od tego samego producenta co oprogramowanie do zabezpieczenia stacji roboczej.
 - iii. Raport musi posiadać co najmniej: listę zainstalowanych aplikacji, listę usług systemowych, informacje o systemie operacyjnym i sprzęcie, listę aktywnych procesów i połączeń sieciowych, harmonogram systemu operacyjnego, szczegóły pliku hosts, informacje o sterownikach.
- n. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci operacyjnej, z którego korzystają co najmniej następujące funkcje systemu: antywirus, zaporą osobista, sandbox, antyspyware, metody heurystyczne.
- o. Rozwiązanie musi skanować system wirtualny w trybie online oraz offline w środowisku Hyper-V.

- p. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
 - q. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników oraz grup urządzeń na stacji w oparciu o co najmniej:
 - i. typ urządzenia: pamięci masowe, optyczne pamięci masowe, pamięci masowe Firewire, urządzenia do tworzenia obrazów, drukarki USB, urządzenia Bluetooth, czytniki kart inteligentnych, modemy, porty LPT/COM, urządzenia przenośne.
 - ii. parametry urządzenia: numer seryjny, producent, model.
 - iii. typ dostępu: brak możliwości zapisu, pełen dostęp, ostrzeżenie użytkownika, brak dostępu.
 - r. Rozwiązanie musi automatycznie wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki co najmniej dla następujących usług: MS SQL, Active Directory, IIS, Sysvol, DNS, DHCP, Hyper-V, Konsola centralnego zarządzania tego samego producenta rozwiązania antywirusowego.
 - s. Rozwiązanie musi posiadać wbudowany system IDS, który musi posiadać co najmniej następujące funkcjonalności:
 - i. Ochrona przed anomaliami sieciowymi, w tym co najmniej: Skanowanie portów TCP oraz UDP, Wykrywanie duplikacji adresu IP, Atak zatrutowania ARP, Nieprawidłowa długość pakietu TCP oraz UDP.
 - ii. Ochrona przed atakami typu brute-force dla co najmniej usług oraz protokołów: RDP, SMB, My SQL, MS SQL.
 - iii. Możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.
 - t. Rozwiązanie musi posiadać moduł zapory osobistej, która pochodzi od tego samego producenta rozwiązania antywirusowego.
 - u. Zapora osobista musi działać w oparciu o reguły i musi posiadać co najmniej 60 wbudowanych reguł, stworzonych przez producenta. Zapora osobista musi posiadać co najmniej cztery tryby pracy:
 - i. tryb automatyczny – rozwiązanie blokuje ruch przychodzący i zezwala tylko na połączenia wychodzące,
 - ii. tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,
 - iii. tryb oparty na regułach – rozwiązanie blokuje ruch przychodzący i wychodzący,
 - iv. tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące.
 - v. Administrator musi posiadać możliwość skonfigurowania czasu działania trybu.
6. Ochrona serwera – Linux:
- a. Rozwiązanie musi wspierać systemy w tym co najmniej: RedHat Enterprise Linux (RHEL), Rocky Linux, Ubuntu, Debian, SUSE Linux Enterprise Server (SLES), Oracle Linux, Amazon Linux.
 - b. Rozwiązanie musi zapewniać wykrywanie i usuwanie zagrożeń co najmniej typu: wirus, trojan, robak, adware, spyware, dialer, phishing, backdoor.
 - c. Rozwiązanie musi zapewniać możliwość zdalnego skanowania przy pomocy protokołu ICAP oraz ICAPS.
 - d. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.

- e. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji.
 - f. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.
 - g. Rozwiązanie musi posiadać system wczesnego ostrzegania oparty na chmurze pochodzący od tego samego producenta oprogramowania antywirusowego, który umożliwia co najmniej:
 - i. Konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników.
 - ii. Konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy.
 - h. Rozwiązanie musi zapewniać skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem co najmniej: całego dysku, wybranych katalogów, pojedynczych plików, plików spakowanych oraz skompresowanych, dysków sieciowych, dysków przenośnych.
 - i. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej: wybranych plików, wybranych procesów, wybranych lokalizacji, wybranych rozszerzeń.
 - j. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej. Lokalna konsola administracyjna nie może wymagać do swojej pracy uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web.
 - k. Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, musi w pełni wspierać rozwiązanie Dell EMC Isilon.
 - l. Rozwiązanie musi działać w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszonego mikro-serwisu.
 - m. Rozwiązanie musi wykrywać oraz podejrzane działania w kontenerach i blokować je. Ochrona musi skanować kontener co najmniej w następujących fazach: proces budowania obrazu kontenera, wdrażanie obrazu kontenera.
7. Mobile Device Management:
- a. Konsola centralnego zarządzania dostępna w wersji chmurowej musi posiadać możliwość zarządzania urządzeniami mobilnymi – MDM.
 - b. MDM musi pochodzić od tego samego producenta konsoli centralnego zarządzania.
 - c. MDM musi umożliwiać zarządzanie urządzeniami mobilnymi z systemami: Android, iOS, iPadOS.
 - d. MDM musi posiadać możliwość integracji co najmniej z następującymi rozwiązaniami: Microsoft Entra ID (co najmniej w zakresie synchronizacji użytkowników), Microsoft Intune (co najmniej w zakresie automatycznej rejestracji urządzenia mobilnego z systemem Android w konsoli zdalnego zarządzania), VMware Workspace One (co najmniej w zakresie automatycznej rejestracji urządzenia mobilnego z systemem Android w konsoli zdalnego zarządzania), Apple Business Manager (ABM), Android Enterprise (co najmniej w zakresie Device Owner).
 - e. MDM musi zapewniać wystanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi: usunięcie zawartości urządzenia, przywrócenie urządzenia do ustawień fabrycznych, zablokowanie urządzenia, uruchomienie sygnału dźwiękowego, lokalizację GPS, resetowanie hasła blokady ekranu.
 - f. MDM musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji.
 - g. MDM musi umożliwiać co najmniej:
 - i. Dla systemów iOS oraz iPadOS: konfigurację kont e-mail, konfigurację połączeń VPN, konfigurację połączeń Wi-Fi, konfigurację listy certyfikatów, możliwość uruchomienia trybu jednej aplikacji.

- ii. Dla systemu Android: blokadę wykonywania połączeń, blokadę konfiguracji sieci Wi-Fi, blokadę konfiguracji tuneli VPN, zarządzanie aktualizacjami systemu operacyjnego, blokadę zmiany tapety urządzenia.
- 8. Mobile Threat Defense (MTD) dla systemu Android:
 - a. Rozwiązanie musi posiadać pełne wsparcie dla systemów Android 9 (Pie) oraz nowszych.
 - b. Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania:
 - i. Inteligentne – tylko skanowanie aplikacji w pamięci wewnętrznej i na karcie SD.
 - ii. Dokładne - skanowanie wszystkich typów plików w pamięci wewnętrznej i na karcie SD.
 - c. Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki).
 - d. Rozwiązanie musi posiadać możliwość zdefiniowania poziomu zabezpieczeń urządzenia w tym przynajmniej:
 - i. Złożoność kodu blokady ekranu: Wzór, PIN, Hasło,
 - ii. Przywrócenie urządzenia do ustawień fabrycznych w przypadku przekroczenia dopuszczalnej liczby prób odblokowania ekranu,
 - iii. Zdefiniowanie czasu obowiązywania (ważności) kodu blokady ekranu.
 - e. Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o: nazwę aplikacji, nazwę pakietu, kategorię sklepu Google Play, uprawnienia aplikacji, pochodzenie aplikacji z nieznanego źródła.
 - f. Rozwiązanie musi posiada ochronę przed zagrożeniami typu phishing.
- 9. Sandbox w chmurze:
 - a. Rozwiązanie musi być integralną częścią oprogramowania antywirusowego, bez potrzeby instalacji dodatkowych rozszerzeń.
 - b. Rozwiązanie musi pochodzić od tego samego producenta rozwiązania antywirusowego.
 - c. Rozwiązanie musi wspierać systemy w tym co najmniej: Microsoft Windows 10 oraz 11, Microsoft Windows Server, macOS 11 (Big Sur) oraz nowszych, RedHat Enterprise Linux (RHEL), Rocky Linux, Ubuntu, Debian, SUSE Linux Enterprise Server (SLES), Oracle Linux, Amazon Linux.
 - d. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.
 - e. Rozwiązanie musi wykorzystywać do działania chmurę producenta tego samego rozwiązania antywirusowego.
 - f. Rozwiązanie musi posiadać możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym co najmniej: archiwa, skrypty, pliki wykonywalne, pliki rejestru systemowego (.reg), możliwy spam, dokumenty.
 - g. Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta w tym co najmniej: natychmiast po ich przeanalizowaniu, po upływie 30 dni, nigdy.
 - h. Administrator musi mieć możliwość zdefiniowania maksymalnego rozmiaru przesyłanych próbek.
 - i. Rozwiązanie musi pozwalać na utworzenie listy wykluczeń określonych plików lub folderów z przesyłania.
 - j. Administrator musi mieć możliwość podejrzenia listy plików, które zostały przesłane do analizy z poziomu konsoli centralnego zarządzania.
 - k. Rozwiązanie musi pozwalać na analizowanie plików, bez względu na lokalizację stacji roboczej. W przypadku wykrycia zagrożenia, całe środowisko jest bezzwłocznie chronione.
 - l. Rozwiązanie pozwala na wysłanie dowolnej próbki do analizy przez użytkownika, za pomocą wspieranego produktu. Administrator musi mieć dostęp do informacji jakie pliki zostały wysłane oraz przez kogo zostały wysłane.

- m. Przeanalizowane pliki muszą zostać odpowiednio oznaczone. Analiza pliku musi zakończyć się jednym z poniższych wyników: czysty, podejrzany, bardzo podejrzany, szkodliwy.
- n. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość co najmniej wstrzymania uruchamiania pobieranych plików z następujących źródeł: przeglądarki internetowe, programy poczty e-mail, nośniki wymienne, pliki wyodrębnione z archiwum.
- o. Wykryte zagrożenia muszą być przeniesione w bezpieczny obszar kwarantanny, z której administrator może przywrócić pliki poddane kwarantannie oraz utworzyć dla nich wyłączenia z poziomu konsoli centralnego zarządzania oraz z poziomu klienta antywirusowego.

10. Szyfrowanie:

- a. Rozwiązanie musi pochodzić od tego samego producenta rozwiązania antywirusowego.
- b. Rozwiązanie nie może bazować na rozwiązaniu Microsoft Bitlocker.
- c. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11).
- d. Rozwiązanie musi umożliwiać zarządzanie natywnym szyfrowaniem w systemach macOS (FileVault) poprzez dedykowanego klienta pochodzącego od tego samego producenta rozwiązania antywirusowego.
- e. Rozwiązanie musi posiadać autentykację typu pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny:
 - i. Rozwiązanie musi umożliwiać całkowite oraz czasowe wyłączenia tego uwierzytelnienia.
 - ii. Uwierzytelnienie użytkownika musi odbywać się poprzez hasło, którego złożoność może ustalić administrator konsoli centralnego zarządzania.
- f. W przypadku gdy użytkownik zapomni hasła, administrator musi mieć możliwość wygenerowania hasła odzyskiwania z poziomu konsoli centralnego zarządzania:
 - i. Hasło odzyskiwania po użyciu musi zostać zmodyfikowane.
 - ii. Hasło odzyskiwania nie może być krótsze niż 8 znaków.
 - iii. Hasło odzyskiwania nie może być dłuższe niż 20 znaków.
- g. Rozwiązanie musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI.
- h. Rozwiązanie musi umożliwiać zalogowanie się do systemu przy pomocy metody jednokrotnego logowania (SSO) przy wykorzystaniu poświadczeń użytkownika Active Directory.
- i. Rozwiązanie musi umożliwiać wykorzystanie modułu TPM w wersji co najmniej 2.0.
- j. Rozwiązanie musi wspierać dyski wykorzystujące funkcji OPAL w wersji co najmniej 2.0.
- k. W przypadku awarii urządzenia, administrator musi mieć możliwość wygenerowania pliku odzyskiwania który umożliwia odszyfrowanie dysku.

11. Endpoint Detection and Response / eXtended Detection and Response:

- a. Moduł EDR / XDR musi pochodzić od tego samego producenta rozwiązania antywirusowego.
- b. Ochrona EDR /XDR musi być realizowana przy pomocy dedykowanego konektora, który musi pochodzić od tego samego producenta rozwiązania antywirusowego.
- c. Rozwiązanie musi zbierać co najmniej następujące informacje z systemu operacyjnego:
 - i. tworzenie procesów,
 - ii. uruchamianie, zatrzymanie i modyfikacja usług,
 - iii. utworzenie, uruchomienie, modyfikacja oraz usunięcie zadań w harmonogramie systemowym,
 - iv. usuwanie oraz zmiana nazw plików,
 - v. tworzenie i usuwanie kluczy rejestru systemowego,
 - vi. ładowanie bibliotek DLL,
 - vii. zalogowanie użytkowników,

- viii. elementy sieciowe, w tym co najmniej: pobranie plików wykonywalnych, zestawienie połączeń TCP/IP, zapytania HTTP, zapytania DNS.
- d. Rozwiązanie musi posiadać ponad 1500 wbudowanych reguł, po których wystąpieniu, nastąpi wyzwolenie alarmu bezpieczeństwa:
 - i. Administrator powinien mieć możliwość edytowania akcji przypisanych do reguł utworzonych zarówno przez producenta, jak i przez siebie, a także możliwość wdrażania automatyzacji tych reguł, opartych co najmniej na następujących akcjach: blokowanie pliku wykonywalnego, blokowanie pliku wykonywalnego i poddanie go kwarantannie, blokowanie podejrzanej biblioteki DLL, zakończenie procesu, skanowanie komputera w poszukiwaniu zagrożeń, wyłączenie komputera, izolacja sieciowa hosta, wylogowanie użytkownika.
 - ii. Administrator musi posiadać możliwość utworzenia własnych reguł w oparciu o język XML.
- e. Rozwiązanie musi posiadać możliwość tworzenia wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa:
 - i. Utworzenie wykluczenia musi automatycznie rozwiązywać alarmy historyczne, które pasują do utworzonego wykluczenia.
 - ii. Podstawowe wykluczenia muszą być konfigurowane w oparciu o przynajmniej: proces, proces nadrzędny (proces rodzica), nazwę procesu, ścieżkę procesu, wiersz polecenia, wydawcę, typ podpisu, SHA-1, SHA-2, użytkownika.
 - iii. Administrator musi mieć możliwość utworzenia wykluczeń zaawansowanych w oparciu o język XML.
- f. Rozwiązanie musi mieć możliwość blokowania plików po sumach kontrolnych:
 - i. W ramach blokady musi istnieć możliwość dodania komentarza oraz konfiguracji usuwania blokowanego pliku.
 - ii. Blokowanie pliku musi być możliwe na podstawie co najmniej następujących funkcji skrótu (funkcje hashujące): SHA-1, SHA-256.
- g. Rozwiązanie musi dawać możliwość weryfikacji plików wykonywalnych w środowisku z możliwością podglądu szczegółów wybranego pliku w tym przynajmniej: hash pliku SHA-1, hash pliku SHA-256, hash pliku MD5, typ sygnatury podpisu cyfrowego, wydawcę certyfikatu, wersję pliku, oryginalną nazwę pliku, rozmiar pliku, reputację i popularność pliku w oparciu o system reputacji producenta tego samego rozwiązania antywirusowego, pierwsze uruchomienie pliku w środowisku, ostatnie uruchomienie pliku w środowisku,
- h. Rozwiązanie musi dawać możliwość wykonywania następujących czynności dla plików wykonywalnych oraz plików DLL: oznaczania ich jako bezpieczne lub niebezpieczne, pobierania ich do dalszej analizy, a pobierany plik musi być zabezpieczony hasłem, zablokowania wykonywania i wykorzystania pliku, wysyłania do sandbox tego samego producenta rozwiązania antywirusowego.
- i. Rozwiązanie musi dawać możliwość weryfikacji uruchomionych skryptów w środowisku wraz z informacją dotyczącą parametrów uruchomienia (wiersz poleceń):
 - i. Administrator musi posiadać możliwość oznaczenia skryptu jako bezpieczny lub niebezpieczny,
 - ii. pobierania ich do dalszej analizy, a pobierany plik musi być zabezpieczony hasłem,
 - iii. wysyłania do sandbox tego samego producenta rozwiązania antywirusowego,
 - iv. administrator musi posiadać możliwość szczegółowego podglądu wykonanych przez skrypt czynności w formie tekstowej.
- j. Rozwiązanie musi umożliwiać zestawienie sesji terminalowej powershell do stacji końcowej oraz serwera. Moduł połączenia terminalowego musi być dostępny jedynie dla

użytkowników konsoli posiadających skonfigurowane dwuskładnikowe uwierzytelnienia do konsoli.

