Załącznik do SWZ - Szczegółowy opis przedmiotu zamówienia – wymagania funkcjonalne i niefunkcjonalne Systemu

1. Wstęp

W niniejszym załączniku do SWZ, Zamawiający zawarł wymagania funkcjonalne i niefunkcjonalne jakie musi spełnić System stanowiący przedmiot dostawy i wdrożenia, budowany w oparciu o infrastrukturę sprzętową wyspecyfikowaną w Załączniku nr A.3 do SWZ.

Dla spełnienia wymagań stawianych wobec Systemu, Wykonawca zobowiązany jest dostarczyć niezbędne Oprogramowanie oraz przeprowadzić konfigurację Systemu.

2. Słownik Pojęć

Użyte w dokumencie skróty i pojęcia należy rozumieć w sposób przedstawiony w poniższej tabeli:

Pojęcie / Skrót	Wyjaśnienie / Opis
Moduł e-Platforma	Podsystem e-Usług Systemu, udostępniający pacjentom i personelowi Zamawiającego 3 e-usługi: e-informacja, e-wizyta, e-wniosek
System	System informatyczny stanowiący przedmiot wdrożenia w ramach Umowy z Zamawiającym, składający się z: infrastruktury sprzętowej oraz niezbędnego oprogramowania bazodanowego, systemowego i narzędziowego (aplikacyjnego) do obsługi e-usług (e-Platforma) i elektronicznej dokumentacji medycznej.
EDM	Elektroniczna Dokumentacja Medyczna w rozumieniu Rozporządzenia Ministra Zdrowia z dnia 9 listopada 2015 r. w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania (Dz.U. z 2015 r. poz. 2069).
P1	Elektroniczna Platforma Gromadzenia, Analizy i Udostępniania zasobów cyfrowych o Zdarzeniach Medycznych. System informatyczny mający na celu umożliwienie organom administracji publicznej i obywatelom gromadzenie, analizę i udostępnianie zasobów cyfrowych o zdarzeniach medycznych, w zakresie zgodnym z ustawą z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia. Założeniem jest, iż w P1 będzie znajdowała się informacja o zdarzeniach medycznych wszystkich obywateli Polski niezależnie od płatnika, a także obywateli Unii Europejskiej i innych krajów, którzy skorzystają ze świadczeń zdrowotnych na terenie Polski.
P2	Platforma udostępniania on-line przedsiębiorcom usług i zasobów cyfrowych rejestrów medycznych, stanowi uniwersalne narzędzie służące komunikacji w obszarze sektora ochrony zdrowia. System umożliwia dwustronną wymianę dokumentów pomiędzy przedsiębiorcami i podmiotami publicznymi oraz elektroniczną rejestrację i aktualizację danych rejestrowych. Platforma jest dostępna dla użytkowników końcowych, którzy mogą rejestrować i korzystać z jej zasobów oraz funkcjonalności.
Portal Pacjenta	Strona WWW Zamawiającego dostępna w sieci Internet i sieci wewnętrznej Zamawiającego, którego elementem częścią stanie się e-Platforma dostarczona w ramach realizacji niniejszego Zamówienia.
Zamawiający	Podlaski Wojewódzki Ośrodek Medycyny Pracy
ID	Identyfikator wymagania
OPD	Podsystem obsługi pacjenta i obsługi elektronicznej dokumentacji medycznej
NFZ	Narodowy Fundusz Zdrowia
DK	Dział Diagnostyczno-Konsultacyjny
IS	Inspektor Sanitarny
PJSMP	Podstawowa Jednostka Służby Medycyny Pracy
WOMP	Wojewódzki Ośrodek Medycyny Pracy
PIP	Państwowa Inspekcja Pracy
PIS	Państwowa Inspekcja Sanitarna
PPIS	Państwowy Powiatowy Inspektor Sanitarny
SMP	Służba Medycyny Pracy
SZJ	System Zarzadzania Jakością obowiązujący u Zamawiającego
HIS	Hospital Information System – podstawowy system informatyczny do

Pojęcie / Skrót	Wyjaśnienie / Opis
	obsługi części medycznej działalności Zamawiającego
LIS	Laboratory Information System - system informatyczny do obsługi badań laboratoryjnych i współpracy z analizatorami laboratoryjnymi
RIS	Radiological Information System - system informatyczny do obsługi badań radiologicznych i zarządzania aparatami diagnostycznymi
PACS	System informatyczny archiwizacji obrazów i komunikacji, służący do przechowywania i przetwarzania obrazów medycznych (w formacie DICOM)
ERP	Enterprise Resource Planning – system informatyczny do planowania zarządzania ogółem zasobów przedsiębiorstwa (kadry-płace, finanse-księgowość, środki trwałe itp.)
PSIeZ	Podlaski System Informacyjny e-Zdrowie - zbudowany ze środków Europejskiego Funduszu Rozwoju Regionalnego pozyskanych w ramach Regionalnego Programu Operacyjnego Województwa Podlaskiego na lata 2007-2013 na podstawie Decyzji nr UDA-RPPD.04.01.00-20-001/11-00 z dnia 8 listopada 2011r.

3. Informacje o Zamawiającym

Zamawiający jest podmiotem leczniczym niebędącym przedsiębiorcą, w rozumieniu przepisów ustawy z dnia 15 kwietnia 2011 r. o działalności leczniczej (Dz. U. Nr 112, poz. 654, z późn. zm.), działającym w formie samodzielnego publicznego zakładu opieki zdrowotnej.

Nadrzędnym celem Zamawiającego jest świadczenie usług medycznych wynikających z ustawy o służbie medycyny pracy. Działalność ta prowadzona jest zgodnie z obowiązującymi aktami prawnymi i potrzebami pacjentów. Zamawiający prowadzi działalność statutową i komercyjną zgodnie z ustawą o służbie medycyny pracy z dn. 27 czerwca 1997 r. Celem działania jest ochrona zdrowia osób pracujących przed wpływem niekorzystnych warunków związanych ze środowiskiem pracy i sposobem jej wykonywania oraz sprawowanie profilaktycznej opieki zdrowotnej nad pracującymi na terenie województwa podlaskiego. Zamawiający jest jednostką służby medycyny pracy, prowadzoną w formie samodzielnego publicznego zakładu opieki zdrowotnej. Świadczy usługi na rzecz firm, instytucji i osób indywidualnych dbających o profilaktyczną opiekę zdrowotną swoją i swoich pracowników. Zamawiający specjalizuje się w kompleksowej obsłudze w zakresie medycyny pracy, zapewniając usługi medyczne w szerokim zakresie oraz na najwyższym poziomie. Współpracując z lekarzami wielu specjalności zapewnia szeroki wachlarz usług medycznych oferując konsultacje specjalistyczne, badania diagnostyczne i laboratoryjne. Sprawuje nadzór nad innymi jednostkami z terenu województwa, zajmującymi się opieką zdrowotną pracujących. Współpracuje z firmami, instytucjami publicznymi oraz innymi podmiotami w zakresie opieki profilaktycznej.

Do zadań wszystkich placówek Ośrodka należy:

- udzielanie konsultacji podstawowym jednostkom służby medycyny pracy;
- wykonywanie kontroli podstawowych jednostek służby medycyny pracy i osób realizujących zadania tej służby poza zakładami opieki zdrowotnej, w zakresie i w sposób określony w ustawie o służbie medycyny pracy;
- prowadzenie podyplomowego kształcenia z zakresu medycyny pracy, z wyjątkiem tych form, które z mocy odrębnych przepisów są zastrzeżone do kompetencji innych jednostek;
- prowadzenie działalności diagnostycznej i orzeczniczej w zakresie chorób zawodowych;
- rozpatrywanie odwołań od orzeczeń lekarskich wydawanych do celów przewidzianych w Kodeksie pracy;
- programowanie i realizacja działań z zakresu profilaktyki i promocji zdrowia;
- udzielanie konsultacji i opiniowanie spraw dotyczących organizacji i funkcjonowania opieki zdrowotnej nad pracującymi oraz innych spraw związanych z ochroną zdrowia pracujących;
- prowadzenie rejestrów zgłoszeń podjęcia oraz zakończenia działalności lekarza, pielęgniarki, psychologów w zakresie profilaktycznej opieki zdrowotnej nad pracującymi:
  - rejestr lekarzy uprawnionych do przeprowadzania badań profilaktycznych pracujących,
  - rejestr psychologów w służbie medycyny pracy,
  - rejestry podjęcia/zakończenia działalności podmiotu leczniczego sprawującego profilaktyczną opiekę zdrowotną nad pracującymi (praktyki indywidualne, ZOZ-y)
  - rejestr lekarzy uprawnionych woj. podlaskiego;
- udzielanie świadczeń zdrowotnych, w zakresie i na zasadach określonych w ustawie o służbie medycyny pracy, niezbędnych do prowadzenia specjalizacji z medycyny pracy;
- udzielanie świadczeń zdrowotnych na zlecenie jednostek podstawowych służby medycyny pracy w zakresie i na zasadach określonych w ustawie o służbie medycyny pracy;

- przyjmowanie, gromadzenie, przechowywanie i przetwarzanie dokumentacji służby medycyny pracy, przekazanej w związku z likwidacją jednostek organizacyjnych tej służby;
- gromadzenie, przechowywanie i przetwarzanie informacji zawartych w rejestrach, o których mowa w pkt. 8 Ustawy o służbie medycyny pracy oraz dokumentacji z kontroli jednostek podstawowych służby medycyny pracy zarejestrowanych na terenie województwa podlaskiego;
- przeprowadzanie okresowych badań lekarskich realizowanych w trybie art. 229 § 5 Kodeksu pracy, w przypadku, gdy podmiot zatrudniający pracownika uległ likwidacji;
- przeprowadzanie badań i wydawanie orzeczeń lekarskich określonych w odrębnych przepisach;
- współdziałanie z: pracodawcami i ich organizacjami, pracownikami i ich przedstawicielami, a zwłaszcza związkami zawodowymi, Państwową Inspekcją Pracy w zakresie ochrony zdrowia pracujących;
- realizacja zadań zleconych przez województwo podlaskie (działalność konsultacyjna, diagnostyczna i orzecznicza w zakresie patologii zawodowej, poradnictwo dla osób chorych na choroby zawodowe, udzielanie świadczeń w stosunku do uczniów szkół ponadpodstawowych i wyższych oraz uczestników studiów doktoranckich, narażonych na czynniki szkodliwe, uciążliwe i niebezpieczne);
- prowadzenie wydzielonej działalności gospodarczej, z której zyski służą realizacji statutowej PWOMP, w tym
  - udzielanie świadczeń zdrowotnych na podstawie umów z podmiotami administracji publicznej, ubezpieczycielami i innymi osobami fizycznymi lub prawnymi,
  - opracowywanie opinii dla sądów, firm ubezpieczeniowych itp. podmiotów;
  - wynajem lub wydzierżawianie wolnych pomieszczeń i urządzeń.

Ośrodek wykonuje:

1. Badania lekarskie i psychologiczne kierowców:
   - samochodu służbowego
   - transportu drogowego (kat. C,D, C+E, taxi)
   - inspektorów transportu drogowego
   - pojazdów uprzywilejowanych i przewożących wartości pieniężne
   - instruktorów, egzaminatorów
   - skierowanych przez Policję, Starostwo itp.
   - z ustawy o kierujących pojazdami
2. Badania lekarskie i psychologiczne osób występujących o wydanie pozwolenia na broń lub zgłaszających do rejestru broń pneumatyczną oraz posiadających pozwolenie na broń lub zarejestrowaną broń pneumatyczną

- badania odwoławcze

3. Badania pracowników młodocianych
4. Badania lekarskie dla kuratora sądowego, prokuratora, sędziego, kuratora sądowego, komornika sądowego, asesora komorniczego, aplikanta komorniczego, aplikantów aplikacji sędziowskich i prokuratorskich w Krajowej Szkole Sądownictwa i Prokuratury
5. Badania psychologiczne dla prokuratora, sędziego, kuratora sądowego, aplikantów aplikacji sędziowskich i prokuratorskich w Krajowej Szkole Sądownictwa i Prokuratury
6. Badania do świadectwa zdrowia marynarzy
7. Badania lekarskie, psychologiczne i psychiatryczne osób ubiegających się o wydanie albo posiadających licencję detektywów
8. Badania członków ochotniczych straży pożarnych
9. Badania lekarskie profilaktyczne pracowników, przewidziane w kodeksie pracy
   - wstępne
   - kontrolne
   - okresowe
   - badania odwoławcze od orzeczeń lekarskich
10. Badania lekarskie kandydatów do szkół ponadpodstawowych lub wyższych i na kwalifikacyjne kursy zawodowe, uczniów i słuchaczy tych szkół, studentów, słuchaczy kwalifikacyjnych kursów zawodowych oraz doktorantów
    - badania odwoławcze
11. Badania lekarskie, psychologiczne i psychiatryczne osób ubiegających się o wpis lub posiadających wpis na listę kwalifikowanych pracowników ochrony fizycznej
12. Badania odwoławcze pracownika ochrony fizycznej
13. Badania pracownika zabezpieczenia technicznego
14. Badania do celów sanitarno-epidemiologicznych
15. Badania do celu rozpoznania choroby zawodowej
16. Badania do karty oceny narażenia zawodowego
17. Badania do świadectwa zdrowia pracownika żeglugi śródlądowej
18. Badania psychologiczne i psychiatryczne osób ubiegających się lub posiadających prawo do wykonywania lub kierowania działalnością gospodarczą albo bezpośrednio zatrudnionych przy wytwarzaniu i obrocie materiałami wybuchowymi, bronią, amunicją oraz wyrobami o przeznaczeniu wojskowym lub policyjnym
    - badanie odwoławcze

19. Badania osób pracujących w narażeniu na azbest
20. Badanie osób pracujących w komorze hiperbarycznej
21. Kwalifikacja do szczepienia
22. Badania poekspozycyjne
23. Badania osób pracujących w narażeniu na promieniowanie jonizujące
24. Badania na wniosek własny
25. Badania na stanowiska konkursowe
26. Badania nauczycieli i nauczycieli akademickich do celów udzielenia urlopu dla poratowania zdrowia
    - badania odwoławcze
27. Badania do prawa wykonywania zawodu
28. Badania na kurs
29. Badania osób pracujących w tropiku
30. Konsultacje specjalistyczne
31. Badania specjalistyczne poborowych
32. Badania lekarskie i psychologiczne do wykonywania czynności inspektora transportu drogowego
    - badanie odwoławcze

Wykonuje również usługi diagnostyczne

Jednostki organizacyjne Zamawiającego:
1. Poradnia chorób zawodowych
2. Poradnia badań kierowców
3. Poradnia okulistyczna
4. Pracownia psychologiczna,

4. Założenia dla architektury logicznej systemu

System powstały w wyniku realizacji przedmiotu zamówienia winien zostać zbudowany z infrastruktury informatycznej oraz oprogramowania aplikacyjnego z wyróżnieniem dwóch logicznie rozdzielonych podsystemów:
- Podsystemu e-Usług
- Podsystemu Rejestrów

Oba podsystemy muszą bazować na tych samych zbiorach danych: pacjentów, personelu medycznego, usług, umów z partnerami, informacji o przebiegach wizyt, wykonanych badaniach itd.

Podsystem e-Usług, z poziomu Portalu Informacyjnego Placówki dostępnego w sieci Internet, musi udostępniać następujące usługi:
- e-informacja,
- e-wizyta,
- e-wniosek.

Podsystem Rejestrów
- Rejestr lekarzy uprawnionych do przeprowadzania badań profilaktycznych pracowników,
- Rejestr podjęcia oraz zakończenia działalności podmiotu leczniczego i indywidualnej praktyki lekarskiej sprawujących profilaktyczną opiekę zdrowotną nad pracującymi,
- Rejestr zgłoszeń podjęcia i zakończenia działalności psychologa w zakresie profilaktycznej opieki zdrowotnej nad pracującymi,
  Rejestr podmiotów leczniczych, które zawarły umowę z PWOMP na badania profilaktyczne uczniów szkół ponadpodstawowych i wyższych oraz uczestników studiów doktoranckich,

Przedmiotem zamówienia jest rozbudowa istniejącego systemu informatycznego PWOMP o e-Usługi i Rejestry oraz dostarczenie funkcjonalności potrzebnej do funkcjonowania wyżej wymienionych, w taki sposób, aby całość systemu informatycznego, który będzie funkcjonował w Podlaskim Wojewódzkim Ośrodku Medycyny Pracy po zakończeniu prac odzwierciedlał funkcjonalność opisaną w tym załączniku.

Ze względu na to, że Podlaski Wojewódzki Ośrodek Medycyny Pracy ma podpisaną umowę na kontynuację współpracy i utrzymanie Platformy Regionalnej e- Zdrowie, dostawca sytemu w niniejszym postępowaniu ma za zadanie zapewnienie integralności komunikacji systemu PWOMP i e-Zdrowie.
Szczegółowy opis integracji z platformą regionalną znajduje się w załączonym pliku
SWD_131129_PSIEZ_110925_JSO_01,
SWD_EDM_131202_PSIEZ_130631_DKO_01_Z02 - załącznik 2 (specyfikacja formatów danych)
oraz na stronie internetowej Przetargi Urzędu Marszałkowskiego Województwa Podlaskiego:
https://przetargi.wrotapodlasia.pl/pl/zamowienia_publiczne/przetargi/urzad_marszalkowski_wojewodztwa_/zamowienie_1123.html

Szczegółowy opis funkcjonalności jakie musi udostępniać System został zawarty w dalszej części dokumentu.

ROZDZIAŁ 1. Wymagania dla Systemu informatycznego w PWOMP

L.p.	Opis wymagania
1.	System zgodnie z Rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. 2017.2274 t.j.) musi spełniać zasady interoperacyjnego współdziałania na trzech poziomach: semantycznym, organizacyjnym oraz technologicznym. ▪ W zakresie procedur związanych z udostępnianiem dokumentacji medycznej oraz informacji medycznej System musi być zgodny przede wszystkim z zasadami określonymi w Ustawie z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (Dz.U. 2020.849 t.j.). ▪ Dla zapewnienia interoperacyjności Systemu na poziomie semantycznym, Systemu musi być zgodny z wymogami Ustawy z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia (Dz.U. 2021.666 t.j.), umożliwiać tworzenie elektronicznych dokumentów medycznych wg struktur danych określonych przez CEZ (Reguły biznesowe i walidacyjne określające strukturę dokumentów medycznych), udostępnianie informacji o zdarzeniach medycznych do Systemu Informacji Medycznej wg zasad określonych w Rozporządzeniu Ministra Zdrowia z 28 marca 2013 r. w sprawie wymagań dla Systemu Informacji Medycznej oraz dokumencie CEZ pt. Model transportowy danych o Zdarzeniach Medycznych oraz Indeksie Elektronicznej Dokumentacji Medycznej gromadzonych w systemie P1. Interoperacyjność semantyczna musi zostać spełniona również poprzez zapewnienie, że dane medyczne gromadzone w rejestrze świadczeń opieki zdrowotnej będą gromadzone i opisywane wg zasad określonych w Rozporządzeniu Ministra Zdrowia z dnia 20 czerwca 2008 r. w sprawie zakresu niezbędnych informacji gromadzonych przez świadczeniodawców, szczegółowego sposobu rejestrowania tych informacji oraz ich przekazywania podmiotom zobowiązanym do finansowania świadczeń ze środków publicznych. ▪ Dla zapewniania interoperacyjności Systemu na poziomie technologicznym musi umożliwiać wymianę danych z innymi systemami teleinformatycznymi, usługodawcami za pomocą zdefiniowanych przez CEZ protokołów komunikacyjnych i szyfrujących.
2.	System musi być zgodny z normami dotyczącymi służby zdrowia: ▪ ISO/IEC 27002 – norma określająca wytyczne związane z ustanowieniem, wdrożeniem, eksploatacją, monitorowaniem, przeglądem, utrzymaniem i doskonaleniem Systemu Zarządzania Bezpieczeństwem Informacji ▪ PN-ISO/IEC 20000-1:2007 „Technika informatyczna - Zarządzanie usługami - Część 1: Specyfikacja", ▪ PN-ISO/IEC 20000-2:2007 „Technika informatyczna - Zarządzanie usługami - Część 2: Reguły postępowania, ▪ PN ISO/IEC 27001:2007 „Technika informatyczna - Techniki bezpieczeństwa - Systemy zarządzania bezpieczeństwem informacji - Wymagania"
3.	System musi posiadać interfejsy pozwalające na łatwe dołączanie do niego kolejnych podmiotów i platform teleinformatycznych niezależnie od ich producenta.
4.	Wdrożone rozwiązanie będzie posiadało zestaw polis, praktyk i bibliotek, które pozwalają wykorzystać funkcjonalność aplikacji w taki sposób, by można było z niej korzystać jako z zestawu usług, opublikowanych tak, by poziom szczegółowości był dostosowany do potrzeb konsumenta usługi. Publikowane elementy będą niezależne od implementacji i stosować będą pojedynczy, standardowy interfejs.
5.	System musi być przystosowany do uruchomienia na platformie wirtualizacyjnej lub w chmurze prywatnej.
6.	Systemu musi umożliwiać tworzenie, archiwizowanie oraz udostępnianie elektronicznej dokumentacji medycznej, zwłaszcza elektronicznych recept, skierowań, zleceń oraz informacji o zdarzeniach medycznych wg zasad określonych w ustawie o z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia (Dz.U. 2021.666 t.j..)
7.	System musi umożliwiać integrację z platformami P1 i P2. Oznacza to, że system HIS musi umożliwiać tworzenie elektronicznych dokumentów medycznych oraz prowadzenie rejestru świadczeń opieki zdrowotnej, o którym mowa w Rozporządzeniu Ministra Zdrowia z dnia 20 czerwca 2008 r. w sprawie zakresu niezbędnych informacji gromadzonych przez świadczeniodawców, szczegółowego sposobu rejestrowania tych informacji oraz ich przekazywania podmiotom zobowiązanym do finansowania świadczeń ze środków publicznych według standardów i zgodnie z formatami określonymi w Rozporządzeniu Ministra Zdrowia z 28 marca 2013 r. w sprawie wymagań dla Systemu Informacji Medycznej oraz dokumentach

L.p.	Opis wymagania
	opublikowanych przez Centrum e-Zdrowia.
8.	System ma umożliwiać przesyłanie do P1 informacji o trzech obszarach: ▪ informacja o zdarzeniu medycznym, tzw. ExtPLHealthcareEvent ▪ indeksy dokumentów medycznych wytworzonych w ramach tego zdarzenia, tzw. XDSDocumentEntry ▪ informacja o bieżącym komunikacie, tzw. XDSSubmissionSet,
9.	System musi mieć możliwość pracy użytkowej przez 24 godziny na dobę, 7 dni w tygodniu, 365 dni w roku.
10.	Wszystkie udostępniane w systemie funkcjonalności użytkownika muszą być w języku polskim.
11.	System musi działać w architekturze trójwarstwowej, w której przetwarzanie danych, składowanie danych oraz interfejs użytkownika realizowane jest przez osobne moduły.
12.	Wdrażany system musi posiadać wyodrębnione i odseparowane od siebie środowisko produkcyjne i środowisko testowo-szkoleniowe. Środowisko produkcyjne przeznaczone do eksploatacji produkcyjnej usług Systemu, a środowisko testowo-szkoleniowe dla prowadzenia testów poprawek programowych oprogramowania przed jego instalacją w środowisku produkcyjnym, oraz do prowadzenia szkoleń Użytkowników systemu.
13.	System musi zostać dostarczony wraz z pełnym zestawem instalacyjnym oprogramowania obejmujący wszystkie niezbędne komponenty do prawidłowej pracy Systemu (w tym katalogi aplikacji, środowisko uruchomieniowe, czcionki, skróty itd.; dotyczy to również wszystkich ewentualnych wtyczek i rozszerzeń niezbędnych do prawidłowej pracy Systemu, jeżeli aplikacja działa przez przeglądarkę WWW).
14.	System musi posiadać mechanizmy umożliwiające przeprowadzenie centralnej aktualizacji oprogramowania zarówno w środowisku produkcyjnym jak i testowo-szkoleniowym bez konieczności ręcznej aktualizacji na każdej stacji roboczej z osobna.
15.	System musi być zintegrowany pod względem przepływu informacji tj. wymaga się spójnej bazy danych w taki sposób, że informacja raz wprowadzona do Systemu, niezależnie od źródła, będzie dostępna w odpowiednich jego funkcjach i nie wymagać będzie ponownego wprowadzania do wdrażanego Systemu i pozostałych systemów wdrożonych w PWOMP Nie narzuca się konstrukcji systemu, dopuszcza zarówno integrację z lokalną i regionalną warstwą integracyjną PWOMP jak i pracę na jednej bazie danych zależnie od rozwiązania oferowanego przez Wykonawcę. Wykonawca dostarczy niezbędne licencje oprogramowania bazy danych.
16.	System musi działać i udostępniać wszystkie wymagane funkcjonalności na infrastrukturze sprzętowej przeznaczonej na potrzebę budowy Systemu.
17.	System musi posiadać architekturę umożliwiającą dalszą jego rozbudowę.
18.	System musi posiadać narzędzia umożliwiające sprawne zarządzanie personelem, prowadzenie terminarza wizyt, możliwości zarezerwowania wizyty lekarskiej poprzez dostęp do Internetu.
19.	System musi posiadać moduł powiadomień elektronicznych umożliwiających przypominanie o umówionej wizycie lub poradzie.
20.	System musi posiadać narzędzia umożliwiające gromadzenie danych o planowanych i odbytych wizytach.
21.	System musi posiadać narzędzia umożliwiające gromadzenie danych o pacjentach, zrealizowanych usługach, zaleceniach, wydanych skierowaniach i receptach.
22.	System musi posiadać narzędzia umożliwiające tworzenie raportów o odbytych wizytach i zrealizowanych usługach medycznych dla pacjentów.
23.	System musi posiadać narzędzia umożliwiające pacjentom rezerwację wizyty poprzez Internet.
24.	System musi posiadać możliwość przesłania przez pacjenta dokumentacji medycznej drogą elektroniczną.
25.	System musi posiadać narzędzia umożliwiające wgląd lekarzom do elektronicznej historii choroby pacjenta, a także pozwalającą na rezerwację wizyt bezpośrednio przez lekarza.
26.	System powinien umożliwiać posługiwanie się dwoma oznaczeniami: ▪ czasu i daty zaistnienia zdarzenia (kiedy ono miało fizycznie miejsce), ▪ daty i czasu wprowadzenia informacji do Systemu.
27.	System musi umożliwiać eksport całości dokumentacji do formatu XML i PDF. System musi posiadać mechanizmy eksportu całości dokumentacji z jednego widoku, jak również wybranych pacjentów, wg kryteriów wyszukiwania.
28.	System musi posiadać możliwość zdalnego połączenia się przez uprawnionych użytkowników z każdym komputerem pracującym w ramach Systemu.
29.	System musi posiadać mechanizmy umożliwiające użycie bezpiecznego podpisu elektronicznego weryfikowanego przy pomocy ważnego kwalifikowanego certyfikatu w rozumieniu ustawy z dnia 18 września 2001 r. o podpisie elektronicznym lub podpisu potwierdzonego profilem zaufanym ePUAP w rozumieniu ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne. Powyższe dotyczy:

L.p.	Opis wymagania
	▪ elektronicznej dokumentacji medycznej; ▪ elektronicznej dokumentacji medycznej lub danych z tych dokumentów, w zakresie niezbędnym do wykonywania badań diagnostycznych, zapewnienia ciągłości leczenia oraz zaopatrzenia usługobiorców w produkty lecznicze, środki spożywcze specjalnego przeznaczenia żywieniowego i wyroby medyczne; ▪ wniosku o dostęp do danych przetwarzanych w SIM umożliwiających wymianę między usługodawcami danych zawartych w elektronicznej dokumentacji medycznej. Dostawa podpisów kwalifikowanych nie stanowi przedmiotu zamówienia.
30.	Logowanie osoby personelu medycznego do podsystemu e-usług musi odbywać się z wykorzystaniem parametrów logowania (loginu i hasła) tych samych, którymi osoba posługuje się logując do podsystemu obsługi pacjenta i obiegu dokumentacji medycznej.

5. Wymagania bazy danych

L.p.	Opis wymagania
Wymagania bazy danych	
1.	Dostarczone oprogramowanie bazy danych musi mieć możliwość współpracy bazy danych z różnymi platformami sprzętowymi oraz 64-bitowymi systemami operacyjnymi (m.in.: MS Windows, Unix, Linux).
2.	Dostarczone oprogramowanie bazy danych musi mieć następujące cechy: transakcyjna i relacyjna, wyposażona w zintegrowany system zarządzania (RDBMS).
3.	Dostarczone oprogramowanie bazy danych musi zapewniać użycie pól typu XML łącznie z kontrolą poprawności i użyciem zapytań.
4.	Dostarczone oprogramowanie bazy danych musi mieć możliwość synchronicznej i asynchronicznej replikacji danych w co najmniej dwóch niezależnych centrach danych.
5.	Musi istnieć możliwość wykonywania niektórych operacji związanych z utrzymaniem bazy danych bez konieczności pozbawienia dostępu użytkowników do danych. W szczególności dotyczy to tworzenia/przebudowywania indeksów oraz procesu backupu.
6.	Dostarczone oprogramowanie bazy danych musi posiadać mechanizm wyzwalaczy (triggers) i procedur wbudowanych (stored procedures). Mechanizm wyzwalaczy (triggers) musi uwzględniać możliwość ich uruchomienia dla każdego wiersza (each row) lub całości polecenia (statement). Mechanizm wyzwalaczy (triggers) musi uwzględniać możliwość ich uruchomienia przed lub po zdarzeniu (obsługiwane zdarzenia min. insert, update, delete).
7.	Musi istnieć możliwość zapewnienia schematu blokowania (lock) tabel na poziomie wierszy.
8.	Oprogramowanie musi zapewnić mechanizmy zachowywania więzów integralności danych z kaskadowym usuwaniem i modyfikacją rekordów.
9.	Musi istnieć możliwość tworzenia i realizacji polityk (harmonogram, parametry) wykonywania czynności administracyjnych (backup, reorganizacja tabel/indeksów, statystyki)
10.	Dostarczone oprogramowanie bazy danych musi umożliwiać generowanie kopii bezpieczeństwa automatycznie (o określonej porze) i na żądanie operatora oraz umożliwiać odtwarzanie bazy danych z kopii archiwalnej, w tym sprzed awarii.
11.	Dostarczone oprogramowanie bazy danych musi umożliwiać eksport i import danych z bazy danych w formacie tekstowym z uwzględnieniem polskiego standardu znaków.
12.	Dostarczone oprogramowanie bazy danych musi monitorować i zapisywać w logach serwera wszystkie zmiany dokonywane z dowolnego poziomu.
13.	Dostarczone oprogramowanie bazy danych musi zapewniać natywne wersjonowanie rekordów tabel.
14.	Dostarczone oprogramowanie bazy danych musi zapewniać kodowanie natywne plików bazy i backupów.
15.	Dostarczone oprogramowanie bazy danych musi zapewnić natywną kompresję danych, indeksów, backupu.
16.	Dostarczone oprogramowanie bazy danych musi zapewnić integralność danych, a w szczególności: • integralność danych i transakcji na poziomie bazy danych i aplikacji, • efektywny i bezbłędny dostęp użytkowników i procesów do wspólnych danych, • bieżącą kontrolę poprawności wprowadzanych danych.
17.	Dostarczone oprogramowanie bazy danych musi mieć możliwość pracy w dowolnym środowisku zwirtualizowanym, w szczególności opartym na VMware, Hyper-V lub VirtualBox.

L.p.	Opis wymagania
18.	Dostarczone oprogramowanie bazy danych musi zapewniać możliwość definiowania tabel jako zorganizowanych wg wierszy, kolumn lub wierszy/kolumn.
19.	Dostarczone oprogramowanie bazy danych nie może być związane z konkretnym sprzętem (OEM).
20.	Licencja bazy danych nie powinna być specyficzna tylko dla aplikacji, ma być otwarta. Licencja musi być na nieograniczoną liczbę użytkowników oraz na nieograniczoną liczbę połączeń do bazy danych.
21.	Nie dopuszcza się zastosowania oprogramowania bazy danych typu open-source. Dopuszcza się dostarczenie bezpłatnej wersji oprogramowania bazodanowego posiadającego wszystkie cechy i właściwości zdefiniowane w niniejszej tabeli.

6. Wymagania szczegółowe dla Systemu - rejestry i e-usługi

L.p.	Opis wymagania
Wymagania ogólne dla rejestrów i e-usług	
1.	System umożliwia prowadzenie publicznego Rejestru lekarzy uprawnionych do przeprowadzania badań profilaktycznych pracowników.
2.	System umożliwia prowadzenie publicznego Rejestru podjęcia oraz zakończenia działalności podmiotu leczniczego i indywidualnej praktyki lekarskiej sprawujących profilaktyczną opiekę zdrowotną nad pracującymi.
3.	System umożliwia prowadzenie publicznego Rejestru zgłoszeń podjęcia i zakończenia działalności psychologa w zakresie profilaktycznej opieki zdrowotnej nad pracującymi.
4.	System umożliwia prowadzenie publicznego rejestru - Ewidencji podmiotów leczniczych, które zawarły umowę z Zamawiającym na badania profilaktyczne uczniów/studentów/słuchaczy.
5.	System umożliwia udostępnienie zasobów cyfrowych czterech ww. rejestrów publicznych w celu ich ponownego wykorzystania przez inne podmioty za pomocą własnych serwisów WWW.
6.	System udostępnia dane z rejestrów, dane te będą udostępnione za pośrednictwem przeglądarki internetowej.
7.	System umożliwia skorzystanie z trzech e-usług: e-informacja, e-wniosek, e-wizyta.
8.	Dostęp do e-usług: e-informacja, e-wniosek, e-wizyta jest możliwy z poziomu Portalu Pacjenta (e-Platforma)
9.	Dostęp do e-usług możliwy jest za pomocą Portalu Pacjenta (e-Platforma) po zalogowaniu się poprzez podanie loginu i hasła.
10.	Dostęp do usług: e-informacja, e-wniosek, e-wizyta jest możliwy na urządzeniach mobilnych (komputer przenośny, smartfon, tablet).
Usługa e-Informacja	
11.	System udostępnia dane z rejestrów za pośrednictwem usługi e-Informacja, dostępnej z poziomu przeglądarki internetowej.
12.	Usługa jest dostępna dla osób posiadających konto w Portalu Użytkowników zalogowanych do tego portalu.
13.	Usługa umożliwi osobom podlegającym badaniom lekarskim dopuszczającym do pracy lub podjęcia nauki i pracy znalezienie miejsca, gdzie można przeprowadzić badanie.
14.	Osoba posiadająca konto w portalu po wpisaniu swoich danych, w tym miejsca zamieszkania, otrzyma dostęp do listy podmiotów, które przeprowadzają badania.
15.	Pracodawca oraz pracownik po wprowadzeniu danych dotyczących miejsca zamieszkania lub pracy ma możliwość zapoznania się z listą adresowa najbliżej położonych podmiotów leczniczych wyspecjalizowanych w medycynie pracy.
16.	Lista będzie uporządkowana według trafności miejsca zamieszkania.
17.	Informacja o zarejestrowanych przez Zamawiającego podmiotach wyspecjalizowanych w zakresie medycyny pracy będą również udostępniane za pomocą interfejsu API, w celu ich ponownego wykorzystania przez inne instytucje.
18.	Dane z rejestrów są możliwe do pozyskania na poziomie umożliwiającym pobranie tych danych w postaci ustrukturalizowanej oraz w edytowalnym formacie (*.xls lub *.csv)
19.	Dane z rejestrów są możliwe do pozyskania na poziomie umożliwiającym ich linkowanie w dowolnych serwisach w sieci Internet (system udostępnia źródło danych, możliwe jest automatyczne importowanie danych do innych serwisów).
Usługa e-Wniosek	
20.	Usługa umożliwia podmiotom podlegającym wpisowi do rejestru (Rejestr lekarzy uprawnionych do przeprowadzania badań profilaktycznych pracowników, Rejestr podjęcia oraz zakończenia

L.p.	Opis wymagania
	działalności podmiotu leczniczego i indywidualnej praktyki lekarskiej sprawujących profilaktyczną opiekę zdrowotną nad pracującymi, Rejestr zgłoszeń podjęcia i zakończenia działalności psychologa w zakresie profilaktycznej opieki zdrowotnej nad pracującymi, Ewidencja podmiotów leczniczych, które zawarły umowę z Zamawiającym na badania profilaktyczne uczniów/studentów/słuchaczy), tj. lekarzom, psychologom, podmiotom leczniczym i praktykom lekarskim złożenie wniosku o wpis do rejestru.
21.	Usługa umożliwia przedsiębiorcom przeprowadzenie kompletnej procedury rejestracji, tj. wypełnienie i złożenie wniosku elektronicznego i zweryfikowanie jego poprawności.
22.	Usługa umożliwia przedsiębiorcom załączenie do wniosku o rejestrację skanów dokumentów źródłowych (np. prawo wykonywania zawodu lekarza, dyplom potwierdzający uzyskanie przez lekarza specjalizacji w dziedzinie medycyny pracy, dyplom ukończenia uczelni medycznej, zaświadczenie o dodatkowych uprawnieniach).
23.	Usługa umożliwia podpisanie przez przedsiębiorcę wniosku podpisem elektronicznym.
24.	W przypadku gdy osoby uprawnione do złożenia wniosku posiadać będą kwalifikowany podpis elektroniczny lub profil zaufany ePUAP usługa umożliwi formalne złożenie wniosku wraz z załącznikami stanowiącymi dokumenty źródłowe (np. prawo wykonywania zawodu lekarza, dyplom potwierdzający uzyskanie przez lekarza specjalizacji w dziedzinie medycyny pracy, dyplom ukończenia uczelni medycznej, zaświadczenie o dodatkowych uprawnieniach).
25.	W przypadku gdy osoba uprawniona nie posiada kwalifikowanego podpisu elektronicznego lub profilu zaufanego ePUAP usługa umożliwia wstępną rejestrację (wprowadzenie danych do systemu informatycznego wymaganych prawem oraz załączenie skanów dokumentów źródłowych), a następnie wygenerowanie formularza papierowego wniosku.
26.	W przypadku gdy osoba uprawniona nie posiada kwalifikowanego podpisu elektronicznego system umożliwi wnioskodawcy umówienie się na spotkanie w siedzibie Zamawiającego za pośrednictwem usługi e-wizyta (w celu złożenia wniosku w postaci papierowej podpisanego odręcznie oraz przestawienia do wglądu oryginałów dokumentów źródłowych).
27.	Usługa umożliwia Zamawiającemu wygenerowanie decyzji o wpisie do rejestru do wnioskodawcy w postaci papierowej.
28.	Usługa umożliwia Zamawiającemu wygenerowanie decyzji o wpisie do rejestru do wnioskodawcy w postaci dokumentu opatrzonego podpisem elektronicznym.
29.	Usługa umożliwia odebranie przez przedsiębiorcę zaświadczenia o wpisie do rejestru w formie dokumentu podpisanego podpisem elektronicznym.
30.	Usługa umożliwia utworzenie dla wnioskodawcy profilu użytkownika w Portalu Pacjenta (e-Platformie) przez nadanie wnioskodawcy loginu i hasła oraz nadanie uprawnień pozwalających na korzystanie z usług e-wizyta i e-Informacja.
Usługa e-Wizyta	
31.	Usługa umożliwia złożenie wniosku o rejestrację w przypadku, gdy osoba uprawniona do podpisu wniosku, nie zdecyduje się na użycie kwalifikowanego podpisu elektronicznego lub profilu zaufanego ePUAP.
32.	Przedsiębiorcy starający się o wpis do rejestrów (lekarze, psycholodzy, podmioty lecznicze, praktyki lekarskie) mogą za pośrednictwem usługi e-wizyta umówić się na spotkanie z pracownikami Zamawiającego w celu omówienia zasad i warunków związanych z procesem rejestracji lub aktualizacji danych w rejestrze.
33.	Przedsiębiorcy starający się o wpis do rejestrów (lekarze, psycholodzy, podmioty lecznicze, praktyki lekarskie) mogą za pośrednictwem usługi e-wizyta umówić się na spotkanie z pracownikami Zamawiającego w celu dokończenia rozpoczętego za pomocą usługi e-Wniosek procesu rejestracji (dostarczenie wniosku w postaci papierowej wraz z dokumentami źródłowymi, np. prawo wykonywania zawodu lekarza, dyplom potwierdzający uzyskanie przez lekarza specjalizacji w dziedzinie medycyny pracy, dyplom ukończenia uczelni medycznej, zaświadczenie o dodatkowych uprawnieniach).
Wymagania dla Rejestru zgłoszeń podjęcia i zakończenia działalności podmiotu leczniczego i indywidualnej praktyki lekarskiej sprawujących profilaktyczną opiekę zdrowotną nad pracującymi, Rejestru zgłoszeń podjęcia i zakończenia działalności psychologa w zakresie profilaktycznej opieki zdrowotnej nad pracującymi, Ewidencji podmiotów leczniczych, które zawarły umowę z Zamawiającym na badania profilaktyczne uczniów/studentów/słuchaczy	
34.	Rejestr zgłoszeń podjęcia i zakończenia działalności umożliwia dodanie/edycję danych opisujących jednostkę: nazwa, dane adresowe, dane kontaktowe, kod resortowy, REGON, typ świadczeniodawcy, data rozpoczęcia i zakończenia działalności, kod działalności SMP, rodzaj placówki (NZOZ, PZOZ, PPL, GP, GPL, ZPCh), organ tworzący, kod świadczeniodawcy, nr Księgi Rejestrowej OIL lub Wojewody
35.	Rejestr umożliwia wybór jednostki poprzez wyszukanie jednostki wg: nazwy, miasta, kodu pocztowego, powiatów
36.	Rejestr umożliwia wybór jednostki poprzez filtrowanie wyświetlanej listy jednostek z użyciem filtrów: Rodzaj placówki, Powiat, Miasto, Kod pocztowy, Ulica.
37.	Rejestr dla wskazanej jednostki umożliwia przyporządkowanie zatrudnionego personelu z