- k. Rozwiązanie musi posiadać mechanizm sztucznej inteligencji, który będzie wspomagał administratora w tworzeniu wykluczeń dla pojawiających się w środowisku alertów.
 - l. Rozwiązanie musi wspierać integrację z zewnętrznymi silnikami do przeprowadzenia głębszej analizy plików, w tym co najmniej VirusTotal.
12. Zamawiający wymaga licencji dla 600 stanowisk na okres 36 miesięcy, z możliwością przedłużenia. Licencja powinna obejmować wsparcie techniczne, usuwanie usterek oraz aktualizacje oprogramowania.
13. Oprogramowanie musi być zakupione w oficjalnym kanale dystrybucyjnym producenta. Na wezwanie Zamawiającego Wykonawca musi dostarczyć oświadczenie producenta oferowanego oprogramowania, potwierdzające pochodzenie oprogramowania z oficjalnego kanału dystrybucyjnego producenta.

10. Przetątnik dostępowy PoE – 10 sztuk

Przedmiotem zamówienia jest 10 szt. przetątników dostępowych PoE z licencjami N1-CloudCampus,Foundation na min. 3 lata umożliwiającą podłączenie do systemu zarządzania iMaster NCE-Campus będącego w posiadaniu Zamawiającego.

Wymagania:

1. Przetątnik musi być dedykowanym urządzeniem sieciowym przystosowanym do zainstalowania w szafie rack. Wraz z urządzeniem należy dostarczyć niezbędne akcesoria umożliwiające instalację przetątnika w szafie rack. System operacyjny (firmware) dostarczony przez producenta urządzenia. Zamawiający nie dopuszcza dostarczenia urządzenia z zainstalowanym systemem operacyjnym firmy trzeciej.
2. Wymagane parametry fizyczne:
 - a. możliwość montażu w stelażu/szafie 19"
 - b. wysokość maksymalna 1U
 - c. wewnętrzny zasilacz 230V AC (nie dopuszcza się rozwiązania zewnętrznego).
 - d. zakres temperatur pracy ciągłej co najmniej od -5 do +50 °C
 - e. zakres wilgotności pracy co najmniej 5% - 95%
 - f. port USB do obrazów systemu, konfiguracji i certyfikatów
 - g. ochrona przed przepięciami: ±6 kV
 - h. MTBF: minimum 35 lat
3. Przetątnik musi posiadać minimum:
 - a. 48 portów 10/100/1000BASE-T PoE+ zgodnych z 802.3af oraz 802.3at. Budżet mocy PoE minimum 840 W.
 - b. 4 porty 10GE SFP+
 - c. Każde urządzenie należy dostarczyć 2 wkładkami 10GE SFP+ SM LC oraz 2 wkładkami 10GE SFP+ MM LC
 - d. Każde urządzenie musi zostać dostarczone razem z oryginalnym kablem DAC SFP+ 10G 1m
4. Wszystkie porty muszą być dostępne od frontu urządzenia.
5. Funkcje PoE: Perpetual PoE (utrzymanie zasilania PD podczas restartu), Fast PoE (zasilanie natychmiast po uruchomieniu)
6. Urządzenie musi być wyposażone w minimum 2 moduły wentylatorów.
7. System chłodzenia powietrzem z automatyczną regulacją prędkości wentylatorów
8. Przetątnik musi umożliwiać łączenie w stosy z zachowaniem następującej funkcjonalności:
 - a. Zarządzanie stosem poprzez jeden adres IP
 - b. Do min. 9 jednostek w stosie
 - c. Magistrala stackująca o wydajności minimum 40Gb/s

- d. Możliwość tworzenia połączeń link aggregation zgodnie z 802.3ad dla portów należących do różnych jednostek w stosie (ang. cross-stack link aggregation)
 - e. Stos przełączników powinien być widoczny w sieci jako jedno urządzenie logiczne z punktu widzenia protokołu Spanning-Tree
 - f. Zachowanie konfiguracji przy wymianie jednostki w stosie
 - g. Jeżeli realizacja funkcji łączenia w stosy wymaga dodatkowych interfejsów stackujących to w ramach niniejszego postępowania Zamawiający wymaga ich dostarczenia wraz z kablami stackującymi o długości min. 1m
9. Układ przełączający o wydajności min. 224 Gbps, wydajność przełączania przynajmniej 168 Mpps
10. Obsługa min. 32 000 adresów MAC
11. Wbudowana pamięć RAM min. 2 GB. Procesor min. dwurdzeniowy o taktowaniu min. 1 GHz.
12. Obsługa min. 4000 sieci VLAN jednocześnie oraz obsługa 802.1Q tunneling (QinQ)
13. Możliwość skonfigurowania min. 1000 interfejsów VLANIF działających równocześnie
14. Obsługa standardów IEEE:
- a. CFM zgodny z 802.1ag
 - b. EFM zgodny z 802.3ah
15. Obsługa standardu Y.1731
16. Obsługa mechanizmów ERPS G.8032
17. Obsługa protokołu HSRP IPv4 i IPv6 lub VRRP IPv4 i IPv6
18. Obsługa protokołu GVRP lub GARP
19. Wsparcie dla protokołów IEEE 802.1w Rapid Spanning Tree oraz IEEE 802.1s Multi-Instance Spanning Tree.
20. Obsługa min. 4 000 tras dla routingu IPv4
21. Obsługa min. 1 000 tras dla routingu IPv6
22. Obsługa protokołów routingu OSPF, OSPFv3, RIP, RIPv6, PIM-SM, PIM-DM. Jeżeli do obsługi powyższych funkcjonalności wymagana jest licencja to należy ją dostarczyć w ramach niniejszego postępowania
23. Obsługa protokołów LLDP i LLDP-MED.
24. Obsługa protokołu Bidirectional Forwarding Detection (BFD)
25. Przełącznik musi posiadać funkcjonalność DHCP Server, DHCP relay, DHCP client
26. Obsługa ruchu multicast:
- a. IGMP v1, v2 i v3
 - b. IGMP Snooping v1, v2 i v3
27. Mechanizmy związane z zapewnieniem bezpieczeństwa sieci:
- a. autoryzacja użytkowników w oparciu o IEEE 802.1x
 - b. możliwość utworzenia minimum 2000 list ACL dla IPv4 i IPv6
 - c. możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC zarządzanie urządzeniem przez HTTPS, SNMP i SSHv2 za pomocą protokołów IPv4 i IPv6
 - d. możliwość filtrowania ruchu w oparciu o adresy MAC, IPv4, IPv6, porty TCP/UDP
 - e. obsługa mechanizmów Port Security oraz Dynamic ARP Inspection
 - f. możliwość synchronizacji czasu zgodnie z NTP
28. Obsługa funkcjonalności UDLD lub DLDP lub równoważnej
29. Implementacja co najmniej ośmiu kolejek sprzętowych QoS na każdym porcie wyjściowym z możliwością konfiguracji dla obsługi ruchu o różnych klasach:
- a. klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy adres MAC, docelowy adres MAC, źródłowy adres IP, docelowy adres IP, źródłowy port TCP, docelowy port TCP
 - b. wsparcie dla mechanizmów QoS z wykorzystaniem algorytmu karuzelowego, np.: WRR, WDRR, DRR
30. Urządzenie musi posiadać mechanizm do badania jakości połączeń (IP SLA) z możliwością badania takich parametrów jak: jitter, opóźnienie, straty pakietów dla wygenerowanego

strumienia testowego UDP. Urządzenie musi mieć możliwość pracy jako generator oraz jako odbiornik pakietów testowych IP SLA. Urządzenie musi umożliwiać konfigurację liczby wysyłanych pakietów UDP w ramach pojedynczej próbki oraz odstępu czasowego pomiędzy kolejnymi wysyłanymi pakietami UDP w ramach pojedynczej próbki. Jeżeli funkcjonalność IP SLA wymaga licencji to Zamawiający wymaga jej dostarczenia w ramach niniejszego postępowania

31. Wymagane opcje zarządzania:

- a. możliwość lokalnej i zdalnej obserwacji ruchu na określonym porcie, polegająca na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do urządzenia
- b. plik konfiguracyjny urządzenia musi być możliwy do edycji w trybie off-line (tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC)
- c. urządzenie musi posiadać wbudowany port USB pozwalający na podłączenie zewnętrznej pamięci FLASH w celu przechowywania obrazów systemu operacyjnego, plików konfiguracyjnych lub certyfikatów elektronicznych
- d. dedykowany port konsoli musi być zgodny ze standardem RS-232

32. Urządzenie musi być fabrycznie nowe i nieużywane wcześniej w żadnych projektach, wyprodukowane nie wcześniej niż 6 miesięcy przed dostawą i nieużywane przed dniem dostarczenia z wyłączeniem używania niezbędnego dla przeprowadzenia testu ich poprawnej pracy.

33. Urządzenia muszą pochodzić z autoryzowanego kanału dystrybucji producenta przeznaczonego na teren Unii Europejskiej, a korzystanie przez Zamawiającego z dostarczonego produktu nie może stanowić naruszenia majątkowych praw autorskich osób trzecich.

34. Zamawiający wymaga, aby przetącniki posiadały 3-letni serwis gwarancyjny świadczony przez Wykonawcę (lub autoryzowany serwis) na bazie wsparcia serwisowego wykupionego u producenta oferowanych urządzeń. Wymiana uszkodzonego elementu w trybie 9x5xNBD. Okres gwarancji liczony będzie od daty sporządzenia protokołu zdawczo-odbiorczego przedmiotu zamówienia. Zamawiający na etapie dostawy będzie wymagał oświadczenia producenta potwierdzającego nabycie oraz zarejestrowanie serwisu gwarancyjnego na Zamawiającego. Wszystkie koszty związane z naprawami gwarancyjnymi nie mogą obciążać Zamawiającego (np. koszty wysyłki).

35. Bezpłatny dostęp do najnowszych wersji oprogramowania na stronie producenta przez cały okres serwisu gwarancyjnego dla urządzeń.

36. Przetącnik musi dostarczony z licencją N1-CloudCampus,Foundation na min. 3 lata umożliwiającą podłączenie do systemu zarządzania iMaster NCE-Campus będącego w posiadaniu Zamawiającego.

11. Przetącnik szkieletowy – 2 sztuki

Przedmiotem zamówienia są 2 szt. przetącników szkieletowych z licencjami N1-CloudCampus,Foundation na min. 3 lata umożliwiającą podłączenie do systemu zarządzania iMaster NCE-Campus będącego w posiadaniu Zamawiającego.

Wymagania:

1. Przetącnik musi być dedykowanym urządzeniem sieciowym przystosowanym do zainstalowania w szafie rack. Wraz z urządzeniem należy dostarczyć niezbędne akcesoria umożliwiające instalację przetącnika w szafie rack. Przetącnik musi posiadać system operacyjny (firmware) dostarczony przez producenta urządzenia; zamawiający nie dopuszcza dostarczenia urządzenia z zainstalowanym systemem operacyjnym firmy trzeciej.
2. Wymagane parametry fizyczne:
 - a. możliwość montażu w stelażu/szafie 19”

- b. dwa wewnętrzne redundantne zasilacze 230V AC typu hot-swap (nie dopuszcza się rozwiązania zewnętrznego). Każde urządzenie musi zostać dostarczone z 2 zasilaczami umożliwiające wymianę w trakcie pracy urządzenia (ang. hot-swap).
 - c. zakres temperatur pracy ciągłej co najmniej od -5 do +45 °C
 - d. zakres wilgotności pracy co najmniej 5% - 95%
 - e. port USB umożliwiający podłączenie zewnętrznej pamięci flash
 - f. ochrona przed przepięciami: ± 3 kV
 - g. MTBF: minimum 40 lat
3. Przepływ powietrza przód-tył (od strony portów w kierunku zasilaczy)
4. Urządzenie musi być wyposażone w 4 moduły wentylatorów umożliwiające wymianę w trakcie pracy urządzenia (ang. hot-swap).
5. Przetątnik musi posiadać:
 - a. min 24 porty 10GE SFP+
 - b. min 4 porty 40GE/100GE QSFP28 (Jeśli obsługa portów 100GE wymaga dodatkowej licencji to Zamawiający nie wymaga jej dostarczenia, ale zastrzega, aby była możliwość rozbudowy w przyszłości)
6. Wszystkie powyższe porty muszą być dostępne od frontu urządzenia.
7. Każde urządzenie należy dostarczyć z 2 wkładkami 40GE SM LC, 2 wkładkami 40GE MM LC, 12 wkładkami 10GE SFP+ SM LC oraz 12 wkładkami 10GE SFP+ MM LC
8. Przetątnik musi umożliwiać łączenie w stosy z zachowaniem następującej funkcjonalności:
 - a. Zarządzanie stosem poprzez jeden adres IP
 - b. Do min. 9 jednostek w stosie
 - c. Magistrała stackująca o wydajności min. 160Gb/s
 - d. Możliwość tworzenia połączeń link aggregation zgodnie z 802.3ad dla portów należących do różnych jednostek w stosie (ang. cross-stack link aggregation)
 - e. Stos przetątników powinien być widoczny w sieci jako jedno urządzenie logiczne z punktu widzenia protokołu Spanning-Tree
 - f. Jeżeli realizacja funkcji łączenia w stosy wymaga dodatkowych interfejsów stackujących to w ramach niniejszego postępowania Zamawiający wymaga ich dostarczenia.
 - g. Zamawiający dopuszcza, aby możliwość łączenia w stosy była realizowana za pomocą portów typu uplink QSFP28. Każde urządzenie musi zostać dostarczone razem z oryginalnym kablem DAC QSFP+ 40G 1m
9. Układ przetątniający o wydajności min. 1.68 Tbps, wydajność przetątniania przynajmniej 485 Mpps
10. Obsługa min. 380 000 adresów MAC
11. Wbudowana pamięć RAM min. 4 GB
12. Procesor min. czterordzeniowy
13. Urządzenie musi mieć wbudowaną pamięć flash o pojemności min. 2 GB
14. Obsługa min. 4000 sieci VLAN jednocześnie oraz obsługa 802.1Q tunneling (QinQ)
15. Możliwość skonfigurowania min. 1024 interfejsów vlan interface SVI działających równocześnie
16. Obsługa ramek jumbo o wielkości min. 9216 bajtów
17. Obsługa protokołu GVRP
18. Wsparcie dla protokołów IEEE 802.1w Rapid Spanning Tree oraz IEEE 802.1s Multi-Instance Spanning Tree. Wymagane wsparcie dla min. 64 instancji protokołu MSTP
19. Obsługa min. 255 000 tras dla routingu IPv4
20. Obsługa min. 80 000 tras dla routingu IPv6
21. Obsługa protokołów routingu OSPF, OSPFv3, IS-IS, IS-ISv6, BGPv4, BGPv4+, RIP, RIPng, PIM-SM, PIM-DM i SSM. Jeżeli do obsługi powyższych funkcjonalności wymagana jest licencja to należy ją dostarczyć w ramach niniejszego postępowania
22. Obsługa min. 16 wirtualnych tablic routingu-forwardingu (VRF)
23. Obsługa protokołów LLDP i LLDP-MED