L.p.	Opis wymagania
	zachowaniem informacji: telefon kontaktowy pracownika, data rozpoczęcia działalności, data zakończenia działalności, data wpłynięcia zgłoszenia, kwalifikacji, dodatkowych przeszkoleń, wieku, wzoru pieczęci.
38.	Wyświetlana lista personelu danej jednostki może zostać zawężona z wykorzystaniem filtra „personel aktualny/archiwalny" oraz możliwością wyszukania po fragmencie nazwiska.
39.	Rejestr umożliwia wywołanie okna Rejestru uprawnionych do przeprowadzania badań profilaktycznych w celu dodania/edycji informacji o pracownikach uprawnionych do wykonywania takich badań.
40.	Dla wskazanej placówki, okno Rejestru zgłoszeń umożliwia bezpośrednio przejście do funkcjonalności zaplanowania kontroli placówki, księgi kontroli, harmonogramu.
Wymagania dla Rejestru uprawnionych do przeprowadzania badań profilaktycznych pracowników	
41.	Rejestr uprawnionych do przeprowadzania badań profilaktycznych pracowników umożliwia przechowywanie (dodawanie/edycję) danych o osobach uprawnionych do przeprowadzania badań profilaktycznych.
42.	Rejestr umożliwia dodanie personelu z zachowaniem informacji o pracowniku: rodzaj pracownika (pracownik placówki, pracownik zewnętrzny, osoba niezatrudniona, stażysta, pracownik MP), nazwisko, imię, drugie imię, tytuł naukowy, PESEL, nr prawa wykonywania zawodu, tytuł zawodowy, data urodzenia, telefon, mail, ich stopnie i lata ich uzyskania, dane adresowe, znane języki obce, nazwa praktyki lub NIP (jeśli dotyczy), stopień specjalizacji, dodatkowe przeszkolenia, wzór pieczęci.
43.	Rejestr umożliwia wyświetlenie listy osób uprawnionych do przeprowadzania badań profilaktycznych z możliwością wyszukania.
44.	Rejestr umożliwia wyświetlenie listy osób uprawnionych do przeprowadzania badań profilaktycznych z możliwością zawężenia listy do lekarzy z przyporządkowaniem/bez przyporządkowania numeru księgi.
45.	Rejestr umożliwia wyświetlenie listy osób uprawnionych do przeprowadzania badań profilaktycznych z możliwością zawężenia listy z wykorzystaniem filtrów: organ tworzący, miasto, powiat, rok urodzenia, nr księgi, zawód, specjalizacja, stopień specjalizacji, status (aktywny/nieaktywny/spoza województwa), data wpisu do rejestru (od-do), data rozpoczęcia działalności (od-do), data zakończenia działalności (od-do), dodatkowe przeszkolenia.
46.	Dla pracownika już dodanego, wpisanego do Rejestru możliwe jest wprowadzanie/edytowanie informacji: data wpisu, status (aktywny/nieaktywny/spoza województwa), data wydruku potwierdzenia, podstawa wpisu (dla pielęgniarek).
47.	Dla pracownika już dodanego, wpisanego do Rejestru możliwe jest wprowadzanie/edytowanie informacji: uprawnienia, miejsca pracy, inne uwagi.
48.	Dla wskazanej osoby Rejestr prezentuje na tym samym ekranie listę jednostek, do których przypisana jest ta osoba.
49.	Lista jednostek, do których przypisana jest dana osoba, może być zawężona do wybranej jednostki lub do grupy jednostek o statusie aktywny/nieaktywny.
50.	Dla wskazanej osoby Rejestr umożliwia wysłanie dowolnej wiadomości SMS-em i mailem.
51.	Dla wskazanej osoby Rejestr umożliwia zapisanie informacji o zaświadczeniach i orzeczeniach wymaganych dla utworzenia sprawozdania MZ-35A.
52.	Walidacja zatrudnienia w Rejestrze zgłoszeń podjęcia i zakończenia działalności oraz Rejestrze uprawnionych do przeprowadzenia badań profilaktycznych - użytkownik ma możliwość zatrudnienia tego samego pracownika w danej jednostce wyłącznie w przypadku, gdy została wprowadzona data zakończenia działalności.
53.	W oknie edycji danych pracownika system pozwala np. dla lekarzy na wprowadzenie specjalizacji w ramach Medycyny Pracy poprzez wybranie odpowiedniej z wcześniej zdefiniowanych specjalizacji. Dodatkowo, z rozwijanej listy system daje możliwość wprowadzenia stopnia specjalizacji a w osobnym polu daty ukończenia kursu.
54.	Dla zgłoszonych do Rejestru uprawnionych do przeprowadzania badań profilaktycznych lekarzy Medycyny Pracy system pozwala na prowadzenie automatycznej numeracji księgi wraz z możliwością odnotowania daty wpisu do księgi, wydania potwierdzenia oraz wydruku pieczątki, dodatkowych przeszkoleń niezbędnych do badań z uwagi na warunki pracy (promieniowanie jonizujące, wykonujących prace w warunkach tropikalnych, morskich i podwodnych oraz pracowników wyjeżdżających do pracy lub powracających z pracy z warunków tropikalnych, wykonujących prace na stanowiskach związanych z bezpieczeństwem ruchu kolejowego
55.	System umożliwia wysłanie bezpośrednio z okna Rejestru Uprawnionych Do Przeprowadzania Badań Profilaktycznych wiadomości za pomocą poczty elektronicznej lub wiadomości SMS osobie uprawnionej, jeśli zostały podane namiary na konto e-mail i/lub telefon komórkowy.

7. Wymagania funkcjonalne i niefunkcjonalne

L.p.	Opis wymagania
Wymagania integracji z PSIEZ	
56.	System musi zapewniać integrację i spójność danych z Podlaskim Systemem Informacyjnym e-Zdrowie, w zakresie: a. Regionalnego Repozytorium Dokumentacji Medycznej; b. Regionalnego Systemu typu Business Intelligence (BI) z Hurtownią Danych c. Portalu Pacjenta; d. Portalu Menadżerskiego e. Regionalnego Systemu Rejestrów; f. Regionalnej Warstwy Integracyjnej.
57.	Integracja z Podlaskim Systemem Informacyjnym e-Zdrowie musi być realizowana zgodnie z zapisami Specyfikacji Wymiany Danych wraz z załącznikami w wersji 9.1. Dostarczona rozbudowa systemu posiadanego musi spełniać zapisany w niniejszym dokumencie wymagania.
58.	System mu być zintegrowany bezpośrednio za pomocą Regionalnej Warstwy Integracyjnej (RWI) posiadanej już przez PWOM. Regionalna Warstwa Integracyjna jest mechanizmem integracyjnym umożliwiającym pozyskanie danych z podmiotów leczniczych. System zapewnia efektywne pozyskanie elektronicznej dokumentacji medycznej z lokalnych EDM oraz zagregowanych danych transakcyjnych z Lokalnych HD przez lokalne warstwy integracyjne. Rozwiązanie to jest wykorzystywane do transferu danych pomiędzy systemami UMWP (BI/HD oraz Regionalnym Repozytorium Dokumentacji Medycznej) i systemami portalowymi.
59.	System musi korzystać bezpośrednio z Regionalnego Systemu Rejestrów (RSR), który jest systemem rejestrów udostępniającym kluczowe rejestry i dane słownikowe wszystkim pozostałym systemom regionalnym i lokalnym. Dane bazy danych Regionalnego Systemu Rejestrów są udostępniane jedynie uprawnionym osobom.
60.	System musi być zintegrowany z lokalną warstwą integracyjną czyli z mechanizmami integracyjnymi zastosowanymi na poziomie lokalnym służące do wymiany danych pomiędzy systemami w PWOMP i poza nim. System ten zapewnia wymianę danych z jednostką regionalną oraz udostępnienie usługi rejestracji w ramach Portalu Pacjenta projektu PSIeZ.
Funkcjonalności administratora	
61.	Możliwość automatycznej, centralnej aktualizacji aplikacji.
62.	Zabezpieczenie dostępu do programu dla użytkowników, hasło lub logowanie biometryczne lub przez kartę.
63.	Wymuszona okresowa zmiana hasła.
64.	Wbudowane mechanizmy do administrowania prawami użytkowników; zarządzanie uprawnieniami, tworzenie i modyfikacja grup, określanie uprawnień użytkowników na poziomie poszczególnych funkcji.
65.	Możliwość zarządzania użytkownikami, ich prawami, dostępem do komórek organizacyjnych.
66.	Możliwość przydzielania użytkownikom prawa dostępu do wybranych komórek organizacyjnych (np. oddziału).
67.	Administrowanie bazami słownikowymi.
68.	Definicja struktury placówki danych administracyjnych w tym kodów resortowych MZ, REGON.
69.	Możliwość zaewidencjonowania w programie i modyfikacji poszczególnych jednostek organizacyjnych zakładu (gabinety, rejestracje, izby przyjęć, oddziały, laboratoria, pracownie diagnostyczne, itd.).
70.	Możliwość założenia kalendarza dni wolnych dla całej jednostki, pojedynczej jednostki organizacyjnej lub lekarzy.
71.	Definicja kontraktów i usług.
72.	Obsługa słowników personelu z możliwością połączenia z zarządzaniem listą użytkowników.
73.	Wykorzystanie słowników zarówno standardowych (ICD-10, ICD-9 CM, Słownik Kodów Terytorialnych GUS, słownik trybów przyjęcia, słownik płatników i instytucji zewnętrznych itp.), jak i wewnątrzzakładowych, jak, np. ostrzeżeń o wykorzystaniu danego produktu w jednostce w określonym czasie, itp. oraz wykaz leków refundowanych.
74.	Definicja i obsługa ksiąg wykorzystywanych w zakładzie (księga główna, księga odmów, księgi oddziałowe, księga oczekujących itp.).
75.	System medyczny musi być zintegrowany z posiadanym systemem RIS/PACS min. w zakresie przesyłania i odbioru wyników opisowych badań, w tym możliwość otwierania wyników obrazowych w formacie DICOM.
76.	Obsługa systemu e-WUŚ - konfiguracja umożliwiająca co najmniej dwukrotną weryfikację uprawnień pacjentów "hurtowo" o ustalonych, zapisanych w harmonogramie godzinach.

L.p.	Opis wymagania
77.	Możliwość konfiguracji obsługi wielu podmiotów gospodarczych w ramach grupy zakładów.
78.	Możliwość scalania kartotek pacjenta.
79.	System umożliwia automatyczne przypisanie procedur ICD9 po otrzymaniu wyniku badania laboratoryjnego za pomocą HL7.
80.	System umożliwia automatyczne dodawanie procedur po ręcznym wpisaniu wyniku badania.
81.	System musi być zintegrowany z platformą P1 i P2 w wymaganych prawnie terminach.
Funkcjonalności obszaru rejestracji do poradni	
82.	Tworzenie grafików pracy lekarzy na konkretne dni i godziny z podziałem co 15 minut (daty kalendarzowe).
83.	Planowanie lub zapisywanie wizyty wg planu pracy poradni.
84.	Przyjmowanie pacjentów niezależnie od planu pracy.
85.	Przyjmowanie pacjentów poza limitem z dnia.
86.	Musi istnieć możliwość tworzenia blokad grafików dla poradni lub lekarzy określając zakres dat oraz godzinowy.
87.	Możliwość zarejestrowania pacjenta z rozróżnieniem płatnika za konkretną usługą (NFZ, wizyta prywatna, wizyta abonamentowa).
88.	Możliwość rozróżnień kolorystycznych dla planu pracy poradni w zależności od płatnika.
89.	Możliwość kolorystycznego wyróżnienia na kalendarzu pracy przychodni dni, w których zamieszczony został wewnętrzny komunikat dotyczący danego dnia.
90.	Graficzne przedstawienie na kalendarzu przyjęć dnia, w którym brak już wolnych terminów.
91.	Graficzne przedstawieniu na kalendarzu przyjęć dnia, w którym zostali już zarejestrowani pacjenci.
92.	System pozwala sprawdzić w systemie e-WUŚ status ubezpieczenia nowo zarejestrowanego pacjenta.
93.	Możliwość wydrukowania z systemu: ▪ listy pacjentów zarejestrowanych na dany dzień, ▪ koperty na historię choroby, ▪ kartoteki historii choroby, ▪ oświadczenia o posiadaniu ubezpieczenia.
94.	Możliwość kopiowania odbytych wizyt.
95.	Możliwość przypisania wydruków własnych do rejestracji.
96.	Kopiowanie stworzonych grafików na wybrane dni.
97.	Określenie dnia, zakresu godzinowego, średniego czasu wizyty, typu wizyty podczas definiowania bloku z grafikiem.
98.	Tworzenie blokad grafików dla poradni lub lekarzy określając zakres datowy oraz godzinowy
99.	Przeglądanie grafików z wizytami pacjentów w rejestracji dla poszczególnych filii, poradni, lekarzy, rodzaju bloków z grafikami.
100.	Wyświetlanie ilości wolnych terminów wizyt na grafikach.
101.	Wyświetlanie grafików z pierwszym wolnym terminem w danej poradni.
102.	Możliwość rezerwacji wizyty na godzinę.
103.	Rejestracja wizyt o czasach nakładających się na siebie.
104.	Możliwość automatycznego dopasowania długości wizyty do godzin pracy lekarza przy zmianie terminu i lekarza.
105.	Możliwość odwoływania wizyt.
106.	Możliwość zmiany terminu wizyty bez konieczności odwoływania.
107.	Możliwość potwierdzania faktu pojawienia się pacjenta w rejestracji przed wizytą w gabinecie lekarskim. Do czasu potwierdzenia pacjent jest niedostępny w module Gabinet.
108.	Możliwość określenia płatnika oraz: • wprowadzenia uwag, • wydłużenia czasu trwania wizyty podczas rezerwacji terminu.
109.	Możliwość edycji płatnika, uwag po zarezerwowaniu terminu wizyty. Wprowadzone uwagi podczas rejestracji dostępne są w gabinecie lekarskim na liście wizyt.
110.	Automatyczne sprawdzanie prawidłowości powiązań pomiędzy Ubezpieczycielem i Płatnikiem.
111.	Automatyczna podpowiedź listy Płatników po wyborze prywatnego Ubezpieczyciela.
112.	Możliwość wprowadzenia danych ze skierowania oraz danych o uprawnieniach dodatkowych podczas rezerwacji terminu wizyty.
113.	Możliwość znalezienia pacjenta w bazie danych po: ▪ nazwisku, ▪ numerze kartoteki, ▪ numerze PESEL.
114.	Możliwość wprowadzenia danych osobowych pacjenta wraz z nr telefonu oraz informacji o

L.p.	Opis wymagania
	ubezpieczeniu, zakładzie pracy.
115.	Możliwość wprowadzenia informacji o dodaniu pacjenta do kolejek oczekujących w trybie stabilnym lub pilnym.
116.	Możliwość wypełnienia ankiet, dokumentów dla wybranego pacjenta.
117.	Możliwość dołączenia dokumentacji medycznej zewnętrznej pacjenta (np. w postaci skanów dokumentów).
118.	Możliwość przeglądania wizyt historycznych i zaplanowanych w zależności od statusów.
119.	Automatyczne uzupełnienie dokumentu deklaracji na podstawie danych wprowadzonych do kartoteki pacjenta.
120.	Automatyczne sprawdzanie poprawności deklaracji podczas rejestracji.
121.	Możliwość wystawienia paragonu (obsługa drukarki fiskalnej), rachunku, faktury dla pacjenta.
122.	Możliwość przeglądu cenników wizyt i badań.
123.	Możliwość przypisania pacjenta do pakietu, umowy z firmami komercyjnymi. Tylko pacjenci przypisani do danego cennika mogą z niego korzystać.
124.	System posiada wspólną Ewidencję Główną Pacjentów dla wszystkich poradni.
125.	System gromadzi w Karcie Pacjenta: ▪ dane osobowe, ▪ dane adresowe, ▪ adres e-mail, ▪ kartoteki papierowej, ▪ zatrudnienie, ▪ ubezpieczenie, ▪ płatnik, oddział NFZ.
126.	System gromadzi w Karcie Pacjenta dodatkowe dane, takie jak: ▪ wywiad rodzinny, ▪ wywiad środowiskowy, ▪ grupa krwi, ▪ dane opiekuna, ▪ upoważnienie o zgodzie do uzyskania informacji o stanie zdrowia, ▪ upoważnienie o zgodzie do uzyskania dokumentacji medycznej, ▪ rodzaj i nr dokumentu uprawniającego do leczenia, ▪ dane i uprawnienia opiekunów oraz innych osób uprawnionych do otrzymywania informacji na temat stanu pacjenta, ▪ dane osób uprawnionych do odbierania dokumentacji medycznej pacjenta, ▪ dane i uprawnienia opiekunów oraz innych osób uprawnionych do otrzymania dokumentacji pacjenta w przypadku jego śmierci.
127.	System umożliwia zapisanie w Karcie Pacjenta dodatkowych danych jak: ▪ informacja na temat szczepień, ▪ informacji na temat przebytych chorób, ▪ informacji na temat uczulenia na leki i materiały medyczne, ▪ dowolnej informacji na temat pacjenta w postaci ogólnych uwag, ▪ informacji na temat umów, polis związanych z komercyjną/prywatną wizytą.
128.	System pozwala na zapisanie w Karcie Pacjenta nr telefonu, na który będzie wysyłana informacja SMS
129.	System umożliwia odnotowanie i oznaczenie pilnych przypadków.
130.	System dopuszcza do przyjęcia pacjenta przebywającego aktualnie na oddziale, ale ostrzega i wymaga dodatkowo potwierdzenia.
131.	Możliwość wstępnego i sygnalizowanie w systemie rejestrowania pacjenta bez skierowania do jednostki wymagającej skierowań na przyszły dzień wizyty.
132.	System umożliwia wprowadzenia limitów przyjęć do poradni na: ▪ wybrany miesiąc, ▪ dowolny wybrany okres czasu.
133.	System umożliwia wprowadzenie limitu przyjęć dla lekarza: ▪ na wybrany miesiąc, ▪ na dowolny wybrany okres czasu.
134.	Możliwość skanowania dokumentów zewnętrznych do historii choroby z poziomu rejestracji.
135.	Automatyczne otwarcie okna dodania nowego pacjenta po próbie wyszukania pacjenta, który nie był wcześniej w jednostce.