24. Obsługa MPLS wraz ze wsparciem dla L3VPN oraz VPLS. Jeżeli do obsługi powyższych funkcjonalności wymagana jest licencja to należy ją dostarczyć w ramach niniejszego postępowania
25. Przetątnik musi posiadać funkcjonalność DHCP Server
26. Obsługa ruchu multicast:
 - a. IGMP v1, v2 i v3
 - b. IGMP Snooping v1, v2 i v3
27. Mechanizmy związane z zapewnieniem bezpieczeństwa sieci:
 - a. min. 4 poziomy dostęp administracyjny poprzez konsolę
 - b. autoryzacja użytkowników w oparciu o IEEE 802.1x z możliwością przydzielenia VLANu oraz dynamicznego przypisania listy ACL
 - c. możliwość utworzenia minimum 6000 list ACL
 - d. możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC oraz poprzez portal www
 - e. zarządzanie urządzeniem przez HTTPS, SNMP i SSHv2 za pomocą protokołów IPv4 i IPv6 oprogramowania chmurowego producenta oraz przez system zarządzania producenta instalowany na serwerach wirtualizacji dostarczanego ze sprzętem w ramach projektu.
 - f. możliwość filtrowania ruchu w oparciu o adresy MAC, IPv4, IPv6, porty TCP/UDP
 - g. obsługa mechanizmów Port Security, Dynamic ARP Inspection, IP Source Guard, voice VLAN oraz private VLAN (lub równoważny),
 - h. możliwość synchronizacji czasu zgodnie z NTP
28. W ramach niniejszego postępowania Zamawiający wymaga dostarczenia dla każdego urządzenia pełnej i nieograniczonej licencji do systemu zarządzania producenta na okres 3 lat.
29. Obsługa funkcjonalności UDLD lub równoważnej
30. Implementacja co najmniej ośmiu kolejek sprzętowych QoS na każdym porcie wyjściowym z możliwością konfiguracji dla obsługi ruchu o różnych klasach:
 - a. klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy adres MAC, docelowy adres MAC, źródłowy adres IP, docelowy adres IP, źródłowy port TCP, docelowy port TCP
 - b. wsparcie dla mechanizmów QoS opartych o algorytm karuzelowy, np.: DRR, SP, DRR+SP
31. Urządzenie musi posiadać mechanizm do badania jakości połączeń (IP SLA) z możliwością badania takich parametrów jak: jitter, opóźnienie, straty pakietów dla wygenerowanego strumienia testowego UDP.
32. Urządzenie musi mieć możliwość pracy jako generator oraz jako odbiornik pakietów testowych IP SLA.
33. Wymagane opcje zarządzania:
 - a. możliwość lokalnej i zdalnej obserwacji ruchu na określonym porcie, polegająca na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do urządzenia monitorującego przyłączonego do innego portu oraz poprzez określony VLAN
 - b. plik konfiguracyjny urządzenia musi być możliwy do edycji w trybie off-line (tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC)
 - c. urządzenie musi posiadać wbudowany port USB, pozwalający na podłączenie zewnętrznej pamięci FLASH w celu przechowywania obrazów systemu operacyjnego, plików konfiguracyjnych lub certyfikatów elektronicznych
 - d. dedykowany port konsoli zgodny ze standardem RS-232
 - e. dedykowany port zarządzający out-of-band Ethernet 10/100Base-T
34. Wraz z urządzeniami muszą zostać dostarczone:
 - a. pełna dokumentacja w języku polskim lub angielskim
 - b. dokumenty potwierdzające, że proponowane urządzenia posiadają wymagane deklaracje zgodności z normami bezpieczeństwa (CE), lub oświadczenie, że deklaracja nie jest wymagana

35. Urządzenie musi być fabrycznie nowe i nieużywane wcześniej w żadnych projektach, wyprodukowane nie wcześniej niż 6 miesięcy przed dostawą i nieużywane przed dniem dostarczenia z wyłączeniem używania niezbędnego dla przeprowadzenia testu ich poprawnej pracy
36. Wsparcie dla funkcjonalności VXLAN. Jeżeli obsługa powyżej funkcjonalności wymaga dodatkowej licencji to w ramach niniejszego postępowania Zamawiający wymaga jej dostarczenia.
37. Urządzenie musi posiadać funkcjonalności WLAN:
 - a. Przetątnik musi umożliwiać obsługę funkcjonalności kontrolera WLAN celem zarządzania punktami dostępowymi WiFi tego samego producenta. Jeżeli przetątnik nie posiada takiej funkcjonalności należy dostarczyć parę urządzeń w klastrze pełniące rolę kontrolerów WLAN zgodnie z wymaganiami dotyczącymi WLAN.
 - b. Obsługę punktów dostępowych (access-point) pracujących w standardzie: 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac wave 1, 802.11ac wave 2, 802.11ax.
 - c. Mechanizmów uwierzytelniania: WPA/WPA2 with PSK, EAP-MD5, EAP-TLS, PEAP.
 - d. Możliwość zarządzania minimum 1000 access-pointów. Jeżeli powyższa funkcjonalność wymaga licencji to w ramach niniejszego postępowania Zamawiający nie wymaga dostarczenia licencji.
38. Urządzenia muszą pochodzić z autoryzowanego kanału dystrybucji producenta przeznaczonego na teren Unii Europejskiej, a korzystanie przez Zamawiającego z dostarczonego produktu nie może stanowić naruszenia majątkowych praw autorskich osób trzecich
39. Zamawiający wymaga, aby przetątniki posiadały 3-letni serwis gwarancyjny świadczony przez Wykonawcę (lub autoryzowany serwis) na bazie wsparcia serwisowego wykupionego u producenta oferowanych urządzeń. Wymiana uszkodzonego elementu w trybie 9x5xNBD. Okres gwarancji liczony będzie od daty sporządzenia protokołu zdawczo-odbiorczego przedmiotu zamówienia. Zamawiający na etapie dostawy będzie wymagał oświadczenia producenta potwierdzającego nabycie oraz zarejestrowanie serwisu gwarancyjnego na Zamawiającego. Wszystkie koszty związane z naprawami gwarancyjnymi nie mogą obciążać Zamawiającego (np. koszty wysyłki).
40. Bezpłatny dostęp do najnowszych wersji oprogramowania na stronie producenta przez cały okres gwarancyjny urządzeń.
41. Przetątnik musi dostarczony z licencją N1-CloudCampus,Foundation na min. 3 lata umożliwiającą podłączenie do systemu zarządzania iMaster NCE-Campus będącego w posiadaniu Zamawiającego.

12. Bezprzewodowy punkt dostępowy – 14 sztuk

Przedmiotem zamówienia jest 14 szt. bezprzewodowych punktów dostępowych z licencjami N1-CloudCampus,Foundation na min. 3 lata umożliwiającą podłączenie do systemu zarządzania iMaster NCE-Campus będącego w posiadaniu Zamawiającego.

Wymagania:

1. Urządzenie do pracy w sieci bezprzewodowej (punkt dostępowy klasy enterprise) do instalacji wewnątrz budynków.
2. Tryby pracy i zarządzanie: wsparcie Fit AP, Fat AP oraz Cloud-managed, z możliwością zdalnej obsługi przez Bluetooth. Dopuszcza się funkcję Leader AP dla małych wdrożeń bez kontrolera.
3. Separacja ruchu: wsparcie tunelowania do kontrolera oraz lokalnego przetączania (direct forwarding) w celu rozdzielenia ruchu lokalnego od ruchu kierowanego do kontrolera.
4. Standardy radiowe i SSID: zgodność z IEEE 802.11a/b/g/n/ac/ax/be (Wi-Fi 7), z jednoczesną obsługą min. 16 SSID na każde radio.

5. Urządzenie musi obsługiwać standard IEEE 802.11be (Wi-Fi 7), w tym technologie Multi-RU, Multi-Link Operation (MLO) oraz Enhanced Channel Utilization, zapewniające lepsze wykorzystanie pasma i niższe opóźnienia w środowiskach wysokiej gęstości.
6. Moc nadawcza i regulacja: możliwość regulacji mocy; maks. 23 dBm (2,4 GHz) oraz maks. 26 dBm (5 GHz) — zgodnie z przepisami kraju instalacji.
7. Wbudowane inteligentne anteny 2,4/5 GHz, pracujące dookoła lub w trybie wysokiej gęstości; wsparcie modulacji do 4096-QAM (Wi-Fi 7).
8. Urządzenie musi posiadać inteligentny system antenowy z automatycznym beamformingiem oraz funkcją Smart Antenna umożliwiającą dynamiczne kształtowanie wiązki i redukcję zakłóceń międzykanałowych.
9. Interfejsy kablowe i IoT:
 - a. min. 1× 100M/1G/2,5G RJ-45 (PoE IN) zgodny z 802.3at/af,
 - b. min. 1× 10/100/1000 RJ-45,
 - c. 1× USB 2.0 musi umożliwiać podłączenie modułów IoT (np. ZigBee, RFID, BLE) oraz integrację z systemem zarządzania IoT producenta.
10. Zestaw montażowy: dostarczyć akcesoria montażowe do instalacji wewnętrznej (sufit/ściana).
11. Anteny zysku co najmniej 4 dBi (2,4 GHz) i 5 dBi (5 GHz).
12. Praca jednoczesna w paśmie 2,4 GHz (2x2 MIMO) i 5 GHz (4x4 MIMO).
13. Modulacja do 4096-QAM.
14. Obsługa kanałów 20/40/80/160 MHz.
15. Bezpieczeństwo WLAN: WPA2-Personal/Enterprise, WPA3-Personal/Enterprise, 802.1X, PMF (802.11w), DHCP snooping, listy ACL, MACsec na porcie uplink, Secure Boot; dopuszcza się mechanizmy równoważne kontroli ARP/IP (np. ochrona przed spoofingiem) zgodnie z dokumentacją producenta.
16. Wymagana funkcja wbudowanego systemu WIDS/WIPS z automatycznym wykrywaniem i neutralizacją nieautoryzowanych punktów dostępowych (rogue AP).
17. Roaming: wsparcie 802.11k/v oraz 802.11r (fast roaming ≤ 50 ms).
18. Obsługa użytkowników: możliwość jednoczesnej obsługi min. 1000 klientów (specyfikacja urządzenia: do 1200, 600/radio).
19. Wydajność radiowa: łączna szybkość co najmniej 6,45 Gbit/s (do 689 Mbit/s w 2,4 GHz oraz do 5,76 Gbit/s w 5 GHz).
20. Środowisko pracy:
 - a. temperatura pracy od -10°C do +50°C,
 - b. wilgotność pracy 5%–95% (bez kondensacji).
21. Możliwość zasilania DC 12 V ±10% (zewnętrzny zasilacz).
22. Zgodność z IEEE 802.3at/af (PoE/PoE+) przy zasilaniu przez port 2,5G.
23. Wbudowane BLE 5.4.
24. Pobór mocy nie więcej niż 15 W.
25. Zarządzanie przez posiadany przez Zamawiającego kontroler Huawei AC 6508, platformę chmurową producenta, SSHv2/SFTP, telemetria, WebMaster, oraz O&M przez Bluetooth.
26. Urządzenie musi obsługiwać ZTP (Zero-Touch Provisioning) poprzez chmurę producenta lub kontroler lokalny, umożliwiając automatyczną konfigurację po podłączeniu do sieci.
27. Funkcje sieciowe: IPv6/IPv4, IPv6 SAVI, 802.1Q (VLAN), LLDP, Eth-Trunk, HotSpot 2.0, MESH, NAT (w trybie Fat/Cloud), DHCP client, tunelowanie i direct forwarding.
28. Punkt dostępowy musi umożliwiać pracę w trybie Mesh AP, z automatycznym doбором ścieżek i wsparciem szyfrowania 802.11i.
29. Synchronizacja czasu przez NTP.
30. Mechanizmy QoS/HQoS, airtime scheduling, VIP FastPass, identyfikacja aplikacji i priorytetyzacja, w tym możliwość preferowania pasma 5 GHz — band steering lub funkcje równoważne.

31. Wymagana funkcja analizy jakości połączeń użytkowników (Experience Intelligence), umożliwiająca pomiar opóźnień, strat, interferencji i wydajności pasm w czasie rzeczywistym oraz automatyczne optymalizacje radiowe.
32. Wsparcie dla mechanizmów AirTime Fairness, Dynamic Load Balancing oraz Smart Roaming z opóźnieniem przełączenia poniżej 50 ms.
33. MTBF min. 200 000 h
34. EMC odporność: zgodność z IEC 61000-4-2/3/4/5/6
35. Tryb oszczędzania energii: wsparcie Dynamic Power Saving
36. Certyfikaty i normy: bezpieczeństwo EN/IEC 62368-1, radio ETSI EN 300 328 / EN 301 893, EMC EN 301 489-1/-17, EN 55032/55035, IEC/EN 61000-4-x, zgodność z RoHS/REACH/WEEE.
37. Masa poniżej 1 kg.
38. Urządzenia fabrycznie nowe, nieużywane, data produkcji nie wcześniej niż 6 miesięcy przed dostawą.
39. Sprzęt z autoryzowanego kanału dystrybucji, oświadczenie producenta o ważności gwarancji w Polsce.
40. Bezpłatny dostęp do aktualizacji oprogramowania przez cały okres gwarancji.
41. 3-letni serwis gwarancyjny (8×5×NBD) realizowany przez Wykonawcę w oparciu o wsparcie producenta, okres gwarancji od protokołu odbioru.
42. Punkt dostępowy musi dostarczony z licencją N1-CloudCampus, Foundation na min. 3 lata umożliwiającą podłączenie do systemu zarządzania iMaster NCE-Campus będącego w posiadaniu Zamawiającego.

13. Rozszerzenie licencji UTM – 1 komplet

Przedmiotem zamówienia jest rozszerzenie licencji UTM Threat Protection Service zawierającą IPS, URL, AV oraz WAF o 3 lata do firewalla Huawei USG6615F (PN: 02353WAU).

14. Komputer stacjonarny TYP1 – 80 sztuk

Przedmiotem zamówienia jest komputer stacjonarny typu All in One.