L.p.	Opis wymagania
136.	Możliwość automatycznej zmiany drukowanej pieczątki jednostki w zależności od płatnika.
137.	Możliwość wydruku recept przez uprawnione do tego pielęgniarki z poziomu rejestracji.
138.	Prowadzenie Kolejki (AP-KOLCE) przeznaczonej dla świadczeniodawców do prowadzenia list oczekujących na wybrane świadczenia.
139.	Oznacza pacjentów pomyślnie wysłanych do AP-KOLCE oraz pacjentów wysłanych niepoprawnie.
Funkcjonalności obszaru gabinet	
140.	Przegląd listy zarejestrowanych do lekarza pacjentów w zależności od wybranego dnia.
141.	Możliwość przyjęcia pacjentów w innej kolejności niż wynika to z porządku rejestracji.
142.	Dostęp do archiwalnych przyjęć pacjentów.
143.	Funkcjonalność umożliwiająca odczytanie przez lekarza uwag od rejestracji na temat pacjenta.
144.	Możliwość podglądu przez lekarza indywidualnych statystyk z poziomu okna gabinetu lekarskiego.
145.	Możliwość wydruku historii choroby pojedynczo (jednej wizyty) lub zbiorczo dla pacjenta (wszystkie wizyty).
146.	Program umożliwia zdefiniowanie wydruków własnych.
147.	Dostęp do wyników badań pacjenta z poziomu okna gabinetu lekarskiego.
148.	Możliwość podglądu historii wizyt pacjenta w placówce.
149.	Możliwość wykonania badania podmiotowego (wywiadu) na podstawie zdefiniowanych wcześniej ankiet lub szablonów.
150.	Możliwość wykonania badania przedmiotowego na podstawie zdefiniowanych wcześniej ankiet lub szablonów.
151.	Możliwość prowadzenia formularzowej Historii Choroby.
152.	Modyfikacja z poziomu administratora schematów historii choroby.
153.	Dodawanie z poziomu administratora elementów schematu historii choroby.
154.	Możliwość wykonania opisu zabiegu na podstawie zdefiniowanych wcześniej ankiet lub szablonów.
155.	Możliwość kopiowania opisów z poprzednich wizyt.
156.	Możliwość edytowania skopiowanego opisu.
157.	Wykorzystywanie własnych schematów historii choroby.
158.	Możliwość dodawania plików graficznych (w formatach obsługiwanych przez system Windows) do historii choroby.
159.	Możliwość wpisania kodu chorobowego ICD10 jako: ▪ kodu chorobowego wstępnego, ▪ kodu chorobowego zasadniczego, ▪ kodu chorobowego dodatkowego, ▪ kodu chorobowego współistniejącego, ▪ kodu chorobowego V-Y.
160.	Możliwość wybrania kodu chorobowego ICD10 ze słownika według: • kodu, • opisu.
161.	Możliwość ręcznego wpisania kodu chorobowego ICD10.
162.	Możliwość przypisania pacjentowi diety wybranej ze słownika.
163.	Dodawanie uwag do wizyty.
164.	Dodawanie procedur ze słownika ICD9.
165.	Możliwość utworzenia własnych grup procedur.
166.	Możliwość ręcznego dopisania procedury.
167.	Możliwość automatycznego dopisania procedury po wykonaniu badania laboratoryjnego i otrzymaniu zwrotnie wyniku.
168.	Możliwość zamykania procesu leczniczego z poziomu gabinetu lekarskiego.
169.	Możliwość wystawienia skierowania dla pacjenta: ▪ do szpitala, ▪ do specjalisty, ▪ na badania, ▪ na transport, ▪ na badania laboratoryjne, ▪ na badania radiologiczne, ▪ na badania histopatologiczne.
170.	Możliwość wystawiania zaświadczeń opisowych z możliwością edycji.
171.	Możliwość obejrzenia dołączonych plików multimedialnych z jednego okna.
172.	Podgląd na wcześniejsze wpisane szczepienia pacjenta.
173.	Podgląd na wpisane do systemu leki uczulające pacjenta.

L.p.	Opis wymagania
174.	Dostęp do pełnej historii choroby pacjenta wygenerowanej podczas poprzednich pobytów.
175.	System umożliwia wystawianie recept na pacjenta.
176.	Kopiowanie wcześniej wystawionych recept.
177.	Blokada przed ponownym wydrukowaniem tej samej recepty.
178.	Anulowanie błędnie wystawionej recepty.
179.	Sprawdzanie puli dostępnych recept dla danego lekarza z podziałem na: ▪ NFZ, ▪ prywatne, ▪ psychotropowe.
180.	Możliwość wydrukowania recept przed wizytą domową dla konkretnego pacjenta.
181.	Dostęp do informacji o ubezpieczeniu przy wystawianiu recepty.
182.	Przy wystawianiu recept z lekiem refundowanym program dokonuje walidacji ubezpieczenia pacjenta i jeżeli pacjent nie posiada uprawnień do refundacji świadczeń, system podaje komunikat o braku ubezpieczenia pacjenta.
183.	Wprowadzenie leków na receptę.
184.	Wydruk recepty lub nadruk na receptę.
185.	Tworzenie recepty na podstawie wcześniej wystawionych recept.
186.	Możliwość wstawienia jednocześnie do pięciu leków na receptę.
187.	Możliwość tworzenia schematów recept oraz zarzadzania nimi przez lekarza.
188.	Podgląd charakterystyki produktu leczniczego.
189.	Walidacja dla świadczeń z zakresu chemioterapii i programów lekowych podczas uzupełniania pól.
190.	Filtrowanie leków pod kątem refundacji i uaktualnianie bazy.
191.	Wyróżnienie kolorystyczne leków refundowanych i uaktualniania bazy.
192.	Dostęp do informacji o refundacji leków i uaktualniania bazy.
193.	Dostęp do cen leków refundowanych i uaktualnianie bazy.
194.	Wczytanie puli recept.
195.	Wystawianie recept z lekami do przygotowania w aptece (leki recepturowe). Korzystanie ze zdefiniowanych wcześniej szablonów.
196.	Dostęp do skanowanej uprzednio dokumentacji pacjenta.
197.	Wydruk karty informacyjnej dla pacjenta lub dla lekarza kierującego oraz dowolnych definiowalnych raportów związanych z pacjentem lub historią choroby pacjenta.
198.	Możliwość drukowania paragonów fiskalnych.
199.	Możliwość drukowania faktur VAT.
Funkcjonalności obszaru ewidencji pacjentów	
200.	System posiada wspólną Ewidencję Główną Pacjentów dla wszystkich poradni.
201.	System gromadzi w Karcie Pacjenta: ▪ dane osobowe, ▪ dane adresowe, ▪ adres e-mail, ▪ kartoteki papierowej, ▪ zatrudnienie, ▪ ubezpieczenie, ▪ płatnik, oddział NFZ.
202.	System gromadzi w Karcie Pacjenta dodatkowe dane, takie jak: ▪ wywiad rodzinny, ▪ wywiad środowiskowy, ▪ grupa krwi ▪ dane opiekuna, ▪ upoważnienie o zgodzie do uzyskania informacji o stanie zdrowia, ▪ upoważnienie o zgodzie do uzyskania dokumentacji medycznej, ▪ rodzaj i nr dokumentu uprawniającego do leczenia, ▪ dane i uprawnienia opiekunów oraz innych osób uprawnionych do otrzymywania informacji na temat stanu pacjenta, ▪ dane osób uprawnionych do odbierania dokumentacji medycznej pacjenta, ▪ dane i uprawnienia opiekunów oraz innych osób uprawnionych do otrzymania dokumentacji pacjenta w przypadku jego śmierci.

L.p.	Opis wymagania
203.	System umożliwia zapisanie w Karcie Pacjenta dodatkowych danych jak: ▪ informacja na temat szczepień, ▪ informacji na temat przebytych chorób, ▪ informacji na temat uczulenia na leki i materiały medyczne, ▪ informacji na temat wypożyczanego sprzętu, ▪ dowolnej informacji na temat pacjenta w postaci ogólnych uwag, ▪ informacji na temat umów, polis związanych z komercyjną/prywatną wizytą, ▪ informacji o koncie do rejestracji internetowej.
204.	Podgląd na wcześniejsze wpisane szczepienia pacjenta.
205.	Możliwość podglądu wcześniejszych wizyt pacjenta w jednostce.
206.	Dostęp do informacji: ▪ data/godzina rejestracji, ▪ data przyjęcia, ▪ data wypisu, ▪ rodzaj poradni, w której był przyjęty pacjent, ▪ dane lekarza przyjmującego, ▪ data skierowania, ▪ status wizyty, ▪ przyczyna skreślenia.
207.	Filtrowanie informacji z odbytych wizyt przy użyciu parametrów: ▪ data/godzina rejestracji, ▪ data przyjęcia, ▪ data wypisu, ▪ rodzaj poradni, w której był przyjęty pacjent, ▪ dane lekarza przyjmującego, ▪ data skierowania, ▪ status wizyty.
208.	Możliwość dodania pacjenta niezidentyfikowanego.
209.	Wyszukiwanie danych pacjenta z uwzględnieniem danych takich jak: ▪ imię i nazwisko, ▪ nr PESEL.
210.	Filtrowanie danych pacjentów w ewidencji pod kątem: ▪ miejscowości, ▪ roku urodzenia.
211.	Możliwość skanowania i podglądu zeskanowanych dokumentów.
212.	Sprawdzenie statusu ubezpieczenia pacjenta (eWUŚ).
213.	Możliwość wyeksportowania historii wizyt pacjenta w danej jednostce do pliku XML.
214.	Sprawdzanie kolejek oczekujących na wizyty.
215.	System umożliwia przypisanie do pacjenta alergenów lub leków, na które jest uczulony.
216.	Możliwość wystawienie e-ZLA w trybie online oraz alternatywnym.
217.	Możliwość wyświetlenia wszystkich logów związanych z komunikacją z danym pacjentem.
218.	Możliwość dostępu do informacje o powiadomieniach pacjenta, wiadomościach odebranych, zdarzeniach (połączeniach telefonicznych) oraz informacjach związanych z grupowymi wiadomościami wychodzącymi/przechodzącymi
Funkcjonalności obszaru eWUŚ	
219.	Możliwość weryfikacji prawa pacjenta do świadczeń opieki zdrowotnej finansowanych ze środków publicznych w modułach/funkcjonalnościach: • rejestracja i call center, • terminarz, • ewidencja pacjentów, • ruch chorych, • Księga Główna.
220.	Dostęp do historii weryfikacji uprawnień pacjenta.
221.	Możliwość wprowadzenia informacji o przedstawieniu przez pacjenta dokumentu uprawniającego do skorzystania z usług w ramach NFZ lub złożeniu przez pacjenta oświadczenia.
222.	Możliwość cyklicznego automatycznego sprawdzania uprawnień pacjentów.
223.	Możliwość zmiany hasła dostępu użytkownika do systemu eWUŚ.
224.	Podczas logowania do systemu opcjonalnie pojawia się komunikat o wygaśnięciu hasła do eWUŚ.

225.	Sprawdzanie statusu ubezpieczenia eWUŚ na tego świadczeniodawcę, do którego jest przypisana historia choroby (przy obsłudze wielu świadczeniodawców). Aby funkcjonalność działała poprawnie w systemie powinien istnieć odpowiedni użytkownik. Dla sprawdzenia cyklicznego na pacjenta eWUŚ sprawdzany jest na wszystkich dostępnych świadczeniodawców.
Funkcjonalność obszaru zleceń	
226.	Możliwość obsługi elektronicznych zleceń medycznych w tym: ▪ wysłanie zlecenia, ▪ śledzenie stanu wykonania zlecenia, ▪ zwrotne odebranie wyniku zlecenia ▪ automatyczne usuwanie zleceń w przypadku niezgłoszenia się w wyznaczonym terminie do operacji lub zabiegu.
227.	Możliwość wprowadzenia, modyfikacji, przedłużenia oraz anulowania zleceń dla pacjentów. Wprowadzanie zleceń jest możliwe dla wszystkich pacjentów objętych ruchem chorych.
228.	Zapewnienie kontroli wprowadzania podwójnych zleceń oraz kontroli zlecenia pod kątem poprawności i kompletności.
229.	Możliwość wykorzystania kodów kreskowych i czytników do identyfikacji zleceń.
230.	Możliwość wykorzystania danych z modułu do rozliczania kosztów.
231.	Rejestracja etapów wykonania/realizacji zlecenia.
232.	Możliwość anulowanie zlecenia.
233.	Automatyczny zapis daty i czasu, osobę wprowadzającą, zmieniającą i odwołującą zlecenie.
234.	Automatyczny zapis daty i czasu, osobę wprowadzająca oraz zmieniająca wyniki.
235.	Automatyczne aktualizowanie etapu realizacji zlecenia.
236.	Automatyczne przekazanie zlecenia do jednostki realizującej zlecenie.
237.	Automatyczne zwrotne przekazanie wyniku.
238.	Możliwość przedłużania zleceń, zleceń cyklicznych.
239.	Możliwość drukowania skierowań na badania i konsultacje do jednostek zewnętrznych.
240.	Możliwość zapisania w ramach komentarza do zlecenia istotnych danych diagnostycznych (rozpoznanie, kierunek badania, grupa krwi itp.).
241.	Możliwość integracji w trybie online za pomocą standardu HL 7 ver. 2.3 (minimum) (opcja dostępna w przypadku wykupienia licencji modułu HL7).
242.	Blokada modyfikacji zatwierdzonego lub anulowanego zdarzenia przez inna osobę niż twórcą lub administratora.
Funkcjonalności obszaru eZLA	
243.	Możliwość wystawiania elektronicznych zwolnień lekarskich dla pacjenta i/lub jego opiekuna oraz wysyłania tych zwolnień do ZUS. Funkcjonalność wystawiania zwolnień dostępna jest z poziomu okna opisu przebiegu wizyty.
244.	Obsługa trybu alternatywnego - wyświetlenie listy pobranych druków eZLA z poziomu trybu alternatywnego. W przypadku, gdy lista nie została pobrana lub lista dostępnych numerów została wyczerpana, istnieje możliwość pobrania kolejnych wolnych druków. Każdy pobrany numer zwolnienia z ZUS zostanie opatrzony statusem „wydrukowany” jako pobrany z ZUS, nie drukowany fizycznie.
Funkcjonalności obszaru statystyki	
245.	Obsługa bazy pacjentów poradni, zakładu, pracowni.
246.	Wyszukiwanie pacjentów w skorowidzu wg różnych parametrów (min. nazwisko, PESEL, ID Wewnętrzny).
247.	Możliwość automatycznego numerowania pacjentów w Księdze Głównej.
248.	Przegląd danych archiwalnych pacjenta danych z poszczególnych pobytów, wizyt w zakładach diagnostycznych, wyników badań i wizyt w poradniach.
249.	Potwierdzenia wypisu pacjenta pod kątem kompletności i poprawności danych.
250.	Możliwość wygenerowania/wydruku Karty Statystycznej.
251.	Możliwość wygenerowania/wydruku zaświadczenia o pobycie.
252.	Możliwość wygenerowania/wydruku Księgi Głównej.
253.	Możliwość wygenerowania/wydruku skorowidza alfabetycznego do Księgi Głównej.
254.	Obsługa Księgi Oczekujących (kolejki oczekujących).
255.	Obsługa Księgi Poradni.
256.	Obsługa Księgi Pracowni Diagnostycznej.
257.	Obsługa Księgi Zabiegowej.
258.	Elektroniczna komunikacja z NFZ.
259.	Możliwość potwierdzenia przez lekarza zakończenia wizyty lekarskiej wraz ze sprawdzeniem kompletności danych dotyczących pacjenta i wykonanych świadczeń.
260.	Musi istnieć funkcjonalność tworzenia oraz wydruku i eksportu budowanego przez administratora

	dowolnego zestawienia/raportu na bazie danych gromadzonych przez system HIS.
261.	Czas oczekiwania (planowany i rzeczywisty) na poszczególne świadczenia (dane z list oczekujących).
Funkcjonalności obszaru sprawozdawczo-rozliczeniowego	
262.	Możliwość ewidencjonowania umów zawartych z oddziałami NFZ.
263.	Możliwość ręcznego dopisania jednostki miary do konkretnej pozycji na fakturze.
264.	System prowadzi i monitoruje kolejki oczekujących na wykonanie procedur medycznych zgodnie z wymaganiami prawa.
265.	System generuje sprawozdania ze stanu tych kolejek zgodnie z wymaganiami NFZ.
266.	System umożliwia wysyłkę do Centralnej Kolejki Oczekujących (AP-KOLCE).
267.	System umożliwia obsługę faktur zakupowych wraz z informacją o ilość dostępnej substancji leku z faktury i jej wykorzystaniu.
268.	System spełnia wymogi prawne dotyczące rozliczeń świadczeń i umów w służbie zdrowia.
269.	Generowanie sprawozdań do systemów rozliczeniowych płatników świadczeń w formatach wymaganych przez NFZ.
270.	Generowanie wydruków do sprawozdań (sprawozdawczość wymagana przez NFZ).
271.	Przechowywanie informacji o strukturze organizacyjnej zakładu.
272.	Możliwość powiązania struktury organizacyjnej zakładu z kontraktem NFZ (możliwość wskazania, która jednostka organizacyjna w Zakładzie odpowiada jednostkom z kontraktu NFZ).
273.	Automatyczne tworzenie raportu dla NFZ na podstawie wprowadzonych danych w gabinetach i na oddziałach.
274.	Automatyczna zmiana koloru czcionki umowy na czerwony po zaczytaniu paczki z odpowiedziami dla umów, dla których można wystawić rachunek.
275.	Podgląd limitów oraz sumy punktów zaplanowanych zabiegów w poszczególnych miesiącach dla umów NFZ w trakcie planowania zabiegów rehabilitacyjnych.
276.	Możliwość stworzenia wykresów słupkowych odzwierciedlających stan wykorzystania świadczeń w stosunku do limitów NFZ na oferowane świadczenia.
277.	Rozliczenie usług/badań z NFZ według obowiązujących zarządzeń Prezesa NFZ, Rozporządzeń i Ustaw Ministra Zdrowia.
278.	Gruper, który na podstawie danych wprowadzonych podczas wizyty potrafi wskazać pozycję rozliczeniową z katalogu NFZ.
279.	Raporty pozwalające na bieżąco śledzić stan realizacji umowy.
280.	Możliwość nadania drugiego statusu (innego niż z NFZ) dla produktu już rozliczonego.
281.	Możliwość zmiany wersji wysyłki.
282.	Zmiana statusu produktu z wyszczególnieniem zakresu dat, umowy, produktu oraz wyróżnika.
283.	Wybór danych do eksportu – z podziałem na: ▪ kolejki oczekujących, ▪ faktury zakupowe, ▪ rozliczenia, ▪ świadczenia.
284.	Opcja eksportu danych z możliwością zastosowania filtra dla błędnych rekordów.
285.	Możliwość generowania danych do eksportu według: ▪ umowy, ▪ produktu, ▪ wyróżnika, ▪ zakresu dat.
286.	Możliwość importu umów z Narodowym Funduszem Zdrowia oraz aneksów.
287.	Możliwość przypisania umowy do kolejnej jednostki świadczącej usługi.
288.	Generowanie sprawozdań takich jak: ▪ ZD3, ▪ MZ-11, ▪ CZP ▪ MZ-15 ▪ MZ-19 ▪ MZ-29 ▪ MZ-29A ▪ MZ-55
289.	Możliwość filtrowania sprawozdań według umowy, roku i miesiąca.
290.	Przeliczanie wszystkich kolejek.
291.	Przeliczanie wybranej kolejki i wysłania jej do NFZ.

292.	Walidacja kolejek.
293.	Informacja o błędach w kolejce.
294.	Podgląd listy pacjentów oczekujących w kolejce.
295.	Wyszukiwanie pacjenta po numerze PESEL.
296.	Możliwość nadania kodu skreślenia dla wybranego pacjenta lub dla wszystkich rekordów.
297.	System umożliwia podgląd informacji o błędzie przesłanej z NFZ.
298.	Możliwość eksportowania do pliku CSV lub HTML danych o świadczeniach.
299.	Możliwość konfiguracji rozliczeń z wieloma oddziałami NFZ.
300.	Możliwości definiowania konta bankowego na umowę.
Funkcjonalności obszaru elektronicznej dokumentacji medycznej	
301.	Generowanie i przechowywanie elektronicznej dokumentacji medycznej w formie HL7 CDA (dla dokumentów wskazanych w ROZPORZĄDZENIU MINISTRA ZDROWIA z dnia 8 maja 2018 r. w sprawie rodzajów elektronicznej dokumentacji medycznej) oraz w formie PDF wraz z informacjami pozwalającymi na zidentyfikowanie osoby generującej dokument.
302.	System ma mieć możliwość zarządzania obiegiem elektronicznej dokumentacji medycznej w zakresie: • definiowania ról do użytkowników (np. lekarz, pielęgniarka) z podziałem na komórki organizacyjne lub w ramach całego podmiotu, • definiowania wymagalności podpisywania elektronicznych dokumentów przez określone role użytkowników (wymagane role oraz kolejność podpisywania/akceptowania dokumentu), • system prezentuje użytkownikowi listę dokumentów które muszą być przez niego elektronicznie podpisane/zatwierdzone, • system daje możliwość wprowadzenia odmowy podpisania dokumentu przez użytkownika z adnotacją o przyczynach odmowy, • system kontroluje, czy wszystkie wymagane role/użytkownicy podpisali się na danym dokumencie, • system ma możliwość kontroli wersjonowania dokumentu.
303.	W przypadku dokonania ponownego wygenerowania dokumentu, tworzony jest nowy PDF oraz XML odkładany jako kolejna wersja dokumentu przechowywana w module EDM.
304.	Możliwość podpisania certyfikatem elektronicznym (kwalifikowanym lub niekwalifikowanym) albo certyfikatem PUE wystawionym przez ZUS wygenerowanego dokumentu PDF oraz XML.
305.	Możliwość wyszukiwania dokumentów.
306.	Brak możliwości modyfikowania zarejestrowanych dokumentów w module EDM.
307.	Możliwość przypisywania ról/uprawnień dla użytkowników w celu podpisywania określonych elektronicznych dokumentów medycznych.
308.	Możliwość automatycznego zapisywania drukowanych dokumentów w wersji elektronicznej oraz zapamiętywania wszelkich zmian dokonywanych na tych dokumentach wraz z kolejnym wydrukiem (wersjonowanie). Funkcjonalność pozwala również na podpisywanie dokumentu PDF podpisem elektronicznym.
309.	Możliwość informowania użytkownika o liczbie dokumentów elektronicznych które musi podpisać (powiązanych z rolą użytkownika).
310.	Możliwe jest podpisanie/odmowa podpisania zbiorczo grupy dokumentów.
311.	Dla wskazanego dokumentu możliwość wyświetlenia informacji o pacjencie, dla którego został wygenerowany dokument, miejscu wytworzenia dokumentu, rodzaju dokumentu, informacji o tym, czy dokument został dodany w formie elektronicznej, dacie wytworzenia dokumentu, statusie podpisania.
Funkcjonalności obszaru archiwum	
312.	Możliwość ewidencjonowania archiwum papierowego.
313.	Możliwość nadania statusu dokumentacji medycznej: ▪ Wypożyczenie, ▪ Zwrot, ▪ Zniszczenie, ▪ Odnalezienie, ▪ Kopia, ▪ Planowe zniszczenie, ▪ Archiwum.