Wymagania:

1. Komputer stacjonarny typu All in One.
2. Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji obliczeniowych, aplikacji graficznych, dostępu do internetu oraz poczty elektronicznej.
3. Procesor min. 14-rdzeniowy, osiągający w teście PassMark CPU Mark wynik min. 31000 punktów – wydruk ze strony należy dołączyć do oferty:
https://www.cpubenchmark.net/cpu_list.php potwierdzający spełnienie wymogów SWZ lub wynik równoważny w innym teście. W przypadku użycia przez oferenta równoważnych testów wydajności Zamawiający zastrzega sobie, iż w celu sprawdzenia poprawności przeprowadzenia testów oferent musi dostarczyć zamawiającemu oprogramowanie testujące, oba równoważne porównywalne zestawy oraz dokładny opis użytych testów wraz z wynikami w celu ich sprawdzenia w terminie nie dłuższym niż 7 dni od otrzymania zawiadomienia od zamawiającego.
4. Pamięć operacyjna min. 16 GB DDR5 z możliwością rozbudowy do min 64GB.
5. Pamięć masowa min. 512 GB M.2 PCIe NVMe z możliwością montażu drugiego dysku M.2 PCIe NVMe.
6. Karta graficzna zintegrowana z procesorem, ze wsparciem dla DirectX 12, OpenGL 4.5 oraz dla rozdzielczości 4096x2160@60Hz osiągająca w teście Average G3D Mark wynik minimum 1800 punktów. Do oferty należy dołączyć wydruk ze strony: <http://www.videocardbenchmark.net> potwierdzający spełnienie wymogów SIWZ

7. Obudowa typu All in One – zintegrowany komputer w obudowie wraz z monitorem z matrycą IPS min 23,8” o parametrach:
 - a. rozdzielczość min 1920 x 1080 @ 60 Hz
 - b. kąty widzenia pion/poziom: min 178/178 stopni
 - c. komputer wyposażony w stand/nogę umożliwiającą:
 - i. kąty pochylecia w pionie min -5/+20 stopni
 - ii. regulacja wysokości do 130 mm
 - iii. swivel/obróć w poziomie +/- 45 stopni
 - d. Komputer musi posiadać system diagnostyczny (sprzętowy lub programowy na poziomie BIOS) informujący o awariach kluczowych komponentów (CPU, RAM, Grafika) Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej (złącze blokady Kensingtona)
 - e. Zasilacz o mocy min. 200W, dedykowany przez producenta komputera. Dopuszcza się zasilacz zewnętrzny lub wewnętrzny
8. Wyposażenie multimedialne: karta dźwiękowa zintegrowana z płytą główną; wbudowane dwa głośniki stereo.
9. Możliwość odczytania z BIOS:
 - a. Wersji BIOS wraz z datą wydania wersji
 - b. Modelu procesora, prędkości procesora, liczby rdzeni, wielkość pamięci cache L1/L2/L3
 - c. Informacji o ilości pamięci RAM wraz z informacją o jej prędkości, pojemności i obsadzeniu na poszczególnych slotach
 - d. Informacji o dysku twardym: model, pojemność,
 - e. Informacji o napędzie optycznym: model,
 - f. Informacji o MAC adresie karty sieciowej
 - g. Informacji o kontrolerze Audio
 - h. Informacji o producencie komputera w tym logo, modelu i wielkości matrycy
10. Możliwość wyłączenia/włączenia zintegrowanej karty sieciowej LAN i osobno karty WiFi, kontrolera audio, kamery, wbudowanych głośników, mikrofonu, portów USB (bok, tył), funkcjonalności ładowania zewnętrznych urządzeń przez port USB i osobno dla portu USB-C, poszczególnych slotów m.2, funkcji TurboBoost, kontrolera RAID, wirtualizacji z poziomu BIOS bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych.
11. Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z dysku twardego, zewnętrznych urządzeń oraz sieci bez potrzeby uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych.
12. Możliwość ustawienia hasła na poziomie administratora, bez potrzeby uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych.
13. BIOS musi posiadać funkcję update BIOS z opcją automatycznego update BIOS przez sieć włączaną na poziomie BIOS przez użytkownika bez potrzeby uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych.
14. Diagnostyka uruchamiana z BIOS działająca bez obecności systemu operacyjnego czy dysku twardego umożliwiającą na przeprowadzenie testów diagnostycznych w tym m.in.:
 - a. test procesora
 - b. test dysku twardego w tym SSD
 - c. test pamięci RAM
 - d. test płyty głównej
 - e. klawiatury
15. BIOS musi posiadać możliwość:

- a. skonfigurowania hasła „Power On” oraz ustawienia hasła dostępu do BIOSu (administratora) w sposób gwarantujący utrzymanie zapisanego hasła nawet w przypadku odłączenia wszystkich źródeł zasilania i podtrzymania BIOS,
 - b. możliwość ustawienia hasła na dysku (drive lock)
 - c. blokady/wyłączenia portów USB, karty sieciowej, karty audio;
 - d. kontroli sekwencji boot-ącej;
 - e. startu systemu z urządzenia USB
 - f. funkcja blokowania BOOT-owania stacji roboczej z zewnętrжных urządzeń
16. Komputer musi posiadać zintegrowany w płycie głównej aktywny układ zgodny ze standardem Trusted Platform Module (TPM v 2.0)
17. Możliwość zapięcia linki typu Kensington do dedykowanego złącza w obudowie komputera
18. Czujnik otwarcia obudowy zintegrowany trwale z płytą główną i zarządzany z poziomu BIOS w zakresie min włączyć/wyłączyć.
19. Zaimplementowany w BIOS system diagnostyczny z graficznym interfejsem użytkownika w języku polskim lub angielskim, umożliwiający przetestowanie w celu wykrycia usterki zainstalowanych komponentów w oferowanym komputerze bez konieczności uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych. Minimalne funkcjonalności systemu diagnostycznego:
- a. informacje o systemie, min.: Procesor: typ procesora, jego obecną prędkość. Pamięć RAM: rozmiar pamięci RAM, osadzenie na poszczególnych slotach, szybkość pamięci, nr seryjny, typ pamięci, nr części, nazwa producenta. Dysk twardy: model, typ, wersja firmware, nr seryjny, procentowe zużycie dysku, temperaturę pracy dysku. Wentylator: aktualną prędkość i obciążenie. Data wydania i wersja BIOS. Nr seryjny komputera
 - b. możliwość przeprowadzenia szybkiego oraz szczegółowego testu kontrolującego komponenty komputera
 - c. możliwość przeprowadzenia testów poszczególnych komponentów a w szczególności: procesora, pamięci RAM, dysku twardego, karty dźwiękowej, klawiatury, myszy, sieci, napędu optycznego, płyty głównej, portów USB, karty graficznej
 - d. rejestr przeprowadzonych testów zawierający min.: datę testu, wynik, identyfikator awarii
 - e. Komputer musi być wyposażony w mechanizm ochrony i samonaprawy BIOS w przypadku jego uszkodzenia lub nieautoryzowanej modyfikacji, działający na poziomie sprzętowym (niezależnie od systemu operacyjnego).
 - f. Komputer musi być wyposażony w BIOS posiadający mechanizm samokontroli i samoczynnej autonaprawy, działający automatycznie przy każdym uruchomieniu komputera, który sprawdza integralność i autentyczność uruchamianego podsystemu BIOS oraz musi chronić Master Boot Record (MBR) oraz GUID Partition Table (GPT) przed uszkodzeniem lub usunięciem..
20. Certyfikaty i standardy:
- a. Certyfikat ISO 9001 dla producenta sprzętu (załączyć dokument potwierdzający spełnianie wymogu)
 - b. Deklaracja zgodności CE (załączyć do oferty)
 - c. Dokument potwierdzający posiadanie certyfikatu lub oświadczenie producenta, że oferowany model komputera jest zgodny z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych,
 - d. Dokument potwierdzający posiadanie certyfikatu lub oświadczenie producenta, że oferowany model komputera poprawnie współpracuje z oferowanym systemem operacyjnym,
 - e. Komputer musi spełniać wymogi normy Energy Star
 - f. Wymagany certyfikat lub wpis dotyczący oferowanego modelu komputera w internetowym katalogu <http://www.energystar.gov> – dopuszcza się wydruk ze strony internetowej

- g. Komputer musi spełniać wymogi normy EPEAT na poziomie min GOLD dla Polski
 - h. Wymagany certyfikat lub wpis dotyczący oferowanego modelu komputera w internetowym katalogu <http://www.epeat.net> – wymaga się wydruku ze strony internetowej
21. Maksymalnie 20 dB z pozycji operatora w trybie IDLE, pomiar zgodny z normą ISO 9296 / ISO 7779; wymaga się dostarczenia odpowiedniego certyfikatu lub deklaracji producenta.
22. System operacyjny fabrycznie przeinstalowany przez producenta - klasy desktop musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:
- a. Dostępne dwa rodzaje graficznego interfejsu użytkownika:
 - i. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
 - ii. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych,
 - b. Interfejsy użytkownika dostępne w wielu językach do wyboru – w tym Polskim i Angielskim,
 - c. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, pomoc, komunikaty systemowe,
 - d. Wbudowany system pomocy w języku polskim;
 - e. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim,
 - f. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modulem „uczenia się” pisma użytkownika – obsługa języka polskiego.
 - g. Funkcjonalność rozpoznawania mowy, pozwalającą na sterowanie komputerem głosowo, wraz z modulem „uczenia się” głosu użytkownika.
 - h. Możliwość dokonywania bezpłatnych aktualizacji i poprawek w ramach wersji systemu operacyjnego poprzez Internet, mechanizmem udostępnianym przez producenta systemu z możliwością wyboru instalowanych poprawek oraz mechanizmem sprawdzającym, które z poprawek są potrzebne,
 - i. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego,
 - j. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego,
 - k. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6,
 - l. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami,
 - m. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi),
 - n. Funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer,
 - o. Możliwość zarządzania stacją roboczą poprzez polityki grupowe – przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji,
 - p. Rozbudowane, definiowalne polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji,
 - q. Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu, zgodnie z określonymi uprawnieniami poprzez polityki grupowe,
 - r. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników.
 - s. Mechanizm pozwalający użytkownikowi zarejestrowanego w systemie przedsiębiorstwa/instytucji urządzenia na uprawniony dostęp do zasobów tego systemu.

- t. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych,
- u. Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi.
- v. Obsługa standardu NFC (near field communication),
- w. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących);
- x. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny;
- y. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509;
- z. Mechanizmy logowania do domeny w oparciu o:
 - i. Login i hasło,
 - ii. Karty z certyfikatami (smartcard),
 - iii. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),
- aa. Mechanizmy wieloelementowego uwierzytelniania.
- bb. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5,
- cc. Wsparcie do uwierzytelnienia urządzenia na bazie certyfikatu,
- dd. Wsparcie dla algorytmów Suite B (RFC 4869),
- ee. Wsparcie wbudowanej zapory ogniowej dla Internet Key Exchange v. 2 (IKEv2) dla warstwy transportowej IPsec,
- ff. Wbudowane narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk;
- gg. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach,
- hh. Wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń,
- ii. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem,
- jj. Rozwiązanie służące do automatycznego zbudowania obrazu systemu wraz z aplikacjami. Obraz systemu służyć ma do automatycznego upowszechnienia systemu operacyjnego inicjowanego i wykonywanego w całości poprzez sieć komputerową,
- kk. Rozwiązanie ma umożliwiać wdrożenie nowego obrazu poprzez zdalną instalację,
- ll. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe,
- mm. Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe
- nn. Udostępnianie modemu,
- oo. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej,
- pp. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci,
- qq. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.),
- rr. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu),
- ss. Wbudowany mechanizm wirtualizacji typu hypervisor, umożliwiający, zgodnie z uprawnieniami licencyjnymi, uruchomienie do 4 maszyn wirtualnych,

- tt. Mechanizm szyfrowania dysków wewnętrznych i zewnętrznych z możliwością szyfrowania ograniczonego do danych użytkownika,
 - uu. Wbudowane w system narzędzie do szyfrowania partycji systemowych komputera, z możliwością przechowywania certyfikatów w mikrochipie TPM (Trusted Platform Module) w wersji minimum 1.2 lub na kluczach pamięci przenośnej USB,
 - vv. Wbudowane w system narzędzie do szyfrowania dysków przenośnych, z możliwością centralnego zarządzania poprzez polityki grupowe, pozwalające na wymuszenie szyfrowania dysków przenośnych,
 - ww. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania partycji w usługach katalogowych,
 - xx. Możliwość instalowania dodatkowych języków interfejsu systemu operacyjnego oraz możliwość zmiany języka bez konieczności reinstalacji systemu,
23. Wbudowane porty i złącza:
- a. porty video: 1szt. HDMI OUT oraz 1 szt. HDMI-IN
 - b. min. 6 x USB min. 3.2 w tym min: 1 szt USB Typ-C o przepustowości do 10 Gbps oraz 1 szt USB Typ-A o przepustowości do 10 Gbps
 - c. port sieciowy RJ-45
 - d. port audio COMBO
 - e. chowana w obrysie komputera kamera internetowa min 2 MP z min. dwoma mikrofonami
24. Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) portów i złączy nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek, adapterów itp.
25. Karta sieciowa 10/100/1000 Ethernet RJ 45 (zintegrowana) z obsługą PXE, WoL,
26. Karta WiFi 6 Wireless 2x2 z Bluetooth min. 5.3 M.2 Combo
27. Płyta główna wyposażona w:
- a. min. 2 złącza SODIMM z obsługą do 64GB pamięci RAM
 - b. min. 1 złącze M.2 PCIe x1 dla WLAN
 - c. min. 2 złącza M.2 PCIe dla dysków SSD w tym min. 1 szt PCIe x4
28. Klawiatura USB w układzie QWERTY, z wyspą numeryczną;
29. Mysz optyczna USB z min dwoma klawiszami oraz rolką (scroll).
30. Wbudowana w płytę główną technologia zarządzania i monitorowania komputera na poziomie sprzętowym działająca niezależnie od stanu czy obecności systemu operacyjnego oraz stanu włączenia komputera podczas pracy na zasilaczu sieciowym AC, obsługująca zdalną komunikację siecią w oparciu o protokół IPv4:
- a. zdalne przejęcie konsoli tekstowej systemu, przekierowanie procesu ładowania systemu operacyjnego,
 - b. zdalne przejęcie pełnej konsoli graficznej systemu tzw. KVM Redirection (Keyboard, Video, Mouse) bez udziału systemu operacyjnego ani dodatkowych programów, również w przypadku braku lub uszkodzenia systemu operacyjnego,
 - c. możliwość konfiguracji parametrów funkcji zarządzania (m.in. parametrów kont uprawnionych do zarządzania sprzętowego).
31. Wsparcie techniczne producenta:
- a. Ogólnopolska, telefoniczna infolinia/linia techniczna producenta komputera (ogólnopolski numer – w ofercie należy podać numer telefonu) dostępna w czasie obowiązywania gwarancji na sprzęt i umożliwiająca po podaniu numeru seryjnego urządzenia:
 - i. weryfikację konfiguracji fabrycznej wraz z wersją fabrycznie dostarczonego oprogramowania (system operacyjny, szczegółowa konfiguracja sprzętowa - CPU, HDD, pamięć)
 - ii. sprawdzenie czasu obowiązywania i typ udzielonej gwarancji
 - b. Możliwość aktualizacji i pobrania sterowników do oferowanego modelu komputera w najnowszych certyfikowanych wersjach przy użyciu dedykowanego darmowego

oprogramowania producenta lub bezpośrednio z sieci Internet za pośrednictwem strony www.producenta.komputera po podaniu numeru seryjnego komputera lub modelu komputera

- c. Możliwość weryfikacji czasu obowiązywania i reżimu gwarancji bezpośrednio z sieci Internet za pośrednictwem strony www.producenta.komputera.

32. 3-letnia gwarancja producenta, serwis musi być realizowany w miejscu użytkowania sprzętu. Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych oraz posiadać autoryzację producenta komputera

15. Komputer stacjonarny TYP 2 – 40 sztuk

Przedmiotem zamówienia jest komputer stacjonarny typu All in One z DVD.

Wymagania:

1. Komputer stacjonarny typu All in One.
2. Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji obliczeniowych, aplikacji graficznych, dostępu do internetu oraz poczty elektronicznej.
3. Procesor min. 14-rdzeniowy, osiągający w teście PassMark CPU Mark wynik min. 31000 punktów – wydruk ze strony należy dołączyć do oferty:
https://www.cpubenchmark.net/cpu_list.php potwierdzający spełnienie wymogów SWZ lub wynik równoważny w innym teście. W przypadku użycia przez oferenta równoważnych testów wydajności Zamawiający zastrzega sobie, iż w celu sprawdzenia poprawności przeprowadzenia testów oferent musi dostarczyć zamawiającemu oprogramowanie testujące, oba równoważne porównywalne zestawy oraz dokładny opis użytych testów wraz z wynikami w celu ich sprawdzenia w terminie nie dłuższym niż 7 dni od otrzymania zawiadomienia od zamawiającego.
4. Pamięć operacyjna min. 16 GB DDR5 z możliwością rozbudowy do min. 64GB.
5. Pamięć masowa min. 512 GB M.2 PCIe NVMe z możliwością montażu drugiego dysku M.2 PCIe NVMe.
6. Karta graficzna zintegrowana z procesorem, ze wsparciem dla DirectX 12, OpenGL 4.5 oraz dla rozdzielczości 4096x2160@60Hz osiągająca w teście Average G3D Mark wynik minimum 1800 punktów. Do oferty należy dołączyć wydruk ze strony: <http://www.videocardbenchmark.net> potwierdzający spełnienie wymogów SIWZ
7. Obudowa typu All in One – zintegrowany komputer w obudowie wraz z monitorem z matrycą IPS min 23,8” o parametrach:
 - a. rozdzielczość min 1920 x 1080 @ 60 Hz
 - b. kąty widzenia pion/poziom: min 178/178 stopni
 - c. komputer wyposażony w stand/nogę umożliwiającą:
 - i. kąty pochylecia w pionie min -5/+20 stopni
 - ii. regulacja wysokości do 130 mm
 - iii. swivel/obróć w poziomie +/- 45 stopni
 - d. Komputer musi posiadać wbudowany napęd DVD/RW lub zamawiający dopuszcza dostarczenie zewnętrznego napędu DVD/RW na złącze USB, pochodzącego od producenta komputera..
 - e. Komputer musi posiadać system diagnostyczny (sprzętowy lub programowy na poziomie BIOS) informujący o awariach kluczowych komponentów (CPU, RAM, Grafika)Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej (złącze blokady Kensingtona)
 - f. Zasilacz o mocy min. 200W, dedykowany przez producenta komputera. Dopuszcza się zasilacz zewnętrzny lub wewnętrzny.
8. Wyposażenie multimedialne: karta dźwiękowa zintegrowana z płytą główną; wbudowane dwa głośniki stereo.