314.	Adnotacja o osobie wypożyczającej/wydającej dokumentacje medyczne.
315.	Automatyczny druk dokumentu PDF podczas wydruków: karty informacyjnej, wypisu, z przypisaniem go do historii choroby.
316.	Przechowywanie dokumentów elektronicznych wraz z wersjonowaniem.
317.	Możliwość podpisu dokumentu PDF.
318.	Możliwość bezpośredniej obsługi urządzeń skanujących w celu dołączania zeskanowanych dokumentów do kartoteki pacjenta
Funkcjonalności medycyny pracy	
319.	System umożliwia realizację procesów obsługi pacjenta: • rejestracja pacjenta w: Poradni Chorób Zawodowych, Poradni Szkoleniowej Medycyny Pracy, Poradni Badań Kierowców. Pracowni Psychologicznej, Odwoławczej Pracowni Psychologicznej • ze względu na cel wizyty: rejestracja w celu udzielenia profilaktycznego świadczenia zdrowotnego (profilaktyka, patologia zawodowa, kierowcy, odwołania), rejestracja w celu udzielenia ambulatoryjnego świadczenia zdrowotnego na indywidualne życzenie pacjenta, rejestracja w celu udzielenia świadczenia zdrowotnego w ramach umowy z innym zakładem opieki zdrowotnej, indywidualną lub grupową praktyką lekarską.
320.	System umożliwia realizację procesów obsługi pacjenta: • opis procesu leczniczego: w Poradni Medycyny Pracy (m.in.: badania profilaktyczne z wydaniem zaświadczenia dla celów przewidzianych w Kodeksie pracy, badania profilaktyczne z wydaniem zaświadczenia realizowanych w trybie art. 229 § 5 Kodeksu pracy, w przypadku gdy podmiot, który zatrudniał pracownika, uległ likwidacji, badanie profilaktyczne z wydaniem zaświadczenia dla celów przewidzianych w Kodeksie pracy z uwzględnieniem trybu odwoławczego, badanie z wydaniem zaświadczenia dotyczącego możliwości kształcenia się pacjenta we wskazanym kierunku, badanie diagnostyczno-orzecznicze w celu rozpoznania choroby zawodowej, badanie w celu wydania orzeczenia lekarskiego dla kierowcy w trybie art. 75 ust.1 pkt.1-6 ustawy o kierujących pojazdami), • opis procesu leczniczego w poradniach specjalistycznych (pacjent pierwszorazowy, kontynuacja leczenia), • opis procesu rehabilitacji leczniczej związanej z patologią zawodową.
321.	System wspiera obsługę „trybu standardowego" medycyny pracy (badania profilaktyczne i konsultacje, wydawanie orzeczeń o zdolności/niezdolności do pracy) poprzez obsługę zdarzeń: • przeprowadzenie wstępnego wywiadu z pacjentem przez pielęgniarkę medycyny pracy oraz wizyta w gabinecie lekarza orzecznika, który przeprowadza pełny wywiad z pacjentem, • dodanie skierowań na konsultacje specjalistyczne lub badania dodatkowe uwarunkowane zagrożeniami związanymi ze stanowiskiem pracy wskazanym na skierowaniu, • wystawianie orzeczenia i przekazanie go pacjentowi, • wprowadzenie orzeczenia do Księgi Orzeczeń w systemie.
322.	Dla wizyt typu „medycyna pracy" możliwość skierowania na dodatkowe badania przez lekarza orzecznika, umożliwienie „doplanowania" dodatkowych badań związanych z czynnikami szkodliwymi.
323.	Możliwość planowania więcej niż dwóch wizyt u orzecznika oraz możliwość doplanowania dodatkowych konsultacji w procesie orzeczniczym dla każdej wizyty u orzecznika.
324.	Możliwość określenia planowania ostatniej wizyty u orzecznika: tylko gdy są inne konsultacje, zawsze, bez planowania, z pytaniem o planowanie (system za pomocą komunikatu będzie pytał o zaplanowanie ostatniej wizyty, bez względu na ilość konsultacji i/oraz badań).
325.	Po zaplanowaniu wizyty i konsultacji możliwość wprowadzenia dodatkowych konsultacji przez wprowadzenia dodatkowego narażenia do listy wybranych narażeń lub pojedynczego wprowadzenia dodatkowej procedury lekarskiej bądź pomocniczej. W przypadku wybrania dodatkowego narażenia system automatycznie przedstawi na liście konsultacji dodatkowe pozycje związane z nowym narażeniem.
326.	Funkcja "Doplanuj", pozwalająca na doplanowanie narażeń dla zaplanowanych już wizyt (niezbędne w sytuacji, w której została już zaplanowana konsultacja/badanie, po czym do takiej pozycji użytkownik dodaje nowe narażenie).
327.	W oknie narażeń dla wizyty typu „konsultacyjna w procesie orzeczniczym" umożliwienie skopiowanie zaplanowanej wizyty konsultacyjnej z możliwością ponownego jej zaplanowania oraz umożliwienie przejęcia do obecnego procesu wizyty Medycyny Pracy innych wizyt.
328.	Podgląd dostępnych terminów konsultacji oraz funkcja planowania dla narażeń dostępne są w osobnym oknie. W oknie, w którym znajduje się lista proponowanych terminów wizyt związanych z medycyną pracy, użytkownik może zmienić poszczególne terminy wizyt pacjenta.
329.	Możliwość: • zaplanowania niezaplanowanych narażeń - po dodaniu nowych można ponownie zaplanować nowo dodane (nie ma walidacji na wymagalność wizyty u orzecznika przy takim doplanowaniu. Wizyta u orzecznika nadal jest wymagana dla pierwszego planowania); • doplanowania narażeń dla zaplanowanych już wizyt - w sytuacji, gdy istnieje już

	zaplanowana konsultacja/badanie i do takiej pozycji trzeba dodać nowe narażenie; • odplanowania - dla aktualnych (nie w trakcie lub archiwalnych) historii chorób system oznacza je jako „archiwalne” oraz dodaje status „pacjent nie zgłosił się”. Dodatkowo pozycje rozliczeniowe, które nie są jeszcze rozliczone są usuwane, zlecone badania, które nie są wykonane są usuwane, również puste zlecenia. Na liście zaplanowanych konsultacji\badań takie odplanowane konsultacje\badania są oznaczone np. kolorem czerwonym.
330.	Możliwość odplanowania wizyt, badań i konsultacji (bez zmiany listy narażeń) pojedynczo lub zbiorczo (wszystkich).
331.	Odplanowanie wizyty orzeczniczej umożliwia odplanowanie wszystkich wizyt związanych z tą wizytą orzeczniczą. System wyświetli zapytanie o ustawienie wizyt oraz badań jako archiwalnych.
332.	W przypadku zmiany terminu badania możliwość zmiany jednostki, jeżeli w konfiguracji systemu istnieje inna o tym samym kodzie resortowym oraz zmiany daty i godziny badania.
333.	Na potrzeby komercji dla medycyny pracy w systemie można definiować umowy wzorcowe (umowa wzorcowa to umowa, która zawiera pozycje i opcjonalnie definicje ograniczenia lokalizacji na umowie, można ją wykorzystać do utworzenia nowych umów).
334.	Możliwość podpięcia umowy wzorcowej podczas dodawania nowej umowy. Do takiej umowy zostają przepisane wszystkie pozycje i ograniczenia z umowy wzorcowej, nie jest możliwa edycja przepisanych pozycji, przy podpięciu umowy nie jest przepisywany nagłówek umowy (waluta, płatnik itp.). Można natomiast dodawać nowe pozycje, nie kolidujące z przepisanymi z umowy wzorcowej. Jeśli nowo dodawana pozycja na umowie wzorcowej będzie kolidować z pozycją na umowie podrzędnej, to taka pozycja zostanie zastąpiona pozycją z umowy wzorcowej.
335.	Dla wizyt typu medycyna pracy przy przypisywaniu płatnika/firmy podczas edycji słownika możliwość wyboru płatnika ze słownika (widoczne są nazwa płatnika, dane adresowe oraz NIP i REGON). Jeżeli w konfiguracji płatników dane zostały uzupełnione, podczas wyboru płatnika ze słownika, dane firmy zostaną uzupełnione na podstawie danych wskazanego płatnika. Jeżeli wskazany płatnik nie posiada wprowadzonych danych adresowych itp. użytkownik ma możliwość uzupełnienia brakujących danych.
336.	Podczas edycji rejestracji dla wizyt typu ,,proces orzeczniczy'' oraz ,,konsultacja w procesie orzeczniczym'' możliwość podpięcia zarejestrowanej wizyty do procesu orzeczniczego. System waliduje: zarejestrowana wizyta nie może posiadać żadnych narażeń. musi być zgodna co do pacjenta, płatnika, ubezpieczyciela oraz umowy, musi posiadać minimum jedną przypisaną procedurę medyczną.
337.	Podczas rejestracji wizyty typu „proces orzeczniczy” program nie wymaga dodania pozycji rozliczeniowej.
338.	Możliwość takiego skonfigurowania wizyty konsultacyjnej w procesie orzeczniczym, by nie było jej widać na pozycjach HCH u lekarza orzecznika.
339.	Możliwość doplanowania danych badań pomocniczych (np.: morfologia krwi, badanie EKG, RTG klatki piersiowej itp.). W zależności od konfiguracji pozycje rozliczeniowe ze skopiowanej konsultacji leczniczej lub pomocniczej (badanie diagnostyczne lub laboratoryjne) mogą zostać dodane lub nie do rozliczenia.
340.	W przypadku, gdy w procedurze postępowania danego narażenia dla badania pomocniczego jest określona pozycja rozliczeniowa, pozycja ta będzie dodawana do rozliczenia wraz z limitami, cenami oraz ograniczeniami lokalizacji wynikającymi z danej umowy.
341.	Dla badań skonfigurowanych jako CITO system po wprowadzeniu narażeń i zaplanowaniu poszczególnych konsultacji i badań, na oknie zlecenia oraz wyników do zlecenia automatycznie wskaże dane zlecenie/badanie jako przeprowadzone w trybie CITO.
342.	Wybór wolnych terminów z filtrowaniem po datach - jako data początkowa oraz końcowa brane są pod uwagę daty wprowadzone/ustawione w oknie narażeń. W przypadku zmiany bądź wprowadzenia kolejnej wizyty u orzecznika w oknie wyboru wolnego terminu system będzie pokazywał terminy po ostatniej konsultacji u specjalisty. Dla zmiany wizyt konsultacyjnych, jeśli jest równocześnie planowana z wizytą w poradni medycyny pracy, na liście zostaną wyświetlone godziny po wizycie u orzecznika.
343.	Na oknie planowania narażeń możliwość przejrzenia całego procesu w ramach medycyny pracy. Na liście wizyt zostanie wyświetlona informacja o poradni, gabinecie, terminie wizyty oraz obecnym statusie. Na liście zostaną uwzględnione wizyty, które zostały skopiowane lub przyjęte pod dany proces z medycyny pracy.
344.	Definicja umowy/programu/polisy dla medycyny pracy pozwala na określenie czy płatność jest po stronie pacjenta. Dla takiej umowy wszystkie pozycje z wprowadzonego cennika, po wprowadzeniu do danej wizyty, zostaną automatycznie przepisane jako płatne po stronie pacjenta.
345.	Możliwość określenia, czy data badań pomocniczych ma zostać automatycznie pobrana z daty zlecenia lub z daty pierwszej wizyty u orzecznika. W zależności od wartości parametru konfiguracyjnego daty badań pomocniczych w oknie prezentującym proponowane terminy konsultacji brane będą z bieżącej daty zlecenia lub z daty pierwszej wizyty orzeczniczej.
346.	Na oknie konfiguracji umowy możliwość przypisania firmy dla płatnika wskazanego w umowie (przez wybór z listy firm wprowadzonych w księdze adresowej systemu). Po dopisaniu firm do umów z wybranym płatnikiem w oknie Rejestracji istnieje możliwość wybrania firm określonych w

	ramach umowy.
347.	Możliwość dopisywania narażeń oraz procedur przez lekarzy konsultantów. Tacy lekarze mają możliwość kopiowania wybranej wcześniej zaplanowanej wizyty konsultacyjnej oraz usuwania poszczególnych niezaplanowanych narażeń lub niezaplanowanych konsultacji. Zaplanowanie/odplanowanie oraz dodanie pojedynczej procedury postępowania nie są dostępne dla takich lekarzy.
348.	Możliwość zapamiętywania filtrów z medycyny pracy: globalnie, na stację roboczą (na stanowisko pracy niezależnie od zalogowanego użytkownika) lub na użytkownika.
349.	Dla sprawozdań z umów z zakresu Medycyny Pracy wyświetlana jest kolumna, która zawiera informacje dotyczące tego, czy dana usługa pochodzi z zamkniętego lub otwartego procesu orzeczniczego.
350.	Na oknie narażeń wszystkie pozycje konsultacyjne, które są spoza danej umowy, są oznaczone kolorem wraz z dodatkową informacją ("spoza umowy")
351.	Dla procedur, dla których został zaznaczony znacznik „procedura dostępna tylko dla zgodnych rodzajów badań” użytkownik ma możliwość wprowadzenia procedury postępowania zależnie od rodzaju badania. Procedura taka w oknie narażeń jest dostępna wyłącznie wówczas, gdy rodzaj badania danej wizyty będzie się pokrywał z wprowadzoną procedurą postępowania oraz lokalizacją.
352.	Dla danego czynnika szkodliwego (narażenia) system nie pozwala dodać po raz drugi procedury postępowania w obrębie danej lokalizacji
Dokumentacja i raporty statystyczne	
353.	System umożliwia wygenerowanie raportów statystycznych: • Sprawozdanie miesięczne/kwartalne/zbiorcze roczne z wykonanych badań lekarskich, • Sprawozdanie miesięczne/kwartalne/półroczne/roczne z wykonanych badań – Poradnia Medycyny Pracy, • Sprawozdanie miesięczne/kwartalne/półroczne/roczne z wykonanych badań – Pracownie, • Sprawozdanie miesięczne/kwartalne/półroczne/roczne z wykonanych badań – Pracownie pozostałe, • Wykaz wydanych orzeczeń dla pracowników szkół podstawowych, średnich, wyższych.
354.	System umożliwia wygenerowanie dokumentacji wykorzystywanej w działalności WOMP: • MZ-35A - Sprawozdanie lekarza przeprowadzającego badania profilaktyczne pracujących, • Wniosek o wpis do rejestru lekarzy przeprowadzających badania profilaktyczne, • Zaświadczenie o dokonaniu wpisu do rejestru lekarzy przeprowadzających badania profilaktyczne (wzór MZ), • Wydruk wzoru pieczęci, • Księga przeprowadzonych kontroli, • Protokół kontroli lekarza, • Protokół kontroli pielęgniarki, • Orzeczenie Lekarskie o kierujących pojazdami art 75 ust 1 pkt 1-5, • Orzeczenie Lekarskie o kierujących pojazdami art 75 ust 1 pkt 6, • Orzeczenie Lekarskie o kierujących pojazdami art. 75 ust 1 pkt 1-5 w trybie odwoławczym, • Orzeczenie Lekarskie o kierujących pojazdami art 75 ust 1 pkt 6 w trybie odwoławczym, • Oświadczenie dot. stanu zdrowia kierowcy – Ankieta, • Karta badania lekarskiego – kierowca, • Karta badania profilaktycznego, • Orzeczenie lekarskie - Kodeks pracy (symbol 21, 22, 23) w trybie odwoławczym, • Orzeczenie lekarskie - Kodeks pracy (symbol 31, 33, 34, 35) w trybie odwoławczym, • Orzeczenie lekarskie (broń i amunicja) w trybie odwoławczym, • Orzeczenie lekarskie (komornik) w trybie odwoławczym, • Orzeczenie lekarskie (ochrona fizyczna) w trybie odwoławczym, • Orzeczenie lekarskie dot. urlopu dla poratowania zdrowia – nauczyciel akademicki w trybie odwoławczym, • Orzeczenie lekarskie dot. urlopu dla poratowania zdrowia – nauczyciel szkoły podstawowej, średniej w trybie odwoławczym, • Zaświadczenie lekarskie dla ucznia, • Zgłoszenie podejrzenia choroby zawodowej (wzorzec MZ), • Skierowanie na badania w celu rozpoznania choroby zawodowej, • Skierowanie na badania w związku z podejrzeniem choroby zawodowej), • Karta oceny narażenia zawodowego w związku z podejrzeniem choroby zawodowej (wzorzec MZ), • Karta badania w związku z podejrzeniem choroby zawodowej, • Orzeczenie lekarskie o rozpoznaniu choroby zawodowej, • Orzeczenie lekarskie o braku podstaw do rozpoznania choroby zawodowej (wzorzec MZ), • Wniosek o ocenę narażenia zawodowego, • Skierowanie do zakładu rehabilitacji w związku ze stwierdzoną patologią zawodową,

	• Wynik konsultacji dla podstawowej jednostki medycyny pracy, • Amiantus - Badanie profilaktyczne pracowników narażonych na pył azbestu, • Karta Badania I – Amiantus (zielona), • Karta Badania II – Amiantus (różowa), • Orzeczenie lekarskie dla pracownika narażonego na pył azbestu, • Karta badania laryngologicznego dla MP, • Karta badania psychologicznego, • Karta badania psychologicznego dla kierowcy, • Karta badania okulistycznego dla MP, • Karta badania neurologicznego dla MP.
355.	System umożliwia wygenerowanie dokumentacji wykorzystywanej w działalności jednostki medycyny pracy: • Karta badania profilaktycznego, • Orzeczenie lekarskie - Kodeks pracy (symbol 21, 22, 23), • Orzeczenie lekarskie - Kodeks pracy (symbol 31, 33, 34, 35), • Orzeczenie sanitarno-epidemiologicznych, • Karta badania do celów sanitarno-epidemiologicznych, • Skierowanie na badania laboratoryjne, • Skierowanie do pracowni/na konsultacje, • Skierowanie na konsultację psychologiczną, • Zaświadczenie dla kobiety w ciąży/karmiącej, • Zaświadczenie dla osoby niepełnosprawnej, • Karta badania lekarskiego (bron i amunicja), • Karta badania lekarskiego (pracownik ochrony, detektyw), • Orzeczenie lekarskie (broń i amunicja), • Orzeczenie lekarskie (komornik), • Orzeczenie lekarskie (ochrona fizyczna), • Orzeczenie lekarskie dot. urlopu dla poratowania zdrowia – nauczyciel akademicki, • Orzeczenie lekarskie dot. urlopu dla poratowania zdrowia – nauczyciel szkoły podstawowej, średniej.

8. Wymagania dla bezpieczeństwa i ochrony danych osobowych

L.p.	Opis wymagania
1.	System musi spełniać wymagania bezpieczeństwa na poziomie wysokim opisanym w Załączniku do rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.
2.	System musi zostać zaprojektowany oraz wdrożony zgodnie z najlepszymi praktykami bezpieczeństwa, w zakresie technologii, jaka zostanie zastosowana do jego budowy.
3.	System informatyczny musi posiadać zaimplementowane mechanizmy kontroli dostępu do danych.
4.	W Systemie musi być rejestrowany odrębny identyfikator dla każdego użytkownika.
5.	System musi posiadać spójny i zaawansowany mechanizm kontroli dostępu. Dostęp do danych w Systemie będzie możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia.
6.	System musi wymuszać zmianę hasła nie rzadziej niż co 30 dni, a hasło musi składać się co najmniej z 8 znaków i zawierać: małe i wielkie litery oraz cyfry lub znaki specjalne.
7.	System musi posiadać funkcjonalność automatycznego wylogowania się z aplikacji po określonym czasie nieaktywności użytkownika.
8.	System musi posiadać ochronę przed zagrożeniami pochodzącymi z sieci publicznej opartą na fizycznych lub logicznych zabezpieczeniach chroniących przed nieuprawnionym dostępem.
9.	Dane z Systemu przesyłane w sieci publicznej muszą być zaszyfrowane. Niezbędne certyfikaty do szyfrowania danych zapewni Zamawiający.
10.	System musi być zabezpieczony przed: • działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego; • utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.
11.	System musi posiadać mechanizm backupu oraz archiwizacji danych.
12.	System musi mieć możliwość wykonywania kopii bezpieczeństwa w trakcie działania Systemu – bez konieczności jego zatrzymywania.
13.	System powinien umożliwiać ograniczenie dostępu do danych, funkcji systemu, procesów systemowych stosownie do danego stanowiska pracy tj. według zasady „w Systemie widzę tylko to co muszę, aby wypełniać swoje obowiązki”.