9. Możliwość odczytania z BIOS:
 - a. Wersji BIOS wraz z datą wydania wersji
 - b. Modelu procesora, prędkości procesora, liczby rdzeni, wielkość pamięci cache L1/L2/L3
 - c. Informacji o ilości pamięci RAM wraz z informacją o jej prędkości, pojemności i obsadzeniu na poszczególnych slotach
 - d. Informacji o dysku twardym: model, pojemność,
 - e. Informacji o napędzie optycznym: model,
 - f. Informacji o MAC adresie karty sieciowej
 - g. Informacji o kontrolerze Audio
 - h. Informacji o producencie komputera w tym logo, modelu i wielkości matrycy
10. Możliwość wyłączenia/włączenia zintegrowanej karty sieciowej LAN i osobno karty WiFi, kontrolera audio, kamery, wbudowanych głośników, mikrofonu, portów USB (bok, tył), funkcjonalności ładowania zewnętrznych urządzeń przez port USB i osobno dla portu USB-C, poszczególnych slotów m.2, funkcji TurboBoost, kontrolera RAID, wirtualizacji z poziomu BIOS bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych.
11. Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z dysku twardego, zewnętrznych urządzeń oraz sieci bez potrzeby uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych.
12. Możliwość ustawienia hasła na poziomie administratora, bez potrzeby uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych.
13. BIOS musi posiadać funkcję update BIOS z opcją automatycznego update BIOS przez sieć włączaną na poziomie BIOS przez użytkownika bez potrzeby uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych.
14. Diagnostyka uruchamiana z BIOS działająca bez obecności systemu operacyjnego czy dysku twardego umożliwiającą na przeprowadzenie testów diagnostycznych w tym m.in.:
 - a. test procesora
 - b. test dysku twardego w tym SSD
 - c. test pamięci RAM
 - d. test płyty głównej
 - e. klawiatury
15. BIOS musi posiadać możliwość
 - a. skonfigurowania hasła „Power On” oraz ustawienia hasła dostępu do BIOSu (administratora) w sposób gwarantujący utrzymanie zapisanego hasła nawet w przypadku odłączenia wszystkich źródeł zasilania i podtrzymania BIOS,
 - b. możliwość ustawienia hasła na dysku (drive lock)
 - c. blokady/wyłączenia portów USB, karty sieciowej, karty audio;
 - d. kontroli sekwencji boot-ącej;
 - e. startu systemu z urządzenia USB
 - f. funkcja blokowania BOOT-owania stacji roboczej z zewnętrznymi urządzeniami
16. Komputer musi posiadać zintegrowany w płycie głównej aktywny układ zgodny ze standardem Trusted Platform Module (TPM v 2.0);
17. Możliwość zapięcia linki typu Kensington do dedykowanego złącza w obudowie komputera
18. Czujnik otwarcia obudowy zintegrowany trwale z płytą główną i zarządzany z poziomu BIOS w zakresie min włączyć/wyłączyć.
19. Zaimplementowany w BIOS system diagnostyczny z graficznym interfejsem użytkownika w języku polskim lub angielskim, umożliwiający przetestowanie w celu wykrycia usterki zainstalowanych komponentów w oferowanym komputerze bez konieczności uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych. Minimalne funkcjonalności systemu diagnostycznego:

- a. informacje o systemie, min.: Procesor: typ procesora, jego obecną prędkość. Pamięć RAM: rozmiar pamięci RAM, osadzenie na poszczególnych slotach, szybkość pamięci, nr seryjny, typ pamięci, nr części, nazwa producenta. Dysk twardy: model, typ, wersja firmware, nr seryjny, procentowe zużycie dysku, temperaturę pracy dysku. Wentylator: aktualną prędkość i obciążenie. Data wydania i wersja BIOS. Nr seryjny komputera
 - b. możliwość przeprowadzenia szybkiego oraz szczegółowego testu kontrolującego komponenty komputera
 - c. możliwość przeprowadzenia testów poszczególnych komponentów a w szczególności: procesora, pamięci RAM, dysku twardego, karty dźwiękowej, klawiatury, myszy, sieci, napędu optycznego, płyty głównej, portów USB, karty graficznej
 - d. rejestr przeprowadzonych testów zawierający min.: datę testu, wynik, identyfikator awarii
20. Komputer musi być wyposażony w mechanizm ochrony i samonaprawy BIOS w przypadku jego uszkodzenia lub nieautoryzowanej modyfikacji, działający na poziomie sprzętowym (niezależnie od systemu operacyjnego) Komputer musi być wyposażony w BIOS posiadający mechanizm samokontroli i samoczynnej autonaprawy, działający automatycznie przy każdym uruchomieniu komputera, który sprawdza integralność i autentyczność uruchamianego podsystemu BIOS oraz musi chronić Master Boot Record (MBR) oraz GUID Partition Table (GPT) przed uszkodzeniem lub usunięciem.
21. Certyfikaty i standardy:
- a. Certyfikat ISO 9001 dla producenta sprzętu (załączyć dokument potwierdzający spełnianie wymogu)
 - b. Deklaracja zgodności CE (załączyć do oferty)
 - c. Dokument potwierdzający posiadanie certyfikatu lub oświadczenie producenta, że oferowany model komputera jest zgodny z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych,
 - d. Dokument potwierdzający posiadanie certyfikatu lub oświadczenie producenta, że oferowany model komputera poprawnie współpracuje z oferowanym systemem operacyjnym,
 - e. Komputer musi spełniać wymogi normy Energy Star
 - f. Wymagany certyfikat lub wpis dotyczący oferowanego modelu komputera w internetowym katalogu <http://www.energystar.gov> – dopuszcza się wydruk ze strony internetowej
 - g. Komputer musi spełniać wymogi normy EPEAT na poziomie min GOLD dla Polski
 - h. Wymagany certyfikat lub wpis dotyczący oferowanego modelu komputera w internetowym katalogu <http://www.epeat.net> – wymaga się wydruku ze strony internetowej
22. Maksymalnie 20 dB z pozycji operatora w trybie IDLE, pomiar zgodny z normą ISO 9296 / ISO 7779; wymaga się dostarczenia odpowiedniego certyfikatu lub deklaracji producenta.
23. System operacyjny fabrycznie przeinstalowany przez producenta - klasy desktop musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:
- a. Dostępne dwa rodzaje graficznego interfejsu użytkownika:
 - i. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
 - ii. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych,
 - b. Interfejsy użytkownika dostępne w wielu językach do wyboru – w tym Polskim i Angielskim,
 - c. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimedialny, pomoc, komunikaty systemowe,
 - d. Wbudowany system pomocy w języku polskim,
 - e. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim,

- f. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się” pisma użytkownika – obsługa języka polskiego,
- g. Funkcjonalność rozpoznawania mowy, pozwalającą na sterowanie komputerem głosowo, wraz z modułem „uczenia się” głosu użytkownika,
- h. Możliwość dokonywania bezpłatnych aktualizacji i poprawek w ramach wersji systemu operacyjnego poprzez Internet, mechanizmem udostępnianym przez producenta systemu z możliwością wyboru instalowanych poprawek oraz mechanizmem sprawdzającym, które z poprawek są potrzebne,
- i. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego,
- j. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego,
- k. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6,
- l. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami,
- m. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi),
- n. Funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer,
- o. Możliwość zarządzania stacją roboczą poprzez polityki grupowe – przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji,
- p. Rozbudowane, definiowalne polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji,
- q. Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu, zgodnie z określonymi uprawnieniami poprzez polityki grupowe,
- r. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników,
- s. Mechanizm pozwalający użytkownikowi zarejestrowanego w systemie przedsiębiorstwa/instytucji urządzenia na uprawniony dostęp do zasobów tego systemu,
- t. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych,
- u. Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi,
- v. Obsługa standardu NFC (near field communication),
- w. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących),
- x. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny,
- y. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509,
- z. Mechanizmy logowania do domeny w oparciu o:
 - i. Login i hasło,
 - ii. Karty z certyfikatami (smartcard),
 - iii. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),
- aa. Mechanizmy wieloelementowego uwierzytelniania,

- bb. Wsparcie dla uwierzytelniania na bazie Kerberos v.5,
- cc. Wsparcie do uwierzytelnienia urządzenia na bazie certyfikatu,
- dd. Wsparcie dla algorytmów Suite B (RFC 4869),
- ee. Wsparcie wbudowanej zapory ogniowej dla Internet Key Exchange v. 2 (IKEv2) dla warstwy transportowej IPsec,
- ff. Wbudowane narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk,
- gg. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach,
- hh. Wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń,
- ii. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem,
- jj. Rozwiązanie służące do automatycznego zbudowania obrazu systemu wraz z aplikacjami. Obraz systemu służyć ma do automatycznego upowszechnienia systemu operacyjnego inicjowanego i wykonywanego w całości poprzez sieć komputerową,
- kk. Rozwiązanie ma umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację,
- ll. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe,
- mm. Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe,
- nn. Udostępnianie modemu,
- oo. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej,
- pp. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci,
- qq. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.),
- rr. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu),
- ss. Wbudowany mechanizm wirtualizacji typu hypervisor, umożliwiający, zgodnie z uprawnieniami licencyjnymi, uruchomienie do 4 maszyn wirtualnych,
- tt. Mechanizm szyfrowania dysków wewnętrznych i zewnętrznych z możliwością szyfrowania ograniczonego do danych użytkownika,
- uu. Wbudowane w system narzędzie do szyfrowania partycji systemowych komputera, z możliwością przechowywania certyfikatów w mikrochipie TPM (Trusted Platform Module) w wersji minimum 1.2 lub na kluczach pamięci przenośnej USB,
- vv. Wbudowane w system narzędzie do szyfrowania dysków przenośnych, z możliwością centralnego zarządzania poprzez polityki grupowe, pozwalające na wymuszenie szyfrowania dysków przenośnych,
- ww. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania partycji w usługach katalogowych,
- xx. Możliwość instalowania dodatkowych języków interfejsu systemu operacyjnego oraz możliwość zmiany języka bez konieczności reinstalacji systemu,

24. Wbudowane porty i złącza:

- a. porty video: 1szt. HDMI OUT oraz 1 szt. HDMI-IN
- b. min. 6 x USB min. 3.2 w tym min: 1 szt USB Typ-C o przepustowości do 10 Gbps oraz 1 szt USB Typ-A o przepustowości do 10 Gbps
- c. port sieciowy RJ-45
- d. port audio COMBO

- e. chowana w obrysie komputera kamera internetowa min 2 MPz min. dwoma mikrofonami
- 25. Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) portów i złączy nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek, adapterów itp.
- 26. Karta sieciowa 10/100/1000 Ethernet RJ 45 (zintegrowana) z obsługą PXE, WoL,
- 27. Karta WiFi 6 Wireless 2x2 z Bluetooth min. 5.3 M.2 Combo
- 28. Płyta główna wyposażona w:
 - a. min. 2 złącza SODIMM z obsługą do 64GB pamięci RAM
 - b. min. 1 złącze M.2 PCIe x1 dla WLAN
 - c. min. 2 złącza M.2 PCIe dla dysków SSD w tym min. 1 szt PCIe x4
- 29. Klawiatura USB w układzie QWERTY, z wyspą numeryczną,
- 30. Mysz optyczna USB z min dwoma klawiszami oraz rolką (scroll),
- 31. Wbudowana w płytę główną technologia zarządzania i monitorowania komputera na poziomie sprzętowym działająca niezależnie od stanu czy obecności systemu operacyjnego oraz stanu włączenia komputera podczas pracy na zasilaczu sieciowym AC, obsługująca zdalną komunikację sieciową w oparciu o protokół IPv4:
 - a. zdalne przejęcie konsoli tekstowej systemu, przekierowanie procesu ładowania systemu operacyjnego,
 - b. zdalne przejęcie pełnej konsoli graficznej systemu tzw. KVM Redirection (Keyboard, Video, Mouse) bez udziału systemu operacyjnego ani dodatkowych programów, również w przypadku braku lub uszkodzenia systemu operacyjnego,
 - c. możliwość konfiguracji parametrów funkcji zarządzania (m.in. parametrów kont uprawnień do zarządzania sprzętowego).
- 32. Ogólnopolska telefoniczna infolinia/linia techniczna producenta komputera (ogólnopolski numer – w ofercie należy podać numer telefonu) dostępna w czasie obowiązywania gwarancji na sprzęt i umożliwiająca po podaniu numeru seryjnego urządzenia:
 - a. weryfikację konfiguracji fabrycznej wraz z wersją fabrycznie dostarczonego oprogramowania (system operacyjny, szczegółowa konfiguracja sprzętowa - CPU, HDD, pamięć)
 - b. sprawdzenie czasu obowiązywania i typ udzielonej gwarancji
- 33. Możliwość aktualizacji i pobrania sterowników do oferowanego modelu komputera w najnowszych certyfikowanych wersjach przy użyciu dedykowanego darmowego oprogramowania producenta lub bezpośrednio z sieci Internet za pośrednictwem strony www producenta komputera po podaniu numeru seryjnego komputera lub modelu komputera
- 34. Możliwość weryfikacji czasu obowiązywania i reżimu gwarancji bezpośrednio z sieci Internet za pośrednictwem strony www producenta komputera.
- 35. 3-letnia gwarancja producenta, serwis musi być realizowany w miejscu użytkowania sprzętu. Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych oraz posiadać autoryzację producenta komputera

16. Laptop – 4 sztuki

Przedmiotem zamówienia jest komputer przenośny typu notebook.

Wymagania:

- 1. Komputer przenośny typu notebook z ekranem 16".
- 2. Ekran 16" o rozdzielczości min. WUXGA (1920x1200) w technologii LED IPS przeciwoodblaskowy, jasność min. 300 nitów, kontrast min 1000:1,
- 3. Procesor: Klasy x86, zaprojektowany dla komputerów przenośnych, posiadający minimum 12 rdzeni fizycznych. Procesor musi uzyskiwać wynik minimum 17 800 punktów w teście Passmark CPU Mark (według danych na stronie cpubenchmark.net). Zamawiający dopuszcza procesory o architekturze hybrydowej (Performance/Efficient cores).

4. Pamięć operacyjna min. 32GB DDR5, możliwość rozbudowy do min. 64GB.
5. Pamięć masowa min. 1TB SSD PCIe M.2 NVMe.
6. Karta graficzna zintegrowana w procesorze ze sprzętowym wsparciem dla DirectX 12, OpenGL 4.6, OpenCL 2.2.
7. Karta dźwiękowa stereo, wbudowane m.in. dwa głośniki stereo. Wbudowana w obudowę matrycy kamera min. 2MP lub wyższej wraz z min. dwoma mikrofonami z funkcją redukcji szumów otoczenia. Mechaniczna przestona kamery zintegrowana w ramce matrycy.
8. Bateria min. 3-cell, 60 WHr. Zasilacz min. 60W.
9. System operacyjny fabrycznie przeinstalowany przez producenta - klasy desktop musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:
 - a. Dostępne dwa rodzaje graficznego interfejsu użytkownika:
 - i. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
 - ii. Dotykowy umożliwiający sterowanie dotykem na urządzeniach typu tablet lub monitorach dotykowych,
 - b. Interfejsy użytkownika dostępne w wielu językach do wyboru – w tym Polskim i Angielskim,
 - c. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, pomoc, komunikaty systemowe,
 - d. Wbudowany system pomocy w języku polskim,
 - e. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim,
 - f. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się” pisma użytkownika – obsługa języka polskiego,
 - g. Funkcjonalność rozpoznawania mowy, pozwalającą na sterowanie komputerem głosowo, wraz z modułem „uczenia się” głosu użytkownika,
 - h. Możliwość dokonywania bezpłatnych aktualizacji i poprawek w ramach wersji systemu operacyjnego poprzez Internet, mechanizmem udostępnianym przez producenta systemu z możliwością wyboru instalowanych poprawek oraz mechanizmem sprawdzającym, które z poprawek są potrzebne,
 - i. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego,
 - j. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego,
 - k. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6,
 - l. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami,
 - m. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi),
 - n. Funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer,
 - o. Możliwość zarządzania stacją roboczą poprzez polityki grupowe – przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji,
 - p. Rozbudowane, definiowalne polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji,
 - q. Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu, zgodnie z określonymi uprawnieniami poprzez polityki grupowe,
 - r. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników,

- s. Mechanizm pozwalający użytkownikowi zarejestrowanego w systemie przedsiębiorstwa/instytucji urządzenia na uprawniony dostęp do zasobów tego systemu,
- t. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych,
- u. Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi,
- v. Możliwość obsługi standardu NFC (near field communication),
- w. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących),
- x. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny,
- y. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509,
- z. Mechanizmy logowania do domeny w oparciu o:
 - i. Login i hasło,
 - ii. Karty z certyfikatami (smartcard),
 - iii. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),
- aa. Mechanizmy wieloelementowego uwierzytelniania,
- bb. Wsparcie dla uwierzytelniania na bazie Kerberos v.5,
- cc. Wsparcie do uwierzytelnienia urządzenia na bazie certyfikatu,
- dd. Wsparcie dla algorytmów Suite B (RFC 4869),
- ee. Wsparcie wbudowanej zapory ogniowej dla Internet Key Exchange v. 2 (IKEv2) dla warstwy transportowej IPsec,
- ff. Wbudowane narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk,
- gg. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach,
- hh. Wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń,
- ii. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem,
- jj. Rozwiązanie służące do automatycznego zbudowania obrazu systemu wraz z aplikacjami. Obraz systemu służyć ma do automatycznego upowszechnienia systemu operacyjnego inicjowanego i wykonywanego w całości poprzez sieć komputerową,
- kk. Rozwiązanie ma umożliwiać wdrożenie nowego obrazu poprzez zdalną instalację,
- ll. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe,
- mm. Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe,
- nn. Udostępnianie modemu,
- oo. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej,
- pp. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci,
- qq. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.),

- rr. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu),
 - ss. Wbudowany mechanizm wirtualizacji typu hypervisor, umożliwiający, zgodnie z uprawnieniami licencyjnymi, uruchomienie do 4 maszyn wirtualnych, Mechanizm szyfrowania dysków wewnętrznych i zewnętrznych z możliwością szyfrowania ograniczonego do danych użytkownika,
 - tt. Wbudowane w system narzędzie do szyfrowania partycji systemowych komputera, z możliwością przechowywania certyfikatów w mikrochipie TPM (Trusted Platform Module) w wersji minimum 1.2 lub na kluczach pamięci przenośnej USB,
 - uu. Wbudowane w system narzędzie do szyfrowania dysków przenośnych, z możliwością centralnego zarządzania poprzez polityki grupowe, pozwalające na wymuszenie szyfrowania dysków przenośnych,
 - vv. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania partycji w usługach katalogowych,
 - ww. Możliwość instalowania dodatkowych języków interfejsu systemu operacyjnego oraz możliwość zmiany języka bez konieczności reinstalacji systemu.
10. Certyfikaty i standardy:
- a. Certyfikat ISO 9001 (lub równoważny) w wersji aktualnej na dzień składania ofert dla producenta sprzętu (należy załączyć do oferty),
 - b. Certyfikat ISO 14001 (lub równoważny) w wersji aktualnej na dzień składania ofert dla producenta sprzętu (należy załączyć do oferty),
 - c. Deklaracja zgodności CE (załączyć do oferty),
 - d. Dokument potwierdzający posiadanie certyfikatu lub oświadczenie producenta, że oferowany model komputera jest zgodny z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych,
 - e. Dokument potwierdzający posiadanie certyfikatu lub oświadczenie producenta, że oferowany model laptopa poprawnie współpracuje z oferowanym systemem operacyjnym,
 - f. Certyfikat EPEAT na poziomie GOLD dla Polski. Wymagany wpis dotyczący oferowanej stacji dostępowej w internetowym katalogu <http://www.epeat.net> - dopuszcza się wydruk ze strony internetowej
 - g. Certyfikat Energy Star 8.0 – komputer musi znajdować się na liście zgodności dostępnej na stronie www.energystar.gov
 - h. Certyfikat TCO 9 – wymagany wpis dla modelu na stronie TCO <https://tcocertified.com/>
 - i. Zgodność z MIL-STD 810H – potwierdzone oświadczeniem producenta komputera oraz do zweryfikowania w ogólnodostępnych materiałach produktowych.
11. Głośność: Maksymalny poziom ciśnienia akustycznego w pozycji operatora nie może przekraczać 25 dB w trybie bezczynności (IDLE) przy pracującym układzie chłodzenia (zgodnie z normą ISO 7779). (wartość do zweryfikowania w dokumentacji technicznej komputera).
12. Waga max. 2,50 kg z baterią.
13. Możliwość odczytania z BIOS:
- a. Wersji BIOS wraz z datą wydania wersji,
 - b. Modelu procesora, prędkości procesora, wielkość pamięci cache L1/L2/L3,
 - c. Informacji o ilości pamięci RAM wraz z informacją o jej prędkości, pojemności i obsadzeniu na poszczególnych slotach,
 - d. Informacji o dysku twardym: model,
 - e. Informacji o MAC adresie karty sieciowej,
 - f. Zaimplementowany w BIOS podstawowy system diagnostyczny umożliwiający przetestowanie w celu wykrycia usterki zainstalowanych komponentów w oferowanym komputerze bez konieczności uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych. Minimalne funkcjonalności systemu diagnostycznego:

- i. test procesora
 - ii. test pamięci RAM
 - iii. test dysku twardego
 - iv. test baterii
 - v. test płyty głównej
14. Możliwość wyłączenia/włączenia zintegrowanej karty sieciowej, kontrolera audio, portów USB, funkcjonalności ładowania zewnętrznych urządzeń przez port USB, wewnętrznych głośników, wirtualizacji z poziomu BIOS bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych.
15. Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z dysku twardego, zewnętrznych urządzeń oraz sieci bez potrzeby uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych.
16. Możliwość ustawienia hasła dla BIOS na poziomie administratora, bez potrzeby uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych.
17. Możliwość ustawienia hasła dla dysku twardego w tym również dla dysków NVMe, bez potrzeby uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych.
18. BIOS musi posiadać funkcję update BIOS z opcją automatycznego update BIOS przez sieć włączaną na poziomie BIOS przez użytkownika bez potrzeby uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych.
19. W BIOS musi być zaimplementowany mechanizm trwałego kasowania danych z dysków twardech zainstalowanych w komputerze w tym również dysków SSD NVMe – mechanizm uruchamiany na życzenie przez użytkownika.
20. BIOS musi posiadać następujące cechy:
 - a. możliwość autoryzacji przy starcie komputera każdego użytkownika jego hasłem indywidualnym lub hasłem administratora,
 - b. kontrola sekwencji boot-owej,
 - c. możliwość startu systemu z urządzenia USB,
 - d. funkcja blokowania BOOT-owania stacji roboczej z zewnętrznych urządzeń,
 - e. BIOS musi zawierać nieulotną informację z nazwą produktu, jego numerem seryjnym, wersją BIOS, zainstalowanym fabrycznie systemem operacyjnym, a także informację o: typie zainstalowanego procesora, ilości pamięci RAM,
21. Możliwość zapięcia linki typu Kensington.
22. Komputer musi posiadać zintegrowany w płycie głównej aktywny układ zgodny ze standardem Trusted Platform Module (TPM v 2.0).
23. Obudowa o wzmocnionej konstrukcji, spełniająca wymogi normy Mil-Std-810H.
24. Zaimplementowany w BIOS mechanizm zakładania hasła dla dysków twardech zainstalowanych w komputerze w tym również dla dysków SSD NVMe.
25. Zaimplementowany system diagnostyczny z graficznym interfejsem użytkownika w języku polskim lub angielskim, umożliwiający przetestowanie w celu wykrycia usterki zainstalowanych komponentów w oferowanym komputerze bez konieczności uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych. System diagnostyczny może być zainstalowany na ukrytej dedykowanej partycji dysku twardego. Minimalne funkcjonalności systemu diagnostycznego:
 - a. informacje o systemie:
 - i. Procesor: typ procesora, jego obecna prędkość.
 - ii. Pamięć RAM: rozmiar pamięci RAM, osadzenie na poszczególnych slotach, szybkość pamięci, nr seryjny, typ pamięci, nr części, nazwa producenta.
 - iii. Dysk twarde: model, wersja firmware, nr seryjny, procentowe zużycie dysku.
 - iv. Data wydania i wersja BIOS.

- v. Nr seryjny komputera.
 - b. możliwość przeprowadzenia szybkiego oraz szczegółowego testu kontrolującego komponenty komputera
 - c. możliwość przeprowadzenia testów poszczególnych komponentów a w szczególności: procesora, pamięci RAM, dysku twardego, karty dźwiękowej, klawiatury, myszy, sieci, płyty głównej, portów USB, karty graficznej
 - d. rejestr przeprowadzonych testów zawierający min.: datę testu, wynik, identyfikator awarii
 - e. Komputer musi posiadać sprzętowy mechanizm weryfikacji integralności BIOS/UEFI oparty na sprzętowym fundamencie zaufania (Hardware Root of Trust).
 - f. W przypadku wykrycia nieautoryzowanej modyfikacji lub uszkodzenia kodu BIOS, system musi posiadać funkcję automatycznego przywrócenia jego bezpiecznej, fabrycznej wersji bez ingerencji użytkownika.
 - g. Mechanizm bezpieczeństwa musi chronić krytyczne dane rozruchowe (MBR/GPT) oraz umożliwiać bezpieczne odzyskiwanie systemu operacyjnego z chmury producenta (Cloud Recovery) w przypadku awarii dysku.
 - h. Możliwość zdalnego monitorowania incydentów bezpieczeństwa na poziomie BIOS przez administratora (np. poprzez logi WMI lub dedykowane konsole zarządzające).
26. Wbudowane porty i złącza: min. 1 x HDMI 2.1, min. 1 szt. USB typ-A o przepustowości 5 Gbps z ładowaniem zewnętrznych urządzeń, min. 2 szt. USB typu-C z czego min. 2szt. Thunderbolt 4, RJ-45, 1x złącze słuchawkowe stereo/mikrofonowe (combo audio), wbudowana kamera 5MP w obudowę ekranu laptopa i m.in. dwa mikrofony.
27. Karta sieciowa LAN 10/100/1000 Ethernet RJ 45 zintegrowana z płytą główną oraz WiFi 6E 802.11a/b/g/n/ac/ax 2x2 (160MHz) wraz z Bluetooth 5.3 COMBO, zintegrowany z płytą główną lub w postaci wewnętrznego modułu mini-PCI Express.
28. Klawiatura (układ US -QWERTY) odporna na zalanie, podświetlana od dołu z min 2-stopniową regulacją poziomu podświetlenia, z prawej strony wydzielona klawiatura numeryczna..
29. Touchpad/Clickpad
30. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej komputera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.
31. Kąt otwarcia ekranu notebooka min. 165 stopni.
32. **Obudowa:** Wykonana z materiałów o podwyższonej wytrzymałości (aluminium lub stopy magnezu) co najmniej w obrębie obudowy matrycy oraz panelu roboczego (palmrest).
33. Dostępny dedykowany slot wraz z wyprowadzoną instalacją antenową dla modułu WWAN (LTE/5G).
34. Min. 3-letnia gwarancja producenta (dla baterii min 1 rok), wymaga się, aby serwis był świadczony w miejscu użytkowania sprzętu. Firma serwisująca musi posiadać ISO 9001 na świadczenie usług serwisowych oraz posiadać autoryzację producenta komputera. Serwis urządzeń musi być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta

17. Komputer stacjonarny TYP 3 – 4 sztuki

Przedmiotem zamówienia jest komputer stacjonarny dla administratorów.

Wymagania:

1. Komputer stacjonarny typu Tower.
2. Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji obliczeniowych, aplikacji graficznych, dostępu do internetu oraz poczty elektronicznej.
3. Procesor min. 20-rdzeniowy, osiągający w teście PassMark CPU Mark wynik min. 48000 punktów – wydruk ze strony należy dołączyć do oferty:
https://www.cpubenchmark.net/cpu_list.php potwierdzający spełnienie wymogów SIWZ lub

wyników testów równoważnych. W przypadku użycia przez oferenta równoważnych testów wydajności Zamawiający zastrzega sobie, iż w celu sprawdzenia poprawności przeprowadzenia testów oferent musi dostarczyć zamawiającemu oprogramowanie testujące, oba równoważne porównywalne zestawy oraz dokładny opis użytych testów wraz z wynikami w celu ich sprawdzenia w terminie nie dłuższym niż 7 dni od otrzymania zawiadomienia od zamawiającego.