L.p.	Opis wymagania
14.	System musi tworzyć i utrzymywać log systemowy (datę i godzinę z dokładnością do sekundy; adres IP stacji, unikalny identyfikator użytkownika; jeżeli dane w Systemie uległy zmianie to również informacje o tym, z jakiej wartości i na jaką wartość została dokonana zmiana), rejestrujący w szczególności: • Zapisy o zalogowaniu do Systemu i wylogowaniu z Systemu każdego z użytkowników, • Zmianę parametrów konta każdego użytkownika, w szczególności zmianę uprawnień użytkownika, Każdą inną zmianę danych zgromadzonych w Systemie i dopisanie nowych danych do Systemu (wartość początkowa danych powinna być wówczas pusta).
15.	System musi posiadać mechanizm umożliwiający przeglądanie danych o logowaniu użytkowników do Systemu pozwalający na uzyskanie informacji o czasie i miejscach ich pracy tj. kto, od kiedy do kiedy, w której jednostce organizacyjnej (adres IP, nazwa jednostki organizacyjnej) był zalogowany.
16.	Wykonawca Systemu wykona testy penetracyjne systemu. Celem przeprowadzenia testów będzie praktyczna ocena stanu bezpieczeństwa systemu, w szczególności podatności i odporności na próby przełamania zabezpieczeń.
17.	Wykonawca Systemu wykona testy penetracyjne systemu. Celem przeprowadzenia testów będzie praktyczna ocena stanu bezpieczeństwa systemu, w szczególności podatności i odporności na próby przełamania zabezpieczeń. W ramach realizacji testów penetracyjnych systemu oczekuje się realizacji poniższych zadań: • Identyfikacja systemu za pomocą dostępnych serwisów sieciowych (np. WWW, SMTP, FTP, Telnet). • Rozpoznanie dostępnych z obszaru Internetu komputerów, serwerów, serwerów aplikacji, baz danych i urządzeń sieciowych, rodzaju i wersji systemów operacyjnych oraz oprogramowania użytkowego pod kątem wykrywania znanych luk bezpieczeństwa. • Wstępna penetracja systemu za pomocą skanerów portów TCP i UDP oraz skanerów zabezpieczeń powszechnie stosowanych przez hakerów, dostępnych w zasobach sieci Internet. • Testy zabezpieczeń systemu za pomocą profesjonalnych skanerów zabezpieczeń typu ISS Internet Scanner lub WebTrends Security Analyzer. • Analiza topologii sieci komputerowej widzianej z Internetu. • Analiza otrzymanych wyników pod kątem przygotowania symulacji włamań. • Symulacja włamań. • Ocena odporności zabezpieczeń systemu na ataki destrukcyjne za pomocą narzędzi dostępnych w zasobach sieci Internet. • Ocena poprawności reakcji systemu zabezpieczeń na wykonywane ataki. • Analiza bezpieczeństwa systemu zaporowego Firewall. • Analiza wyników testu penetracyjnego pod kątem oceny zagrożenia integralności systemu oraz możliwości dostępu do danych przez osoby nieupoważnione. • Analiza dokumentacji systemu pod kątem bezpieczeństwa (struktura sieci, konfiguracja, zastosowane urządzenia i oprogramowanie).

9. Wymagania w zakresie instruktaży

Zamawiający wymaga przeprowadzania przez Wykonawcę instruktaży dla personelu Zamawiającego zgodnie z wymaganiami przedstawionymi w poniższej tabeli:

L.p.	Opis wymagania
1.	Wykonawca w ramach wdrożenia przeprowadzi instruktaże dla 20 użytkowników, w tym 1 administratora Systemu.
2.	W ramach instruktaży dla użytkowników, Wykonawca przekaże uczestnikom pełną wiedzę niezbędną do poprawnego użytkowania funkcjonalności Systemu.
3.	Instruktaże dla administratorów obejmować będą: • administrowanie konfiguracją Systemu; • administrowanie oprogramowaniem.
4.	Instruktaże dla użytkowników należy przeprowadzić w formie indywidualnych instruktaży stanowiskowych. Dla przeprowadzenia instruktaży Zamawiający zapewni Wykonawcy stanowisko robocze i odpowiednie pomieszczenie wraz z infrastrukturą transmisji danych umożliwiającą dostęp do Systemu.
5.	Czas każdego instruktażu będzie uwzględniać stopień skomplikowania omawianego modułu lub grupy funkcjonalności.
6.	Czas trwania instruktażu dla każdego pracownika winien być nie krótszy niż 3 godziny.
7.	Łączny czas szkolenia wszystkich pracowników Zamawiającego będzie wynosił nie mniej niż 200

L.p.	Opis wymagania
	godzin zegarowych
8.	Przeprowadzenie instruktaży zostanie potwierdzone protokołem sporządzonym w dwóch jednobrzmiących egzemplarzach, po jednym dla Zamawiającego i Wykonawcy, zawierającym dla każdego szkolenia: • nazwę i tematykę i czas trwania szkolenia, • datę i miejsce szkolenia, • imię i nazwisko uczestnika w szkolenia, • imię i nazwisko oraz specjalizację osoby prowadzącej szkolenie. Protokół z przeprowadzenia instruktaży podlegać będzie zatwierdzeniu przez Zamawiającego.

10. Wymagania dla dokumentacji Projektu i Systemu

Zamawiający wymaga, aby Wykonawca wykonał i dostarczył, w sposób przedstawiony poniżej, następujące rodzaje dokumentacji bezpośrednio związanej z przedmiotem zamówienia:

L.p.	Opis wymagania
1.	Dokumentację Powykonawczą zawierającą opis stanu faktycznego (wykonanego wdrożenia i konfiguracji) Systemu.
2.	Plan instruktaży zawierający co najmniej następujące informacje: • informacje o zakresie tematycznym instruktaży; • opis metody i formy instruktaży; • harmonogram instruktaży; • agenda poszczególnych instruktaży;
3.	Instrukcje Użytkownika Systemu zawierające szczegółowy opis sposobu korzystania z poszczególnych funkcjonalności użytkowych Systemu.
4.	Zamawiający wymaga, aby wszystkie dokumenty tworzone w ramach realizacji zamówienia charakteryzowały się wysoką jakością, na którą będą miały wpływ, takie czynniki jak: • Struktura dokumentu, rozumiana jako podział danego dokumentu na rozdziały, podrozdziały i sekcje, w czytelny i zrozumiały sposób; • Zachowanie standardów, a także sposób pisania, rozumianych jako zachowanie spójnej struktury, formy i sposobu pisania dla poszczególnych dokumentów oraz fragmentów tego samego dokumentu; • Kompletność dokumentu, rozumiana jako pełne, bez wyraźnych, ewidentnych braków przedstawienie omawianego problemu obejmujące całość z danego zakresu rozpatrywanego zagadnienia. • Spójność i niesprzeczność dokumentu, rozumianych jako zapewnienie wzajemnej zgodności pomiędzy wszystkimi rodzajami informacji umieszczonymi w dokumencie, jak i brak logicznych sprzeczności pomiędzy informacjami zawartymi we wszystkich przekazanych dokumentach oraz we fragmentach tego samego dokumentu.

ROZDZIAŁ 2. Wymagania dla sprzętu i infrastruktury informatycznej dla PWOMP.

1. Macierz pamięci masowej – 1 szt.

Funkcjonalność/minimalne parametry techniczne/zakres prac:

Macierz	
Nazwa komponentu	**Wymagane minimalne parametry techniczne**
Dyski	Min. 7 dysków min. 1,9 TB ,SSD SAS Read intensive 2,5” Hot-Plug Możliwość rozbudowy do min 24 dysków w oferowanej obudowie Konfiguracja RAID – all flash, hybrid lub HDD
Obsługa RAID	RAID-0,1,5,6,10,50
Konfiguracja macierzy	Możliwość obsługi dysków all flash, hybrid lub HDD
Format macierzy	Native SAN lub DAS
Procesor	Min.2 core 2.2GHz

Porty	Min. 8 portowy kontroler SAS 12Gb/s - podłączenia do serwerów
Kontrolery	2 kontrolery wyposażone w przynajmniej 8GB cache każdy
Thin provisioning	aktywny
Snapshots	Min 1024 na kontroler
Wsparcie dla systemów operacyjnych	Windows 2012R2,2016,2019 Vmware 6.0,6.5,6.7 SLES 12.3 RHEL 6.9,7.4,8.0
Wsparcie virtualizacji	VMware vSphere (ESXi) vCenter; SRM 8.1.x Microsoft Hyper-V XenDesktop 7.1
Obudowa	Rack max 2U
Zasilanie	Zasilacz max 700W Redundantny
Gwarancja	Min. 3 lata naprawa na miejscu u klienta, uszkodzony dysk zostaje u zamawiającego, czas reakcji serwisu NBD

2. Serwer – 2 szt.

Funkcjonalność/minimalne parametry techniczne/zakres prac:

Dostarczenie Klastra 2 serwerów HA pełniące funkcję serwera bazodanowego i serwera aplikacyjnego. Oferent powinien uwzględnić koszty przeniesienia systemów pracujących u zamawiającego na środowisku virtualnym Microsoft HV na środowisko sprzętowe oferowane w ww postępowaniu.

Serwer	
Nazwa komponentu	**Wymagane minimalne parametry techniczne**
Obudowa	Do instalacji w szafie Rack 19", wysokość nie więcej niż 2U, z zestawem szyn do mocowania w szafie i wysuwania do celów serwisowych, wyposażona w zestaw ułatwiający wyprowadzenie przewodów z tyłu serwera.
Procesor	Architektura x86, maksymalny TDP dla procesora – 85W. Minimalna ilość rdzeni dla procesora – 8. Wynik wydajności procesora instalowanego w oferowanym serwerze powinien przekraczać 120 punktów peak w SPEC w teście SPEC CPU2017 Integer Rates opublikowanych przez SPEC.org (www.spec.org) dla konfiguracji dwuprocesorowej. Test przeprowadzony przez producenta serwera musi być zamieszczony na stronie spec.org. Obsługa minimum dwóch procesorów.
Liczba procesorów	Min. 2
Płyta główna	Płyta główna dedykowana do pracy w serwerach, wyprodukowana przez producenta serwera z możliwością zainstalowania do dwóch procesorów wykonujących 64-bitowe instrukcje AMD64 lub EM64T (np. AMD Opteron albo Intel Xeon)
Pamięć operacyjna	Minimum zainstalowane 192GB pamięci RAM Minimum 24 sloty na pamięć, wsparcie pamięci typu RDIMM oraz LRDIMM. Możliwość instalacji minimum 3 TB Ram Pamięć o częstotliwości minimum 2666MHz.
Zabezpieczenie pamięci	ECC
Procesor Graficzny	Zintegrowana karta graficzna z minimum 16MB pamięci osiągająca rozdzielczość 1920x1200 przy 60 Hz. 2 porty VGA (z przodu i z tyłu).
Dyski	Zainstalowane dyski: min. 2 x 1,9TB SSD SAS 6Gb/s
Rozbudowa dysków	Możliwość instalacji 12 dysków 2.5” Możliwość instalacji dysków SED.
Kontroler dyskowy	Zintegrowany na płycie kontroler SATA Zainstalowany kontroler 12 Gb SAS/SATA z obsługą RAID 0, 1, 10, 5, 50, 6, 60 Minimum 8 GB flash-backed cache.

Zasilacz	Minimum dwa redundantne zasilacze o mocy minimum 600W
Interfejsy sieciowe	Min. 2 interfejsy 10GbE Min. 2 interfejsy 1x GbE
Dodatkowe sloty I/O	Minimum wolny 1 slot o prędkości min.x16 Na płycie min 3 slotów PCI Sloty muszą być dostępne dla użytkownika – tj. niezajęte innymi kartami rozszerzeń (ewentualna inna/dwuslotowa karta rozszerzeń uniemożliwiająca obsadzenie kartą dodatkowego slotu eliminuje ten slot z użytku)
Dodatkowe porty	• z przodu obudowy: , 1x USB 2.0, 1x DB-15 video. • z tyłu obudowy: 2x USB 3.0, , 1x DB-15
Chłodzenie	Wentylatory wspierające wymianę Hot-Swap, zamontowane nadmiarowo minimum N+1
Zarządzanie	• Zintegrowany z płytą główną serwera, niezależny od systemu operacyjnego, sprzętowy kontroler zdalnego zarządzania • Monitoring statusu i zdrowia systemu • Logowanie zdarzeń • Umożliwiający Update systemowego firmware • Umożliwiający zdalną konfigurację serwera • Monitoring i możliwość ograniczenia poboru prądu • Zdalne włączanie/wyłączanie/restart • Zdalny dostęp do serwera • Możliwość zdalnej instalacji systemu operacyjnego • Alerty Syslog • Przekierowanie konsoli szeregowej przez SSH • Wyświetlanie danych aktualnych I historycznych dla użycia energii I temperatury serwera
Funkcje zabezpieczeń	Hasło włączania, hasło administratora, moduł TPM. Opcjonalny zamykany panel przedni serwera.
Urządzenia hot swap	Dyski twarde, zasilacze oraz wentylatory
Wspierane Systemy operacyjne	Microsoft Windows Server 2012 R2, 2016 oraz 2019; Red Hat Enterprise Linux 6 (x64) oraz 7; SUSE Linux Enterprise Server 11 (x64), 12, i 15; VMware vSphere (ESXi) 6.0, 6.5, oraz 6.7.
Oprogramowanie do monitorowania i nadzorowania sieci	Wymogi ogólne: a) Oprogramowanie powinno posiadać budowę modułową i składać się z serwera zarządzającego, zdalnych konsoli oraz Agentów. Komunikacja pomiędzy Serwerem a Agentami i Konsolami powinna być nawiązywana przy użyciu szyfrowanego protokołu (TLS lub SSL). Moduły muszą umożliwiać kompleksowy monitoring sieci, monitoring sprzętu komputerowego na stanowiskach użytkowników pod kątem zmian sprzętowych i programowych oraz pomoc w formie interaktywnego połączenia sieciowego z obsługiwanym użytkownikiem. Instalacja Serwera oraz Konsol zarządzających wymaga 64-bitowego systemu operacyjnego Windows. b) Dane, które dotyczą działań pracownika na komputerze, a więc: historia aktywności, polityka korzystania z Internetu oraz aplikacji, dostęp do zewnętrznych nośników danych itp., powinny być odseparowane od danych stricte technicznych tj. informacji o stacji roboczej. Powinny one być również grupowane w osobnym, dedykowanym oknie, aby możliwe było, zgodne z RODO, usuwanie danych wybranego użytkownika bez konieczności usunięcia informacji o stacji roboczej. c) Dostęp do danych osobowych oraz danych z monitoringu, zgodnie z RODO, powinien być objęty kontrolą na poziomie wybranych Administratorów – w programie powinna być możliwość nadawania kontom administracyjnym różnych poziomów dostępu oraz uprawnień zarówno do grup urządzeń, jak i użytkowników. Działania administratorów powinny być logowane oznacza to, że program musi posiadać dziennik z listą czynności wykonanych przez administratorów, które zmodyfikowały obiekty znajdujące się w systemie.

	d) Oprogramowanie powinno posiadać obszar funkcjonalny w formie platformy WWW, który pozwala na tworzenie wielu interaktywnych paneli informacyjnych (dashboardów) z responsywnymi widgetami. Na każdym z dashboardów widgety powinny móc być rozłożone na siatce o rozmiarze ustalonym przez administratora. Obszar pozwala na wyświetlanie danych z całego systemu. Oprogramowanie powinno umożliwiać zarządzanie 35 stacjami roboczymi - Program powinien być dostępny w języku polskim i angielskim wraz z podręcznikiem użytkownika w formie strony internetowej. Należy podać link do strony zawierającej podręcznik użytkownika. - Serwer bazy danych, na której działają wszystkie oferowane moduły powinien umożliwiać pracę dla nieograniczonej ilości użytkowników oraz nielimitowanej pojemności bazy. Należy wskazać nazwę bazy danych dla oferowanego rozwiązania uwzględniając powyższe wymogi. - Wymogi dotyczące poszczególnych funkcji **MONITOROWANIE INFRASTRUKTURY** (BEZAGENTOWO) musi obejmować serwery Windows, Linux, Unix, Mac; routery, przełączniki, urządzenia VoIP i firewalle w zakresie: • wykrywania urządzeń w sieci poprzez skanowanie ping (oraz arp-ping). • wizualizacji stanu urządzeń w postaci ikon urządzeń na mapach sieci. • wizualizacji połączeń pomiędzy urządzeniami a przełącznikami i informacji, do którego portu przełącznika podłączone jest dane urządzenie. • wizualizacji map urządzeń poprzez tworzenie spersonalizowanych map z wykorzystaniem jako tła zaimportowanych obrazków • serwisów TCP/IP, HTTP, POP3, SMTP, FTP i innych wraz z możliwością definiowania własnych serwisów. Program monitoruje czas ich odpowiedzi i procent utraconych pakietów. • zablokowania mapy urządzeń przed przypadkową edycją. • serwerów pocztowych: o program powinien monitorować zarówno serwis odbierający, jak i wysyłający pocztę, o program powinien mieć możliwość monitorowania stanu systemów i wysyłania powiadomienia (e-mail, SMS i inne), w razie gdyby przestały one odpowiadać lub funkcjonowały wadliwie (np. gdy ważne parametry znajdą się poza zakresem), o program powinien posiadać możliwość wykonywania operacji testowych, o program powinien wysyłać powiadomienia, jeśli serwer pocztowy nie działa. • monitorowania serwerów WWW i adresów URL. • obsługi szyfrowania SSL/TLS w powiadomieniach e-mail. • obsługi urządzeń SNMP wspierających SNMP v1/2/3 (np. przełączniki, routery, drukarki sieciowe, urządzenia VoIP itp.) za pomocą nazw. • szyfrowania AES, DES i 3DES dla protokołu SNMPv3, • obsługi komunikatów syslog, pułapek SNMP i ewidencjonowanie odebranych z nich danych, • monitoringu routerów i przełączników wg: o zmian stanu interfejsów sieciowych, o ruchu sieciowego, o podłączonych stacji roboczych, o ruchu generowanego przez podłączone stacje robocze • Program powinien posiadać własny, wbudowany kompilator plików MIB umożliwiający dodawanie definicji dla modułów SNMP • serwisów Windows: monitor serwisów Windows powinien informować gdy serwis przestanie działać oraz pozwalać na jego uruchomienie/zatrzymanie/zrestartowanie. • wydajności systemów Windows: o obciążenie CPU, pamięci, zajętość dysków, transfer sieciowy. Program powinien posiadać Inteligentne Mapy i Oddziały/Jednostki organizacyjne, które służą do lepszego zarządzania logiczną strukturą urządzeń w przedsiębiorstwie (Oddziały/Jednostki organizacyjne) oraz tworzą dynamiczne mapy wg własnych filtrów (Mapy Inteligentne).