4. Pamięć operacyjna min. 2x16 DDR5 z możliwością rozbudowy do min 128GB.
5. Pamięć masowa min. dwa dyski, każdy po 1TB M.2 PCIe NVMe połączone w RAID 1.
6. Karta graficzna zintegrowana z procesorem, ze wsparciem dla DirectX 12, OpenGL 4.5 oraz dla rozdzielczości 4096x2160@60Hz osiągająca w teście Average G3D Mark wynik minimum 1800 punktów. Do oferty należy dołączyć wydruk ze strony: [Http://www.videocardbenchmark.net](http://www.videocardbenchmark.net) potwierdzający spełnienie wymogów SIWZ
7. Obudowa typu Tower z zasilaczem minimum 400W i sprawności minimum 90% przy obciążeniu 100%.
8. Komputer musi posiadać system diagnostyczny (sprzętowy lub programowy na poziomie BIOS) informujący o awariach kluczowych komponentów (CPU, RAM, Grafika)
9. Karta dźwiękowa zintegrowana z płytą główną.
10. Możliwość odczytania z BIOS:
 - a. Wersji BIOS wraz z datą wydania wersji,
 - b. Modelu procesora, prędkości procesora, liczby rdzeni, wielkość pamięci cache L1/L2/L3,
 - c. Informacji o ilości pamięci RAM wraz z informacją o jej prędkości, pojemności i obsadzeniu na poszczególnych slotach,
 - d. Informacji o dysku twardym: model, pojemność,
 - e. Informacji o napędzie optycznym: model,
 - f. Informacji o MAC adresie karty sieciowej,
 - g. Informacji o kontrolerze Audio.
11. Możliwość wyłączenia/włączenia zintegrowanej karty sieciowej LAN, kontrolera audio, portów USB,
12. Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z dysku twardego, zewnętrznych urządzeń oraz sieci bez potrzeby uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych.
13. Możliwość ustawienia hasła na poziomie administratora, bez potrzeby uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych.
14. BIOS musi posiadać funkcję update BIOS z opcją automatycznego update BIOS przez sieć włączaną na poziomie BIOS przez użytkownika bez potrzeby uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych.
15. Diagnostyka uruchamiana z BIOS działająca bez obecności systemu operacyjnego czy dysku twardego umożliwiającą na przeprowadzenie testów diagnostycznych w tym m.in.:
 - a. test procesora
 - b. test dysku twardego w tym SSD
 - c. test pamięci RAM
 - d. test płyty głównej
 - e. klawiatury
16. BIOS musi posiadać możliwość:
 - a. skonfigurowania hasła „Power On” oraz ustawienia hasła dostępu do BIOSu (administratora) w sposób gwarantujący utrzymanie zapisanego hasła nawet w przypadku odłączenia wszystkich źródeł zasilania i podtrzymania BIOS,
 - b. możliwość ustawienia hasła na dysku (drive lock),
 - c. blokady/wyłączenia portów USB, karty sieciowej, karty audio,

- d. kontroli sekwencji boot-ącej,
 - e. startu systemu z urządzenia USB,
 - f. funkcja blokowania BOOT-owania stacji roboczej z zewnętrznych urządzeń.
17. Komputer musi posiadać zintegrowany w płycie głównej aktywny układ zgodny ze standardem Trusted Platform Module (TPM v 2.0).
18. Możliwość zapięcia linki typu Kensington do dedykowanego złącza w obudowie komputera.
19. Czujnik otwarcia zarządzany z poziomu BIOS.
20. Zaimplementowany w BIOS system diagnostyczny z graficznym interfejsem użytkownika w języku polskim lub angielskim, umożliwiający przetestowanie w celu wykrycia usterki zainstalowanych komponentów w oferowanym komputerze bez konieczności uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych. Minimalne funkcjonalności systemu diagnostycznego:
- a. informacje o systemie, min.:
 - i. Procesor: typ procesora, jego obecną prędkość.
 - ii. Pamięć RAM: rozmiar pamięci RAM, osadzenie na poszczególnych slotach, szybkość pamięci, nr seryjny, typ pamięci, nr części, nazwa producenta.
 - iii. Dysk twardy: model, typ, wersja firmware, nr seryjny, procentowe zużycie dysku, temperaturę pracy dysku.
 - iv. Wentylator: aktualną prędkość i obciążenie.
 - v. Data wydania i wersja BIOS.
 - vi. Nr seryjny komputera
 - b. możliwość przeprowadzenia szybkiego oraz szczegółowego testu kontrolującego komponenty komputera
 - c. możliwość przeprowadzenia testów poszczególnych komponentów a w szczególności: procesora, pamięci RAM, dysku twardego, karty dźwiękowej, klawiatury, myszy, sieci, napędu optycznego, płyty głównej, portów USB, karty graficznej
 - d. rejestr przeprowadzonych testów zawierający min.: datę testu, wynik, identyfikator awarii
21. Komputer musi być wyposażony w mechanizm ochrony i samonaprawy BIOS w przypadku jego uszkodzenia lub nieautoryzowanej modyfikacji, działający na poziomie sprzętowym (niezależnie od systemu operacyjnego)
22. Komputer musi być wyposażony w BIOS posiadający mechanizm samokontroli i samoczynnej autonaprawy, działający automatycznie przy każdym uruchomieniu komputera, który sprawdza integralność i autentyczność uruchamianego podsystemu BIOS oraz musi chronić Master Boot Record (MBR) oraz GUID Partition Table (GPT) przed uszkodzeniem lub usunięciem.
23. Certyfikaty i standardy:
- a. Certyfikat ISO 9001 dla producenta sprzętu (załączyć dokument potwierdzający spełnianie wymogu)
 - b. Deklaracja zgodności CE (załączyć do oferty)
 - c. Dokument potwierdzający posiadanie certyfikatu lub oświadczenie producenta, że oferowany model komputera jest zgodny z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych,
 - d. Dokument potwierdzający posiadanie certyfikatu lub oświadczenie producenta, że oferowany model komputera poprawnie współpracuje z oferowanym systemem operacyjnym,
 - e. Komputer musi spełniać wymogi normy Energy Star,
 - f. Wymagany certyfikat lub wpis dotyczący oferowanego modelu komputera w internetowym katalogu <http://www.energystar.gov> – dopuszcza się wydruk ze strony internetowej,
 - g. Komputer musi spełniać wymogi normy EPEAT na poziomie min GOLD dla Polski,

- h. Wymagany certyfikat lub wpis dotyczący oferowanego modelu komputera w internetowym katalogu <http://www.epeat.net> – wymaga się wydruku ze strony internetowej,
- 24. Maksymalny poziom ciśnienia akustycznego w pozycji operatora nie może przekraczać 25 dB w trybie bezczynności (IDLE) przy pracującym układzie chłodzenia (zgodnie z normą ISO 7779).
- 25. System operacyjny fabrycznie przeinstalowany przez producenta - klasy desktop musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:
 - a. Dostępne dwa rodzaje graficznego interfejsu użytkownika:
 - i. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
 - ii. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych,
 - b. Interfejsy użytkownika dostępne w wielu językach do wyboru – w tym Polskim i Angielskim,
 - c. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimedialny, pomoc, komunikaty systemowe,
 - d. Wbudowany system pomocy w języku polskim,
 - e. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim,
 - f. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się” pisma użytkownika – obsługa języka polskiego,
 - g. Funkcjonalność rozpoznawania mowy, pozwalającą na sterowanie komputerem głosowo, wraz z modułem „uczenia się” głosu użytkownika,
 - h. Możliwość dokonywania bezpłatnych aktualizacji i poprawek w ramach wersji systemu operacyjnego poprzez Internet, mechanizmem udostępnianym przez producenta systemu z możliwością wyboru instalowanych poprawek oraz mechanizmem sprawdzającym, które z poprawek są potrzebne,
 - i. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego,
 - j. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego,
 - k. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6,
 - l. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami,
 - m. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi),
 - n. Funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer,
 - o. Możliwość zarządzania stacją roboczą poprzez polityki grupowe – przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji,
 - p. Rozbudowane, definiowalne polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji,
 - q. Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu, zgodnie z określonymi uprawnieniami poprzez polityki grupowe,
 - r. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników,
 - s. Mechanizm pozwalający użytkownikowi zarejestrowanego w systemie przedsiębiorstwa/instytucji urządzenia na uprawniony dostęp do zasobów tego systemu,

- t. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych,
- u. Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi,
- v. Możliwość obsługi standardu NFC (near field communication),
- w. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących),
- x. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny,
- y. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509,
- z. Mechanizmy logowania do domeny w oparciu o:
 - i. Login i hasło,
 - ii. Karty z certyfikatami (smartcard),
 - iii. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),
- aa. Mechanizmy wieloelementowego uwierzytelniania,
- bb. Wsparcie dla uwierzytelniania na bazie Kerberos v.5,
- cc. Wsparcie do uwierzytelnienia urządzenia na bazie certyfikatu,
- dd. Wsparcie dla algorytmów Suite B (RFC 4869),
- ee. Wsparcie wbudowanej zapory ogniowej dla Internet Key Exchange v. 2 (IKEv2) dla warstwy transportowej IPsec,
- ff. Wbudowane narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk,
- gg. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach,
- hh. Wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń,
- ii. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem,
- jj. Rozwiązanie służące do automatycznego zbudowania obrazu systemu wraz z aplikacjami. Obraz systemu służyć ma do automatycznego upowszechnienia systemu operacyjnego inicjowanego i wykonywanego w całości poprzez sieć komputerową,
- kk. Rozwiązanie ma umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację,
- ll. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe,
- mm. Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe,
- nn. Udostępnianie modemu,
- oo. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej,
- pp. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci,
- qq. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.),
- rr. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu),
- ss. Wbudowany mechanizm wirtualizacji typu hypervisor, umożliwiający, zgodnie z uprawnieniami licencyjnymi, uruchomienie do 4 maszyn wirtualnych,

- tt. Mechanizm szyfrowania dysków wewnętrznych i zewnętrznych z możliwością szyfrowania ograniczonego do danych użytkownika,
 - uu. Wbudowane w system narzędzie do szyfrowania partycji systemowych komputera, z możliwością przechowywania certyfikatów w mikrochipie TPM (Trusted Platform Module) w wersji minimum 1.2 lub na kluczach pamięci przenośnej USB,
 - vv. Wbudowane w system narzędzie do szyfrowania dysków przenośnych, z możliwością centralnego zarządzania poprzez polityki grupowe, pozwalające na wymuszenie szyfrowania dysków przenośnych,
 - ww. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania partycji w usługach katalogowych,
 - xx. Możliwość instalowania dodatkowych języków interfejsu systemu operacyjnego oraz możliwość zmiany języka bez konieczności reinstalacji systemu.
26. Wbudowane porty i złącza:
- a. porty video: 1szt. HDMI 2.1 oraz 2 szt. DP 2.1
 - b. z przodu: min. 6 x USB min. 3.2 w tym min: 4 szt USB Typ-A o przepustowości do 10 Gbps oraz 2 szt USB Typ-C o przepustowości do 20 Gbps, port audio COMBO
 - c. z tyłu: min. 5szt. USB
 - d. port sieciowy RJ-45
27. Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) portów i złączy nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek, adapterów itp.
28. Karta sieciowa 10/100/1000 Ethernet RJ 45 (zintegrowana) z obsługą PXE, WoL,
29. Karta WiFi 6 Wireless 2x2 z Bluetooth min. 5.3 M.2 Combo
30. Płyta główna wyposażona w:
- a. min. 4 złącza DIMM z obsługą do 128GB pamięci RAM
 - b. min. 4 złącza SATA 3.0
 - c. min. 1 złącze M.2 PCIe x1 dla WLAN
 - d. min. 3 złącza M.2 PCIe dla dysków SSD
 - e. min. 1x PCI Express Gen 5 x16, 1x PCI Express Gen4 x16, 2x PCI Express Gen3 x1
31. Klawiatura USB w układzie QWERTY, z wyspą numeryczną.
32. Mysz optyczna USB z min dwoma klawiszami oraz rolką (scroll).
33. Wbudowana w płytę główną technologia zarządzania i monitorowania komputera na poziomie sprzętowym działająca niezależnie od stanu czy obecności systemu operacyjnego oraz stanu włączenia komputera podczas pracy na zasilaczu sieciowym AC, obsługująca zdalną komunikację siecią w oparciu o protokół IPv4:
- a. zdalne przejęcie konsoli tekstowej systemu, przekierowanie procesu ładowania systemu operacyjnego,
 - b. zdalne przejęcie pełnej konsoli graficznej systemu tzw. KVM Redirection (Keyboard, Video, Mouse) bez udziału systemu operacyjnego ani dodatkowych programów, również w przypadku braku lub uszkodzenia systemu operacyjnego,
 - c. możliwość konfiguracji parametrów funkcji zarządzania (m.in. parametrów kont uprawnionych do zarządzania sprzętowego).
34. Ogólnopolska telefoniczna infolinia/linia techniczna producenta komputera (ogólnopolski numer – w ofercie należy podać numer telefonu) dostępna w czasie obowiązywania gwarancji na sprzęt i umożliwiająca po podaniu numeru seryjnego urządzenia:
- a. weryfikację konfiguracji fabrycznej wraz z wersją fabrycznie dostarczonego oprogramowania (system operacyjny, szczegółowa konfiguracja sprzętowa - CPU, HDD, pamięć)
 - b. sprawdzenie czasu obowiązywania i typ udzielonej gwarancji
35. Możliwość aktualizacji i pobrania sterowników do oferowanego modelu komputera w najnowszych certyfikowanych wersjach przy użyciu dedykowanego darmowego oprogramowania producenta lub bezpośrednio z sieci Internet za pośrednictwem strony www producenta komputera po podaniu numeru seryjnego komputera lub modelu komputera

36. Możliwość weryfikacji czasu obowiązywania i reżimu gwarancji bezpośrednio z sieci Internet za pośrednictwem strony www producenta komputera.
37. 3-letnia gwarancja producenta, serwis musi być realizowany w miejscu użytkowania sprzętu. Firma serwisująca musi posiadać ISO 9001 na świadczenie usług serwisowych oraz posiadać autoryzację producenta komputera.

18. Monitor – 4 sztuki

Przedmiotem zamówienia jest monitor do komputera stacjonarnego dla administratorów.

Wymagania:

1. Typ panelu LCD IPS, panel matowy
2. Rozmiar Ekranu 31,5" (widoczny)
3. Rozdzielczość zalecana 3840 x 2160 pikseli
4. Współczynnik proporcji 16:9
5. Liczba wyświetlanych kolorów 1.07 miliarda
6. Pokrycie barw sRGB 99%, Display P3 98%
7. Czas reakcji 5 ms
8. Jasność 400 cd/m2
9. Kontrast rzeczywisty nie dynamiczny min 1300:1
10. Kąt widzenia 178 stopni w poziomie, 178 stopni w pionie
11. Złącza:
 - a. 1 x DisplayPort 1.4
 - b. 1 x DisplayPort 1.4 out
 - c. 1 x HDMI 2.0
 - d. 4 x USB 3.2 typ A
 - e. 1x USB typ C
 - f. 1x Thunderbolt 40Gbps (Power Delivery min. 90W)
 - g. 1x RJ-45
12. Wbudowany zasilacz. Zamawiający nie dopuszcza zasilaczy zewnętrznych.
13. Kąt pochylenia | Obrót -5 / 20 (przód/tył)
14. Panel obrotowy PIVOT
15. Regulacja wysokości co najmniej 150mm
16. Możliwość mocowania na ścianie, standard VESA 100 x 100 mm
17. Certyfikaty:
 - a. Monitor winien być wyprodukowany zgodnie z normą ISO-9001 / ISO-14001 lub równoważną.
 - b. Monitor musi posiadać deklarację CE.
 - c. Monitor musi spełniać normę EPEAT poziom GOLD lub równoważny. Potwierdzenie spełnienia powyższego wymogu musi znajdować się na stronie internetowej www.epeat.net.
 - d. Certyfikat TCO
 - e. Certyfikat ENERGY STAR®
18. Dołączone przewody: Kabel sygnałowy DisplayPort, kabel zasilający
 19. 36 miesięcy gwarancji producenta w miejscu instalacji (może być uzyskany poprzez dostarczenie odpowiednich produktów przedłużających standardową gwarancję).
20. Czas reakcji serwisu do końca następnego dnia roboczego.
21. Sprzęt musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucji na rynek Polski.

19. System Zarządzania Bezpieczeństwem Informacji – 1 komplet

Zakres prac dotyczących dokumentacji SZBI:

1. Opracowanie dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (dalej zwanej „SZBI”), w skład której wchodzi następujące dokumenty:
 - a. Polityka Bezpieczeństwa Informacji;
 - b. Polityka Zabezpieczeń IT;
 - c. Plan ciągłości działania;
 - d. Procedura zarządzania incydentami cyberbezpieczeństwa;
 - e. Analiza ryzyka w zakresie Bezpieczeństwa Informacji;
2. Wdrożenie SZBI we współpracy z kierownikiem jednostki lub osobami wyznaczonymi do wdrożenia SZBI.
3. W ramach dokumentacji SZBI ujęte zostaną następujące procedury:
 - a. procedury kontroli dostępu
 - b. zabezpieczenie pomieszczeń i obiektów
 - c. procedury czystego biurka i ekranu
 - d. procedury kopii zapasowych
 - e. procedury ochrony logów
 - f. bezpieczeństwo komunikacji
 - g. zarządzanie bezpieczeństwem sieci
 - h. przesyłanie informacji
 - i. plany ciągłości działania
 - j. procedury zarządzania incydentami
 - k. prywatność i ochrona danych osobowych
 - l. szacowanie ryzyka w obszarze bezpieczeństwa informacji
 - m. szkolenia personelu
4. Szczegółowa zawartość dokumentacji zostanie określona w zależności od stanu faktycznego odpowiadającego strukturze i zasobom Zamawiającego i wdrażanej jednostki w oparciu o wzajemne ustalenia dokonane we współpracy pomiędzy Stronami na etapie deklaracji stosowania oraz wszelkich innych informacji uzyskanych przez Wykonawcę w trakcie realizacji Umowy mogących mieć wpływ na treść dokumentacji. Usługi dotyczące czynności wdrażających dokumentację zostanie uznana za wykonaną po przekazaniu Zleceniodawcy przez Zleceniobiorcę całości dokumentacji SZBI i podpisaniu protokołu odbioru przez Zamawiającego.

20. Audyt końcowy w obszarze cyberbezpieczeństwa – 1 komplet

1. Audyt końcowy ma na celu potwierdzenie zgodności wdrożonego Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) oraz infrastruktury technicznej Szpitala z wymaganiami projektu KPO D1.1.2, w szczególności wskaźnika D21G.R2. Celem audytu jest ocena poziomu dojrzałości w obszarze cyberbezpieczeństwa oraz skuteczności wdrożonych polityk, procedur i zabezpieczeń organizacyjno-technicznych.
2. Audyt obejmuje wszystkie obszary, w których przetwarzane są dane osobowe i dane medyczne, w tym kluczowe systemy informacji medycznej (HIS, LIS, RIS, EDM), infrastrukturę urządzeń medycznych, systemy administracyjne, sieć komputerową, serwery, stacje robocze oraz systemy kopii zapasowych. Audyt ma potwierdzić zgodność z wymaganiami PN-EN ISO/IEC 27001:2022, Rozporządzenia KRI, ustawy o Krajowym Systemie Cyberbezpieczeństwa oraz RODO.
3. Audyt powinien obejmować ocenę zarówno organizacyjną, jak i techniczną, w tym:
 - a. strukturę organizacyjną bezpieczeństwa informacji, role i odpowiedzialności,
 - b. proces zarządzania ryzykiem i incydentami bezpieczeństwa,
 - c. ciągłość działania i ochronę danych (BIA, kopie zapasowe),
 - d. bezpieczeństwo sieci i urządzeń brzegowych (firewall, segmentacja sieci),
 - e. bezpieczeństwo serwerów, platform wirtualizacyjnych i stacji roboczych,

- f. kontrolę dostępu, uwierzytelnianie użytkowników i zarządzanie uprawnieniami,
 - g. logowanie zdarzeń i analizę bezpieczeństwa systemów,
 - h. zarządzanie aktualizacjami i łataniami bezpieczeństwa,
 - i. mechanizmy kopii bezpieczeństwa i przywracania danych.
4. Audyt zostanie przeprowadzony zgodnie z zasadami PN-EN ISO/IEC 19011:2018 i oparty na metodyce audytowej stosowanej w systemach zarządzania bezpieczeństwem informacji. Obejmuje przegląd dokumentacji SZBI, wywiady z personelem, analizę konfiguracji technicznej oraz testy kontrolne wybranych mechanizmów zabezpieczeń. Audyt końcowy może być realizowany w trybie mieszanym (zdalnym i stacjonarnym).
5. Audyt przeprowadzi zespół co najmniej dwóch audytorów posiadających kwalifikacje określone w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. (Dz.U. poz. 1999). Co najmniej jeden audytor musi posiadać certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji wg normy PN-EN ISO/IEC 27001 oraz certyfikat audytora wiodącego systemu zarządzania ciągłością działania wg normy PN-EN ISO 22301.
6. Wyniki audytu zostaną przedstawione w formie raportu zawierającego: opis stanu faktycznego, listę niezgodności i obserwacji, ocenę poziomu dojrzałości cyberbezpieczeństwa, rekomendacje działań doskonalących oraz wypełnioną ankietę dojrzałości zgodnie z wymaganiami projektu KPO D1.1.2. Raport musi być podpisany przez audytora wiodącego.

21. Szkolenia dla kadry kierowniczej i pracowników – 1 komplet

Przedmiotem zamówienia jest platforma elearningowa do szkoleń online, umożliwiająca przeprowadzenie kampanii edukacyjnej z zakresu podstaw bezpieczeństwa w Internecie, bezpieczeństwa informacji podczas pracy zdalnej czy też przy bezpieczeństwa IT przy codziennych obowiązkach. Wykonawca musi dostarczyć platformę dedykowaną 750 użytkownikom Zamawiającego i świadczoną przez okres min. 12 miesięcy.

Wymagania:

1. Platforma musi być dostępna za pomocą dowolnej, nowoczesnej przeglądarki internetowej (Chrome, Firefox, Edge), a sama usługa ma być świadczona z centrum danych znajdującym się na terenie Unii Europejskiej.
2. Dostęp administracyjny musi odbywać się minimum w języku angielskim lub polskim.
3. Dostęp dla użytkownika musi odbywać się minimum w języku polskim, angielskim oraz trzecim wybranym przez Zamawiającego języku.
4. Podczas tworzenia użytkownika, musi być możliwość wyboru domyślnego języka, w którym będzie on otrzymywał powiadomienia, będzie otrzymywał kampanie phishingowe, oraz w którym będzie miał dostęp do szkoleń. Niedopuszczalnym jest konieczność tworzenia osobnej kampanii phishingowej lub kursu per każdy z dostępnych dla Zamawiającego języków.
5. Platforma musi zawierać poszczególne komponenty:
 - a. Moduł szkoleniowy:
 - i. Platforma musi zawierać minimum 250 szkoleń, dostępnych w języku polskim, angielskim oraz trzecim dowolnym języku wybranym przez Zamawiającego
 - ii. W przypadku trzeciego języka liczba szkoleń może być mniejsza, natomiast wymaga się nie mniej szkoleń niż 100
 - iii. Szkolenia muszą być dostępne w postaci filmów, plików audio, prezentacji, broszur oraz interaktywnych gier, zakończonych testami lub quizami sprawdzającymi przyswojenie przedstawianego materiału merytorycznego.
 - iv. Szkolenia muszą zapewniać zakres tematyczny co najmniej w ujęciu:
 1. Ryzyka związanego z AI
 2. Bezpieczeństwa informacji
 3. Klasyfikacji informacji
 4. Cyklu życia informacji

5. Własności intelektualnej
 6. Haseł
 7. Kontroli dostępu
 8. Poczty Email
 9. Bezpieczeństwa w Internecie
 10. Inżynierii społecznej/socjotechnik
 11. Prywatności
 12. Danych płatniczych
 13. Phishingu
 14. Malware/Wirusów/Ransomware
 15. Kradzieży tożsamości
 16. Mediów społecznościowych
 17. Pracy zdalnej
 18. Urządzeń mobilnych
 19. Wycieku danych
 20. Otwartych sieci WiFi
 21. Usług chmurowych
 22. Personalnych urządzeń w organizacji (BYOD)
 23. Bezpieczeństwa w podróży
- v. To samo szkolenie musi być dostępne zarówno w trybie wymagającym interakcji (np. odtworzenie filmu w całości by móc przejść dalej) jak i w trybie przeglądu, który nie wymaga konieczności interakcji by przejść szkolenie.
 - vi. System musi dawać możliwość podzielenia użytkowników na grupy, dla których będą przygotowane indywidualne harmonogramy szkoleń oraz dedykowane kampanie phishingowe.
 - vii. Łączny czas trwania wszystkich materiałów szkoleniowych w języku polskim musi wynosić co najmniej 10 godzin.
- b. Moduł Quizów:
- i. System musi pozwalać na stworzenie quizu, niezwiązanego z żadnym szkoleniem
 - ii. Quizy muszą być dostępne w trzech formatach: ogólnodostępne, tylko dla wybranych użytkowników lub tylko dostępne za pośrednictwem linku
 - iii. Administrator może wybrać czy quiz wymaga pewnej punktacji do zaliczenia czy też nie.
 - iv. Administrator może wybrać, czy quiz można powtarzać w przypadku niepowodzenia
 - v. Pytania do quizów może tworzyć ręcznie administrator lub mogą one być zaciągane z innych modułów systemu
 - vi. Moduł narzędzi dodatkowych. Narzędzia dodatkowe muszą zawierać w sobie grafiki, ulotki, animacje, pozwalające na ich wydruk lub umieszczenie w interaktywnych elementach infrastruktury zamawiającego. Przykładem może być gif umieszczony w stopce maila, informując o zagrożeniach lub prowadzonej kampanii edukacyjnej.
- c. Dedykowana platforma phishingowa:
- i. Platforma phishingowa pozwalająca na generowanie i wysyłanie spreparowanych maili phishingowych do wszystkich użytkowników usługi (wedle ich domyślnego języka) oraz na generowanie, co najmniej, poniższych typów wiadomości e-mail:
 1. z linkiem prowadzącym do stronnym internetowej,
 2. z linkiem do portalu podszywającego się pod usługodawcę i pozwalającego na logowanie (weryfikację, czy użytkownicy są gotowi na

- falszywej stronie portalu zalogować się swoim loginem i hasłem);
platforma musi zapewniać bezpieczeństwo takiej operacji,
3. z załącznikiem zawierającym potencjalnie niebezpieczny kod,
 4. z załącznikiem w postaci dokumentu Word, Excel, PowerPoint, PDF, ZIP zawierającym potencjalnie niebezpieczny kod
- ii. W przypadku, gdy użytkownik pozwoli się oszukać, platforma musi posiadać możliwość automatycznego skierowania takiego użytkownika na dodatkowe szkolenie lub ponowne wykonanie jednego z wcześniej ukończonych szkoleń.
 - iii. Maile phishingowe muszą mieć możliwość dystrybucji w czasie, tak by nie użytkownicy dostali tę samą wiadomość w jednej chwili.
 - iv. Platforma musi posiadać rozbudowaną bazę szablonów maili oraz stron phishingowych, co najmniej maili pochodzących od:
 1. Microsoft Office365
 2. Microsoft Teams
 3. Microsoft Sharepoint
 4. Microsoft OneDrive
 5. DHL
 6. Limitu skrzynki pocztowej
 7. Zoom
 8. Google Drive
 9. Apple
 - v. Platforma musi pozwalać na wgranie własnego szablonu wiadomości Email
- d. Moduł raportujący obejmujący minimum:
- i. status wykonania szkoleń przez użytkowników, z podziałem na grupy i uwzględnieniem terminu wykonania szkoleń oraz wyniku quizów i testów,
 - ii. status kampanii, wraz z raportem o liczbie wysłanych e-maili oraz szczegółach zawierających informację: kto otworzył wiadomość, kto i kiedy pozwolił się oszukać, kto otworzył załącznik, kto wpisał dane w formularzu jaka była platforma oraz przeglądarka z której wykonał tę akcję oraz szczegółowe daty wykonania tych operacji.
6. W ramach świadczonej platformy usługodawca musi:
- a. Przygotować platformę do świadczenia usługi, założyć konta dla użytkowników oraz sprawdzić techniczne elementy związane z zapewnieniem dostarczenia wiadomości phishingowych z platformy do użytkowników,
 - b. Zaproponować do akceptacji Zamawiającego szczegółowy harmonogram szkoleń dopasowany do okresu świadczenia usługi,
 - c. Zaplanować na podstawie harmonogramu całą kampanię szkoleniową i dostarczyć ją użytkownikom za pośrednictwem dedykowanych wiadomości e-mail,
 - d. Dostarczać pełny raport z realizacji szkoleń dla użytkowników oraz przeprowadzonych kampanii po zakończeniu każdego modułu szkoleniowego oraz zbiorcze raporty końcowe,
 - e. Wprowadzić zmiany w harmonogramie i zakresie szkoleń w przypadku potrzeby modyfikacji, zmian kolejności szkoleń lub liczby użytkowników (nie więcej niż 5 zmian w okresie trwania usługi).
 - f. Przeprowadzić minimum 4 kampanie phishingowe
7. Wszystkie moduły (platforma zarządzająca, szkoleniowa, phishingowa, moduł raportowania, moduł quizów, moduł narzędzi dodatkowych) muszą pochodzić od jednego producenta i być świadczone w trybie 24/7/365.
8. Kursy, Quizy oraz Phishing mogą zostać połączone w jedną, spójną kampanię, wykonywaną krok po kroku wedle ustalonego wcześniej harmonogramu, bez konieczności interakcji z zewnątrz.

9. Zgłoszenia i komunikacja z usługodawcą będą przyjmowane w języku polskim w trybie 8x5, przez dedykowany portal serwisowy dostępny w sieci Internet lub wskazany adres email oraz infolinię w języku polskim.
10. Czas reakcji usługodawcy nie może być dłuższy niż 1 godzina – reakcja w postaci połączenia telefonicznego lub odpowiedzi w portalu serwisowym/ odpowiedzi mailowej

22. Instalacja, konfiguracja, wdrożenie i uruchomienie – 1 komplet

Wykonawca zobowiązany jest do wykonania usługi instalacji, konfiguracji, wdrożenia oraz uruchomienia wszystkich dostarczonych w ramach niniejszego postępowania elementów infrastruktury IT i cyberbezpieczeństwa, w szczególności obejmujących serwery, deduplikator, bibliotekę taśmową oraz oprogramowanie do backupu, zgodnie z dokumentacją producentów, najlepszymi praktykami branżowymi oraz wymaganiami Zamawiającego.

Zakres prac obejmuje co najmniej:

1. Instalację fizyczną urządzeń w szafach RACK Zamawiającego, w tym montaż serwerów, deduplikatora, biblioteki taśmowej, przełączników oraz bezprzewodowych punktów dostępowych wraz z podłączeniem zasilania i okablowania sieciowego.
2. Konfigurację sprzętową, w szczególności:
 - o konfigurację macierzy dyskowych i kontrolerów RAID,
 - o konfigurację dysków systemowych i danych,
 - o konfigurację zasilania redundantnego oraz wentylacji,
 - o aktualizację BIOS, firmware, BMC oraz innych komponentów do zalecanych wersji producenta.
3. Instalację i konfigurację systemów operacyjnych, w tym:
 - o instalację dostarczonych systemów operacyjnych zgodnie z licencjami,
 - o konfigurację podstawowych ról i usług systemowych,
 - o integrację z istniejącą infrastrukturą Microsoft Active Directory.
4. Instalację i konfigurację oprogramowania do backupu, w tym:
 - o instalację serwera zarządzającego, serwerów mediów oraz agentów,
 - o konfigurację repozytoriów backupowych (dyskowych i taśmowych),
 - o integrację z deduplikatorem i biblioteką taśmową,
 - o konfigurację mechanizmów deduplikacji, szyfrowania, retencji oraz ochrony typu WORM/Air Gap.
5. Konfigurację polityk kopii zapasowych, obejmującą:
 - o konfigurację harmonogramów backupu,
 - o konfigurację kopii pełnych, przyrostowych i syntetycznych,
 - o konfigurację zadań testowego odtwarzania danych (restore test).
6. Instalację i konfigurację oprogramowania do archiwizacji poczty, w tym:
 - o instalację oprogramowania na serwerze,
 - o archiwizacja poczty z obecnego serwera pocztowego,
 - o instalacja i uruchomienie nowego systemu poczty elektronicznej,
 - o migracja obecnych kont pocztowych i wiadomości przechowywanych na serwerze Postfix (wersja 2.11.0) z bazą danych MySQL.
7. Testy poprawności działania, w tym:
 - o testy poprawności wykonywania kopii zapasowych,
 - o testy odtwarzania danych (plików, maszyn wirtualnych),
 - o testy komunikacji pomiędzy wszystkimi komponentami systemu.
8. Uruchomienie produkcyjne rozwiązania oraz przekazanie go Zamawiającemu do eksploatacji.

9. Dokumentację powdrożeniową, obejmującą co najmniej:
 - opis architektury wdrożonego rozwiązania,
 - opis konfiguracji urządzeń i oprogramowania,
 - wykaz zastosowanych polityk backupu i retencji,
 - instrukcję administracyjną w zakresie podstawowej obsługi systemu.
10. Przeprowadzenie instruktażu/szkolenia administratorów Zamawiającego w zakresie obsługi i administracji wdrożonym rozwiązaniem (min. 1 sesja).

Wdrożenie musi zostać wykonane przez osoby posiadające aktualne certyfikaty techniczne producentów oferowanych rozwiązań, a całość prac zakończona podpisaniem protokołu odbioru potwierdzającego prawidłowe uruchomienie systemu.