	INWENTARYZACJA - program powinien automatycznie gromadzić informacje o sprzęcie i oprogramowaniu na stacjach roboczych oraz: • Prezentować szczegóły dotyczące sprzętu: modelu, procesora, pamięci, płyty głównej, napędów, kart itp. • Obejmować m.in.: zestawienie posiadanych konfiguracji sprzętowych, wolne miejsce na dyskach, średnie wykorzystanie pamięci, informacje pozwalające na wytypowanie systemów, dla których konieczny jest upgrade. • Informować o zainstalowanych aplikacjach oraz aktualizacjach Windows, co bezpośrednio umożliwia audytowanie i weryfikację użytkowania licencji w organizacji. • Zbierać informacje w zakresie wszystkich zmian przeprowadzonych na wybranej stacji roboczej: instalacji/deinstalacji aplikacji, zmian adresu IP itd. • Posiadać możliwość wysyłania powiadomienia np. e-mailem w przypadku zainstalowania programu lub jakiejkolwiek zmiany konfiguracji sprzętowej komputera. • Umożliwiać odczytanie numeru seryjnego (klucze licencyjne). • Umożliwiać automatyczne zarządzanie instalacjami i deinstalacjami oprogramowania poprzez określenie paczek aplikacji wymaganych oraz nieautoryzowanych. • Umożliwiać przegląd informacji o konfiguracji systemu, np. komend startowych, zmiennych środowiskowych, kontach lokalnych użytkowników, harmonogramie zadań itp. • Umożliwia utworzenie listy plików użytkowników z określonym rozszerzeniem (np. filmy .AVI) znalezionych na stacjach roboczych oraz ich zdalne usuwanie wraz z wykrywaniem metadanych plików użytkownika: obrazów (wymiary obrazka), video (długość filmu), audio (długość nagrania), archiwów (liczba plików w środku, rozmiar po wypakowaniu). 10. • Umożliwia wymianę plików do i ze stacją roboczą poprzez funkcję Menedżera plików. Działania administratorów wykonywane w tej funkcji są logowane. **Moduł inwentaryzacji** sprzętu powinien umożliwiać prowadzenie bazy ewidencji majątku IT w zakresie: • przechowywania wszystkich informacji dotyczących infrastruktury IT w jednym miejscu oraz automatycznego aktualizowania zgromadzonych informacji, • definiowania własnych typów (elementów wyposażenia), ich atrybutów oraz wartości – dla danego urządzenia lub oprogramowania istnieje możliwość dodawania dodatkowych informacji, np. numer inwentarzowy, osoba odpowiedzialna, numer i skan faktury zakupu, wartość sprzętu lub oprogramowania, nazwa sprzedawcy, termin upływu i skan gwarancji, termin kolejnego przeglądu (można podać datę, po której administrator otrzyma powiadomienie o zbliżającym się terminie przeglądu lub upływie gwarancji), nazwa firmy serwisującej, inny dowolny załącznik (np. plik .DOCX, .XLSX, .PDF), skan dowolnego dokumentu, czy też własny komentarz; dodatkowo powinien istnieć możliwość importu danych z zewnętrznego źródła (.CSV), • generowania zestawienia wszystkich środków trwałych, w tym urządzeń i zainstalowanego na nich oprogramowania, • archiwizacji i porównywania audytów środków trwałych, • tworzenia kodów kreskowych w Środkach Trwałych, • drukowania kodów kreskowych oraz dwuwymiarowych kodów alfanumerycznych (QR Code) dla środków trwałych, które posiadają numer inwentarzowy, • inwentaryzacji sprzętu posiadającego kody kreskowe za pomocą aplikacji mobilnej na system Android, • inwentaryzacji stacji roboczych niepodłączonych do sieci (bez instalacji Agenta poprzez manualne wykonanie skanów inwentaryzacji offline). • określenia atrybutów wymaganych, które są obowiązkowe dla wszystkich zasobów, • określenia atrybutów dodatkowych tylko dla wybranych typów zasobów • definiowanie własnych list jednokrotnego wyboru jako dodatkowe informacje o zasobie, Inwentaryzacja oprogramowania powinna zapewniać funkcjonalność w zakresie pozyskiwania informacji o oprogramowaniu i audycie licencji poprzez: • Skanowanie plików wykonywalnych i multimedialnych na stacjach roboczych, skanowanie archiwów ZIP.

	• Informacje o aplikacjach używanych w organizacji. • Tworzenie własnych wzorców aplikacji. • Tworzenie dowolnych kategorii aplikacji, np. nowe, zabronione, projektowe itp. • Informacje o komputerach, na których aplikacja została wykryta. • Zarządzanie posiadanymi licencjami. • Wskazywanie osób odpowiedzialnych za licencję. • Wskazanie użytkowników licencji. • Tworzenia powiązań między licencjami a dokumentami w relacji 1:N. • Rozbudowane zarządzanie licencjami poprzez: przypisywanie do użytkownika, przypisywanie do wielu komputerów tego samego użytkownika, przypisywanie wg numerów seryjnych, przypisywanie wg różnych wersji aplikacji na jednym urządzeniu. • Łatwy audyt legalności oprogramowania oraz powiadamianie tylko w razie przekroczenia liczby posiadanych licencji - w każdej chwili istnieje możliwość wykonania aktualnych raportów audytowych. • Zarządzanie posiadanymi licencjami: raport zgodności licencji. Możliwość przypisania do programów numerów seryjnych, wartości itp. Okna audytowe powinny posiadać możliwość filtrowania elementów per jednostka organizacyjna **Moduł wydajności czasu pracy** – program powinien wspierać zarządzanie czasem i analizować aktywność użytkowników poprzez dostarczenie informacji o czasie poświęconym na pracę w poszczególnych aplikacjach i na stronach WWW z dowolnie wybranego okresu. System powinien umożliwić każdemu pracownikowi organizacji dostęp do własnych wskaźników aktywności. Menedżerowie oraz przełożeni mogą uzyskać automatyczny dostęp do aktywności podwładnych w zespołach i indywidualnie oraz mogą przeanalizować aktywności w danym okresie i zyskać pełny obraz obszarów wymagających największego zaangażowania. Dodatkowo moduł gromadzi oraz prezentuje w formie strony www: • Statystyki czasu pracy i osobistej aktywności w wybranym przedziale czasu. • Statystyki aktywności grupy i jej członków widoczne dla menedżera grupy. • Statystyki aktywności podwładnych widoczne dla przełożonego. • Listy odwiedzanych stron internetowych i aplikacji wraz ze spędzonym na nich czasem. • Podglądy list użytkowników korzystających z wybranej aplikacji we wskazanym zakresie czasu. • Statystyki popularności stron i aplikacji w organizacji, grupie i u poszczególnych użytkowników. • Oceny produktywności użytkownika na podstawie czasu spędzonego w aplikacjach i na stronach internetowych. • Grupowanie stron internetowych i aplikacji z podziałem na: produktywne, neutralne i nieproduktywne. **ZDALNA POMOC UŻYTKOWNIKOM** - w ramach kontroli stacji użytkownika powinien być dostępny podgląd pulpitu użytkownika i możliwość przejęcia nad nim kontroli. Podczas dostępu zdalnego, zarówno użytkownik jak i administrator muszą widzieć ten sam ekran. Administrator w trakcie zdalnego dostępu będzie mieć możliwość zablokowania działania myszy oraz klawiatury dla użytkownika. W niniejszym module musi znaleźć się baza zgłoszeń umożliwiająca użytkownikom zgłaszanie problemów technicznych, które z kolei będą przetwarzane i przyporządkowywane odpowiednim administratorom, otrzymującym automatycznie powiadomienie o przypisanym im problemie. Użytkownik powinien mieć możliwość monitorowania procesu rozwiązywania zgłoszonych problemów i ich aktualnych statusów, jak również możliwość wymiany informacji z administratorem poprzez komentarze, które będą wpisywane i widoczne dla obu stron. Moduł ten powinien zawierać również komunikator (czat), który umożliwia przesyłanie wiadomości pomiędzy zalogowanymi użytkownikami i administratorami (wraz z wyszukiwarką wiadomości) oraz bazę wiedzy pomagającą użytkownikom samodzielnie rozwiązywać najprostsze, powtarzające się problemy.

	Moduł pomocy zdalnej będzie umożliwiać również: • pobieranie listy użytkowników z Active Directory, • zarządzanie dostępem pracowników HelpDesku do zgłoszeń poprzez rozbudowany system zarządzania regułami widoczności zgłoszeń, • zarządzanie dostępem do czatu w 3 poziomach uprawnień: pełny dostęp, brak dostępu lub dostęp ograniczony wyłącznie do pomocy technicznej, • tworzenie własnego drzewa kategorii zgłoszeń wraz z możliwością grupowania kategorii w folderach (do 4 poziomów kategorii), • automatyczne przypisywanie konkretnych pracowników helpdesk do zgłoszeń w określonych kategoriach lub pochodzących od określonych grup użytkowników, • procesowanie zgłoszeń użytkowników z wiadomości e-mail, • tworzenie formularzy z niestandardowymi polami opisowymi, dedykowanymi do wybranych kategorii zgłoszeń, • wykonywanie operacji na wielu zgłoszeniach równocześnie, • dołączanie załączników do zgłoszeń, • rozbudowane wyszukiwanie zgłoszeń i artykułów w bazie wiedzy, • szybki dostęp do ostatnich zgłoszeń, artykułów bazy wiedzy i załączników, • wprowadzenie komentarza oraz informacji o czasie poświęconym na rozwiązanie w kreatorze wyświetlanym przy zamykaniu zgłoszenia, • zrzuty ekranowe (podgląd pulpitu), • dystrybucję oprogramowania przez Agenty, • dystrybucję oraz uruchamianie plików za pomocą Agentów (w tym plików MSI), • zadania dystrybucji plików, jeśli komputer jest wyłączony w trakcie zlecania operacji następuje kolejkowanie zadania dystrybucji pliku, • zarządzania procesami systemu Windows (w zakresie: zakończ proces, zakończ drzewo procesu, uruchom nowy proces w sesji użytkownika wraz z parametrami), • wymiany plików do i ze stacji roboczej poprzez funkcję Menedżera plików
Waga	maximum: 35 kg
Gwarancja	Min. 3 lata naprawa na miejscu u klienta, uszkodzony dysk zostaje u zamawiającego, czas reakcji serwisu NBD

3. Serwer – 1 szt.

Funkcjonalność/minimalne parametry techniczne/zakres prac:

Dostarczenie serwera do Backupu z zainstalowanym oprogramowaniem
Oferent powinien uwzględnić koszty wdrożenia i uruchomienia oprogramowania.

Serwer	
Nazwa komponentu	**Wymagane minimalne parametry techniczne**
Obudowa	Wolnostojąca Tower , wysokość nie więcej niż 5U, z zestawem szyn do mocowania w szafie i wysuwania do celów serwisowych, wyposażona w zestaw ułatwiający wyprowadzenie przewodów z tyłu serwera.
Procesor	Architektura x86, maksymalny TDP dla procesora – 85W. Minimalna ilość rdzeni dla procesora – 8. Wynik wydajności procesora instalowanego w oferowanym serwerze powinien przekraczać 110 punktów peak w SPEC w teście SPEC CPU2017 Integer Rates opublikowanych przez SPEC.org (www.spec.org) dla konfiguracji dwuprocesorowej. Test przeprowadzony przez producenta serwera musi być zamieszczony na stronie spec.org. Obsługa minimum dwóch procesorów.
Liczba procesorów	Min. 1
Płyta główna	Płyta główna dedykowana do pracy w serwerach, wyprodukowana przez producenta serwera z możliwością zainstalowania do dwóch procesorów

Pamięć operacyjna	Minimum zainstalowane 64GB pamięci RAM Minimum 16 sloty na pamięć, wsparcie pamięci typu RDIMM oraz LRDIMM. Możliwość instalacji minimum 1 TB Ram Pamięć o częstotliwości minimum 2666MHz.
Zabezpieczenie pamięci	ECC
Procesor Graficzny	Zintegrowana karta graficzna z minimum 16MB pamięci osiągająca rozdzielczość 1920x1200 przy 60 Hz. 2 porty VGA (z przodu i z tyłu).
Dyski	Zainstalowane dyski: min. 2 x 600 GB SAS 10k min 5 x 8TB 7,2k RPM SAS
Kontroler dyskowy	Zintegrowany na płycie kontroler SATA Zainstalowany kontroler RAID 2GB
Zasilacz	Minimum dwa redundantne zasilacze o mocy minimum 600W
Interfejsy sieciowe	Min. 2 interfejsy 10GbE Min. 2 interfejsy 1x GbE
Dodatkowe sloty I/O	Na płycie min 3 slotów PCI Sloty muszą być dostępne dla użytkownika – tj. niezajęte innymi kartami rozszerzeń (ewentualna inna/dwuslotowa karta rozszerzeń uniemożliwiająca obsadzenie kartą dodatkowego slotu eliminuje ten slot z użytku)
Dodatkowe porty	• 8 x USB , 1x DB-15 video.
Zarządzanie	• Zintegrowany z płytą główną serwera, niezależny od systemu operacyjnego, sprzętowy kontroler zdalnego zarządzania • Monitoring statusu i zdrowia systemu • Logowanie zdarzeń • Umożliwiający Update systemowego firmware • Umożliwiający zdalną konfigurację serwera • Monitoring i możliwość ograniczenia poboru prądu • Zdalne włączanie/wyłączanie/restart • Zdalny dostęp do serwera • Możliwość zdalnej instalacji systemu operacyjnego • Alerty Syslog • Przekierowanie konsoli szeregowej przez SSH • Wyświetlanie danych aktualnych I historycznych dla użycia energii I temperatury serwera
Funkcje zabezpieczeń	Hasło włączania, hasło administratora, moduł TPM. Opcjonalny zamykany panel przedni serwera.
Urządzenia hot swap	Dyski twarde, zasilacze oraz wentylatory
Wspierane Systemy operacyjne	Microsoft Windows Server 2012 R2, 2016 oraz 2019; Red Hat Enterprise Linux 6 (x64) oraz 7; SUSE Linux Enterprise Server 11 (x64), 12, i 15; VMware vSphere (ESXi) 6.0, 6.5, oraz 6.7.
Zainstalowany System Operacyjny (SSO)	Licencja ma mieć charakter wieczysty i nie narażać Zamawiającego na dodatkowe koszty w przyszłym użytkowaniu. Licencja ma uprawniać do uruchamiania SSO w środowisku fizycznym i dwóch wirtualnych środowisk systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji. Serwerowy system operacyjny (dalej: SSO) posiada następujące, wbudowane cechy: - Posiada możliwość wykorzystania 320 logicznych procesorów oraz 4 TB pamięci RAM w środowisku fizycznym - Posiada możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności 64TB przez każdy wirtualny serwerowy system operacyjny.

- Posiada możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania do 7000 maszyn wirtualnych.
- Posiada możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.
- Posiada wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.
- Posiada wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.
- Posiada automatyczną weryfikację cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
- Posiada możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy.
- Wbudowane wsparcie instalacji i pracy na wolumenach, które:

pozwalają na zmianę rozmiaru w czasie pracy systemu,

- umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
- umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,
- umożliwiają zdefiniowanie list kontroli dostępu (ACL),
- Posiada wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
- Posiada wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
- Posiada możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET.
- Posiada możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
- Posiada wbudowaną zaporę internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
- Graficzny interfejs użytkownika.
- Zlokalizowane w języku polskim, następujące elementy:

• menu,
• przeglądarka internetowa,
• pomoc,
• komunikaty systemowe.

- Posiada wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
- Posiada możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
- Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
- Pochodzący od producenta systemu serwis zarządzania polityką konsumpcji informacji w dokumentach (Digital Rights Management).
- Posiada możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
- Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,
- Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:

- Podłączenie SSO do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,
- Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
- Zdalna dystrybucja oprogramowania na stacje robocze.

	Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające: Dystrybucję certyfikatów poprzez http Konsolidację CA dla wielu lasów domeny, Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen. Szyfrowanie plików i folderów. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec). Posiada możliwość tworzenia systemów wysokiej dostępności (klastry typu failover) oraz rozłożenia obciążenia serwerów. Serwis udostępniania stron WWW. Wsparcie dla protokołu IP w wersji 6 (IPv6), Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows, Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtulne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji zapewniają wsparcie dla: Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych, Obsługi ramek typu jumbo frames dla maszyn wirtualnych, Obsługi 4-KB sektorów dysków, Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra, Posiada możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk model) Posiada możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta SSO umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet. Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath). Posiada możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego. Posiada mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
Oprogramowanie backupowe	Oprogramowanie do backup 20 systemów wirtualnych lub fizycznych ze wsparciem na 3 lata. Zamawiający dopuszcza oprogramowania w formie subskrypcji **Wymagania ogólne** • Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 6.0, 6.5 oraz 6.7 oraz Microsoft Hyper-V 2012 R2 i 2019. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej • Oprogramowanie musi współpracować z hostami zarządzanymi przez VMware vCenter oraz pojedynczymi hostami. • Oprogramowanie musi współpracować z hostami zarządzanymi przez System Center Virtual Machine Manger, klastrami hostów oraz pojedynczymi hostami. • Oprogramowanie musi zapewniać tworzenie kopii zapasowych wszystkich systemów operacyjnych maszyn wirtualnych wspieranych przez vSphere i Hyper-V

	• Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux. **Całkowite koszty posiadania** • Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej • Oprogramowanie musi tworzyć “samowystarczalne” archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków • Oprogramowanie musi pozwalać na tworzenie kopii zapasowych w trybach: Pełny, pełny syntetyczny, przyrostowy i odwrotnie przyrostowy (tzw. reverse-inremental) • Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji • Oprogramowanie musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć jedną wirtualną pulę pamięci na kopie zapasowe. Wymagane jest wsparcie dla co najmniej trzech pamięci masowych w takiej puli. • Oprogramowanie musi pozwalać na rozszerzenie lokalnej przestrzeni backupowej poprzez integrację z Microsoft Azure Blob, Amazon S3 oraz z innymi kompatybilnymi z S3 macierzami obiektowymi. Proces migracji danych powinien być zautomatyzowany. Jedynie unikalne bloki mogą być przesyłane w celu oszczędności pasma oraz przestrzeni na przechowywane dane. Funkcjonalność ta nie może mieć wpływu na możliwości odtwarzania danych. • Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu. • Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania • Oprogramowanie musi mieć możliwość uruchamiania dowolnych skryptów przed i po zadaniu backupowym lub przed i po wykonaniu zadania snapshota. • Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL oraz Oracle (w tym odtwarzanie point-in-time) • Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji • Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji • Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania • Oprogramowanie musi wspierać backup maszyn wirtualnych używających współdzielonych dysków VHDX na Hyper-V (shared VHDX) • Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych. **Wymagania RPO** • Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej

	• Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta musi być dostępna na wszystkich wspieranych platformach wirtualizacyjnych • Oprogramowanie musi automatycznie wykrywać i usuwać snapshoty-sieroty (orphaned snapshots), które mogą zakłócić poprawne wykonanie backupu. Proces ten nie może wymagać interakcji administratora • Oprogramowanie musi posiadać wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją VMware. • Oprogramowanie musi wspierać kopiowanie backupów na taśmy wraz z pełnym śledzeniem wirtualnych maszyn • Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son) • Oprogramowanie musi umieć korzystać z protokołu DDBOOST w przypadku, gdy repozytorium backupów jest umiejscowione na Dell EMC DataDomain. Funkcjonalność powinna wspierać łącze sieciowe lub FC. • Oprogramowanie musi umieć korzystać z protokołu Catalyst (w tym Catalyst Copy) w przypadku, gdy repozytorium backupów jest umiejscowione na HPE StoreOnce. Funkcjonalność powinna wspierać łącze sieciowe lub FC. • Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016 lub 2019 z systemem pliku ReFS jako repozytorium backupu. Podobna funkcjonalność musi być zapewniona dla repozytoriów opartych o linuxowy system plików XFS. • Oprogramowanie musi mieć możliwość replikacji włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere, pomiędzy hostami ESXi, włączając asynchroniczną replikacją ciągłą. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji. • Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik • Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding) • Oprogramowanie musi posiadać takie same funkcjonalności replikacji dla Hyper-V • Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN) • Oprogramowanie musi dawać możliwość tworzenia backupów ad-hoc z konsoli jak i z klienta webowego vSphere • Oprogramowanie musi przetwarzać wiele wirtualnych dysków jednocześnie (parallel processing) **Wymagania RTO** • Oprogramowanie musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware oraz Hyper-V niezależnie od rodzaju storage'u użytego do przechowywania kopii zapasowych. • Dodatkowo dla środowiska vSphere powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna) • Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w hypervisor. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie musi realizować taką migrację swoimi mechanizmami • Oprogramowanie musi pozwalać na zaprezentowanie

	pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSpehre • Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków • Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack oraz Amazon EC2. • Oprogramowanie musi umożliwić odtworzenie plików na maszynę operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików • Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy VIX API dla platformy VMware i PowerShell Direct dla platformy Hyper-V. • Oprogramowanie musi wspierać odtwarzanie plików z następujących systemów plików: o **Linux** ▪ ext2, ext3, ext4, ReiserFS, JFS, XFS, Btrfs o **BSD** ▪ UFS, UFS2 o **Solaris** ▪ ZFS, UFS o **Mac** ▪ HFS, HFS+ o **Windows** ▪ NTFS, FAT, FAT32, ReFS o **Novell OES** ▪ NSS • Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM oraz Windows Storage Spaces. • Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej. • Oprogramowanie musi wspierać granularne odtwarzanie dowolnych obiektów i dowolnych atrybutów Active Directory włączając hasło, obiekty Group Policy, partycja konfiguracji AD, rekordy DNS zintegrowane z AD, Microsoft System Objects, certyfikaty CA oraz elementy AD Sites. • Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2010 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects"), • Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2005 i nowsze włączając bazy danych z opcją odtwarzania point-in-time, tabele, schemat • Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2010 i nowsze. Opcja odtworzenia elementów, witryn, uprawnień. • Oprogramowanie musi wspierać granularne odtwarzanie baz danych Oracle z opcją odtwarzanie point-in-time wraz z

	włączonym Oracle DataGuard. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Windows oraz Linux. • Oprogramowanie musi pozwalać na zaprezentowanie baz MS SQL oraz Oracle bezpośrednio z pliku kopii zapasowej do działającego serwera bazodanowego • Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN **Ograniczenie ryzyka** • Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu. • Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem • Oprogramowanie musi mieć podobne mechanizmy dla replik w środowisku vSphere • Oprogramowanie musi umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem jakichkolwiek danych. Integracja musi być zapewniona minimalnie dla Windows Defender, Symantec Protection Engine oraz ESET NOD32. • Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego.
Waga	maximum: 35 kg
Gwarancja	Min. 2 lata naprawa na miejscu u klienta, uszkodzony dysk zostaje u zamawiającego, czas reakcji serwisu NBD

4. Firewall – 1 szt.

Funkcjonalność/minimalne parametry techniczne/zakres prac:

Firewall	
Nazwa komponentu	**Wymagane minimalne parametry techniczne**
Wymagania Ogólne	Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu. System musi wspierać IPv4 oraz IPv6 w zakresie: • Firewall. • Ochrony w warstwie aplikacji. • Protokołów routingu dynamicznego.

Redundancja, monitoring i wykrywanie awarii	1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall. 2. W ramach postępowania system musi zostać dostarczony w postaci redundantnej. 3. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. 4. Monitoring stanu realizowanych połączeń VPN.
Interfejsy, Dysk, Zasilanie:	1. System realizujący funkcję Firewall musi dysponować minimum: • 18 portami Gigabit Ethernet RJ-45. • 8 gniazdami SFP 1 Gbps. • 4 gniazdami SFP+ 10 Gbps. 2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. 3. System musi być wyposażony w zasilanie AC.
Parametry wydajnościowe:	1. W zakresie Firewall'a obsługa nie mniej niż 3 mln. jednoczesnych połączeń oraz 260 tys. nowych połączeń na sekundę. 2. Przepustowość Stateful Firewall: nie mniej niż 13 Gbps dla pakietów 512 B. 3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 13 Gbps. 4. Wydajność szyfrowania IPSec VPN nie mniej niż 12 Gbps. 5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 3 Gbps. 6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 3 Gbps. 7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 3 Gbps.
Funkcje Systemu Bezpieczeństwa:	W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych: 1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. 2. Kontrola Aplikacji. 3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. 4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS. 5. Ochrona przed atakami - Intrusion Prevention System. 6. Kontrola stron WWW. 7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3. 8. Zarządzanie pasmem (QoS, Traffic shaping). 9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). 10. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. 11. Analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2. 12. Funkcja lokalnego serwera DNS ze wsparciem dla DNS over TLS (DoT) oraz DNS over HTTPS (DoH) z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system. 13. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje

	zabezpieczeń, rejestrowanie zdarzeń. 14. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz: • Translację jeden do jeden oraz jeden do wielu. • Dedykowany ALG (Application Level Gateway) dla protokołu SIP. 15. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. 16. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików. 17. Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu. • Amazon Web Services (AWS). • Microsoft Azure • Google Cloud Platform (GCP). • OpenStack. • VMware NSX.
Połączenia VPN	1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać: • Wsparcie dla IKE v1 oraz v2. • Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM). • Obsługa protokołu Diffie-Hellman grup 19 i 20. • Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE. • Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. • Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. • Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. • Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth. • Mechanizm „Split tunneling” dla połączeń Client-to-Site. 2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać: • Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0. • Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta. • Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.
Routing i obsługa łączy WAN	1. W zakresie routingu rozwiązanie powinno zapewniać obsługę: • Routingu statycznego. • Policy Based Routingu. • Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.
Funkcje SD-WAN	1. System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN. 2. Reguły SD-WAN powinny umożliwiać określenie aplikacji jako argumentu dla kierowania ruchu.
Zarządzanie pasmem	1. System Firewall musi umożliwiać zarządzanie pasmem poprzez

	określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. 2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji. 3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.
Ochrona przed malware	1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). 2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR. 3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). 4. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze. 5. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików. 6. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.
Ochrona przed atakami	1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. 2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach./Baza sygnatur ataków powinna zawierać minimum 2000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 3. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur. 4. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. 5. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies. 6. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
Kontrola aplikacji	1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. 2. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. 3. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. 4. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur
Kontrola WWW	1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. 2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. 3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard. 4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.

	5. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo. 6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania. 7. W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych url - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.
Uwierzytelnianie użytkowników w ramach sesji	1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą: • Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. • Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. • Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych. 2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego. 3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API. 4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.
Zarządzanie	1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania. 2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów. 3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. 4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow. 5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. 6. Element systemu pełniący funkcję Firewall musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. 7. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.
Logowanie	1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. 2. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. 3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu. 4. Musi istnieć możliwość logowania do serwera SYSLOG.

Certyfikaty	Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje: • ICSA lub EAL4 dla funkcji Firewall.
Serwisy i licencje	W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować: a) Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox,
Gwarancja oraz wsparcie	Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne
Opisy do wymagań ogólnych	1. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania. 2. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

5. Komputer PC 5 szt.

Wymagane jest dostarczenie 5 sztuk komputerów spełniających poniżej opisane minimalne parametry funkcjonalne:

Nazwa komponentu	Wymagane parametry techniczne komputerów
Typ	Komputer stacjonarny. W ofercie wymagane jest podanie modelu, symbolu oraz producenta.
Zastosowanie	Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna.
Procesor	Procesor dedykowany do pracy w komputerach stacjonarnych. Procesor osiągający w teście Passmark CPU Mark, w kategorii Average CPU Mark wynik co najmniej 10000 pkt. według wyników opublikowanych na stronie http://www.cpubenchmark.net/cpu_list.php
Pamięć RAM	8GB DDR4 2666MHz. Możliwość rozbudowy do min 64GB. Jeden slot DIMM wolny.
Pamięć masowa	Dysk 2.5” 512GB HDD
Wydajność grafiki	Zintegrowana karta graficzna osiągająca w teście Passmark G3D Mark, w kategorii Average G3D Mark wynik co najmniej XXX pkt. według wyników opublikowanych na stronie https://www.videocardbenchmark.net/gpu_list.php w dniu XXX.
Wyposażenie multimedialne	Karta dźwiękowa min. czterokanałowa zintegrowana z płytą główną, zgodna z High Definition, wewnętrzny głośnik w obudowie komputera. Port słuchawek i mikrofonu na przednim panelu, dopuszcza się rozwiązanie port combo, na tylnym panelu min. port audio line out.
Obudowa	Typu Small Form Factor z obsługą kart wyłącznie o niskim profilu. Umożliwiająca montaż 1 x dysku 3.5” lub 1 x dysku 2.5” wewnątrz obudowy. Obudowa fabrycznie przystosowana do pracy w orientacji poziomej i pionowej. Otwory wentylacyjne usytuowane wyłącznie na przednim oraz tylnym panelu obudowy. Suma wymiarów obudowy nieprzekraczająca 700 mm. Zasilacz o mocy min. 200W pracujący w sieci 230V 50/60Hz prądu zmiennego i efektywności min. 85% przy obciążeniu zasilacza na poziomie 50% oraz o efektywności min. 82% przy obciążeniu zasilacza na poziomie 100%, Zasilacz w oferowanym komputerze musi się znajdować na stronie http://www.plugloadsolutions.com/80pluspowersupplies.aspx, do oferty należy dołączyć wydruk potwierdzający spełnienie wymogu 80plus, w przypadku, kiedy u producenta występuje kilka zasilaczy które są montowane na etapie produkcji w fabryce załączyć wydruki dla wszystkich zasilaczy. Wydruki 80plus musza być potwierdzone przez producenta lub dołączone oświadczenie producenta komputera, iż wskazane zasilacze przez wykonawcę spełniają 80plus. Moduł konstrukcji obudowy w jednostce centralnej komputera powinien pozwalać na demontaż kart rozszerzeń bez konieczności użycia narzędzi (wyklucza się użycia wkrętów, śrub motylkowych). Obudowa w jednostce centralnej musi być otwierana bez konieczności użycia narzędzi (wyklucza się użycie standardowych wkrętów, śrub motylkowych) oraz powinna posiadać czujnik otwarcia obudowy współpracujący z oprogramowaniem zarządzająco – diagnostycznym. Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej oraz kłódki (oczko w obudowie do założenia kłódki). Wbudowany wizualny system diagnostyczny oparty o sygnalizację LED np. włącznik POWER, służący do sygnalizowania i diagnozowania problemów z komputerem i jego komponentami, sygnalizacja oparta na zmianie statusów diody LED (zmiana barw oraz miganie). System usytuowany na przednim panelu. System diagnostyczny musi sygnalizować: uszkodzenie lub brak pamięci RAM, uszkodzenie płyty głównej, awarię BIOS’u, awarię procesora. Oferowany system diagnostyczny nie może wykorzystywać minimalnej ilości wolnych slotów na płycie głównej, wymaganych wnęk zewnętrznych w specyfikacji i dodatkowych oferowanych przez wykonawcę, oraz nie może być uzyskany przez konwertowanie, przerabianie innych złączy na płycie głównej nie wymienionych w specyfikacji a które nie są dedykowane dla systemu diagnostycznego. Każdy komputer powinien być oznaczony

	niepowtarzalnym numerem seryjnym umieszonym na obudowie, oraz musi być wpisany na stałe w BIOS.
Bezpieczeństwo	Ukryty w laminacie płyty głównej układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego. Próba usunięcia dedykowanego układu doprowadzi do uszkodzenia całej płyty głównej. System diagnostyczny z graficznym interfejsem użytkownika zaszyty w tej samej pamięci flash co BIOS, dostępny z poziomu szybkiego menu boot lub BIOS, umożliwiający przetestowanie komputera a w szczególności jego składowych. System zapewniający pełną funkcjonalność, a także zachowujący interfejs graficzny nawet w przypadku braku dysku twardego oraz jego uszkodzenia, nie wymagający stosowania zewnętrznych nośników pamięci masowej oraz dostępu do internetu i sieci lokalnej. Procedura POST traktowana jest jako oddzielna funkcjonalność.
BIOS	BIOS zgodny ze specyfikacją UEFI, wyprodukowany przez producenta komputera, zawierający logo producenta komputera lub nazwę producenta komputera lub nazwę modelu oferowanego komputera. Pełna obsługa BIOS za pomocą klawiatury i myszy oraz samej myszy. BIOS wyposażony w automatyczną detekcję zmiany konfiguracji, automatycznie nanoszący zmiany w konfiguracji w szczególności: procesor, wielkość pamięci, pojemność dysku. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera, bez dodatkowego oprogramowania (w tym również systemu diagnostycznego) i podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o: wersji BIOS, nr seryjnym komputera, ilości zainstalowanej pamięci RAM, prędkości zainstalowanych pamięci RAM, technologii wykonania pamięci, sposobie obsadzeniu slotów pamięci z rozbiciem na wielkości pamięci i banki, typie zainstalowanego procesora, ilości rdzeni zainstalowanego procesora, typowej prędkości zainstalowanego procesora, minimalnej i maksymalnej osiąganej prędkości zainstalowanego procesora, pojemności zainstalowanego lub zainstalowanych dysków twardych, wszystkich urządzeniach podpiętych do dostępnych na płycie głównej portów SATA, MAC adresie zintegrowanej karty sieciowej, zintegrowanym układzie graficznym, kontrolerze audio. Do odczytu wskazanych informacji nie mogą być stosowane rozwiązania oparte o pamięć masową (wewnętrzną lub zewnętrzną), zaimplementowane poza systemem BIOS narzędzia, np. system diagnostyczny, dodatkowe oprogramowanie. Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z zewnętrznych urządzeń, możliwość ustawienia hasła użytkownika umożliwiającego uruchomienie komputera (zabezpieczenie przed nieautoryzowanym uruchomieniem) przy jednoczesnym zdefiniowanym haśle administratora. Użytkownik po wpisaniu swojego hasła jest wstanie zidentyfikować ustawienia BIOS. Możliwość ustawienia haseł użytkownika i administratora składających się z cyfr, małych liter, dużych liter oraz znaków specjalnych. Możliwość włączenia/wyłączenia kontrolera SATA (w tym w szczególności pojedynczo), Możliwość ustawienia portów USB w trybie „no BOOT" (podczas startu komputer nie wykrywa urządzeń bootujących typu USB). Możliwość wyłączania portów USB pojedynczo. Możliwość dokonywania backup'u BIOS wraz z ustawieniami na dysku wewnętrznym. Oferowany BIOS musi posiadać poza swoją wewnętrzną strukturą menu szybkiego bootowania które umożliwia m.in.: uruchamianie systemu zainstalowanego na dysku twardym, uruchamianie systemu z urządzeń zewnętrznych, uruchamianie systemu z serwera za pośrednictwem zintegrowanej karty sieciowej, uruchomienie graficznego systemu diagnostycznego, wejście do BIOS, upgrade BIOS.
Wirtualizacja	Sprzętowe wsparcie technologii wirtualizacji realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji dla poszczególnych komponentów systemu).
Zgodność z systemami operacyjnymi i standardami	Oferowane modele komputerów muszą poprawnie współpracować z zamawianymi systemami operacyjnymi (jako potwierdzenie poprawnej współpracy Wykonawca dołączy do oferty dokument w postaci wydruku potwierdzający certyfikację rodziny produktów bez względu na rodzaj obudowy, dodatkowo potwierdzony przez producenta oferowanego komputera).
System operacyjny	Zainstalowany system operacyjny Windows 10 Professional, klucz licencyjny Windows 10 Professional musi być zapisany trwale w BIOS i umożliwiać

	instalację systemu operacyjnego zdalnie bez potrzeby ręcznego wpisywania klucza licencyjnego.
Certyfikaty i standardy	Certyfikat ISO9001 dla producenta sprzętu (załączyć dokument potwierdzający spełnianie wymogu) Deklaracja zgodności CE (załączyć do oferty) Urządzenia wyprodukowane są przez producenta, zgodnie z normą PN-EN ISO 50001 Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki (wg wytycznych Krajowej Agencji Poszanowania Energii S.A., zawartych w dokumencie „Opracowanie propozycji kryteriów środowiskowych dla produktów zużywających energię możliwych do wykorzystania przy formułowaniu specyfikacji na potrzeby zamówień publicznych", pkt. 3.4.2.1; dokument z grudnia 2006), w szczególności zgodności z normą ISO 1043-4 dla płyty głównej oraz elementów wykonanych z tworzyw sztucznych o masie powyżej 25 gram.
Wymagania dodatkowe	Wbudowane porty: • 1 x HDMI 1.4 • 1 x DisplayPort 1.4 • 1 x VGA • 1 x RS232 • 8 portów USB wyprowadzonych na zewnątrz obudowy, w układzie: o Panel przedni: 2 x USB 3.2 gen 1 Typu A oraz 2 x USB 2.0 o Panel tylny: 2 x USB 3.2 gen 1 Typu A oraz 2 x USB 2.0 • 1 x port audio typu combo (słuchawka/mikrofon) na przednim panelu • 1 x port audio-out na tylnym panelu obudowy • 1 x RJ – 45 Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) wszystkich portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek lub przewodów połączeniowych itp. Zainstalowane porty nie mogą blokować instalacji kart rozszerzeń w złączach wymaganych w opisie płyty głównej. Karta sieciowa 10/100/1000 zintegrowana z płytą główną, wspierająca obsługę WoL (funkcja włączana przez użytkownika), Płyta główna zaprojektowana i wyprodukowana na zlecenie producenta komputera, trwale oznaczona na etapie produkcji logiem producenta oferowanej jednostki, dedykowana dla danego urządzenia, wyposażona w: 1 x PCIe x16 Gen.3, 1 x PCIe x1, 2 x DIMM z obsługą do 64 GB DDR4 RAM, 2 x SATA w tym min. 1 szt SATA 3.0. Jedno złącze M.2 dla dysków oraz złącze M.2 bezprzewodowej karty sieciowej. Klawiatura USB w układzie polski programisty Mysz laserowa USB z sześcioma klawiszami oraz rolką (scroll) Opakowanie musi być wykonane z materiałów podlegających powtórnemu przetworzeniu.
Ergonomia	Głośność jednostki centralnej mierzona zgodnie z normą ISO 7779 oraz wykazana zgodnie z normą ISO 9296 w pozycji obserwatora w trybie pracy dysku twardego (IDLE) wynosząca maksymalnie **26** dB (załączyć oświadczenie producenta
Wsparcie techniczne producenta	Dedykowany portal techniczny producenta, umożliwiający Zamawiającemu zgłaszanie awarii oraz samodzielne zamawianie zamiennych komponentów. Możliwość sprawdzenia kompletnych danych o urządzeniu na jednej witrynie internetowej prowadzonej przez producenta (automatyczna identyfikacja komputera, konfiguracja fabryczna, konfiguracja bieżąca, Rodzaj gwarancji, data wygaśnięcia gwarancji, data produkcji komputera, aktualizacje, diagnostyka, dedykowane oprogramowanie, tworzenie dysku recovery systemu operacyjnego).
Warunki gwarancji	Gwarancja 3 lat NBD Firma serwisująca musi posiadać ISO 9001:2008 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty. Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. Wsparcie techniczne dla sprzętu będzie dostarczane zdalnie lub w miejscu instalacji urządzenia, w zależności od rodzaju zgłaszanej awarii. W przypadku awarii zakwalifikowanej jako naprawa w miejscu instalacji urządzenia, część zamienna wymagana do naprawy i/lub technik serwisowy przybędzie na

	miejsce wskazane przez klienta na następny dzień roboczy od momentu skutecznego przyjęcia zgłoszenia przez Dział Wsparcia Technicznego. Możliwość sprawdzenia aktualnego okresu i poziomu wsparcia technicznego dla urządzeń za pośrednictwem strony internetowej producenta. Możliwość pobrania aktualnych wersji sterowników oraz firmware urządzenia za pośrednictwem strony internetowej producenta również dla urządzeń z nieaktywnym wsparciem technicznym. Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.

Nazwa komponentu	Wymagane minimalne parametry techniczne monitora
Typ ekranu	Ekran ciekłokrystaliczny z aktywną matrycą IPS 24”
Rozmiar plamki (maksymalnie)	0,27 mm x 0,27 mm
Jasność	300 cd/m2
Kontrast	1000:1
Kąty widzenia (pion/poziom)	178/178 stopni
Czas reakcji matrycy (maksymalnie)	8ms (gray to gray) w trybie normal
Rozdzielczość maksymalna	1920 x 1200 przy 60Hz
Gama koloru	min. 99% sRGB
Częstotliwość odświeżania poziomego	30 – 83 kHz
Częstotliwość odświeżania pionowego	56 – 76 Hz
Pochylenie monitora	W zakresie 26 stopni
Wydłużenie w pionie	Tak, min 130 mm
PIVOT	Tak
Obrót lewo/prawo	Min. 90 stopni
Powłoka powierzchni ekranu	Antyodblaskowa
Podświetlenie	System podświetlenia LED
Zużycie energii	Typowo 18W, maksymalne 42W, czuwanie mniej niż 0,3W
Bezpieczeństwo	Monitor musi być wyposażony dedykowany slot na linkę zabezpieczającą
Waga bez podstawy	Maksymalnie 4kg
Waga z podstawą	Maksymalnie 6kg
Złącze	1x HDMI (v1.4), 1x DisplayPort (v1.2 1 x USB 3.0 1 x USB 2.0
Gwarancja	3 lata na miejscu u klienta Czas reakcji serwisu - do końca następnego dnia roboczego Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta komputera – dokumenty potwierdzające załączyć do oferty. Oświadczenie producenta komputera, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem. Gwarancja zero martwych pikseli
Certyfikaty	ISO 13406-2 lub ISO 9241, EPEAT Silver, Energy Star Monitor musi się znajdować na stronie TCO : http://tcocertified.com/product-finder/
Inne	Monitor musi posiadać trwałe oznaczenie logo producenta jednostki centralnej. Odłączany stand bez użycia narzędzi VESA 100mm.

6. Switch - 2 szt.

Wymagane jest dostarczenie 2 sztuk Switchów spełniających poniżej opisane minimalne parametry techniczne:

Nazwa komponentu	Wymagane minimalne parametry techniczne
Switch	Przełącznik wielowarstwowy L2/L3 Obsługa jakość serwisu (QoS) Konfigurowanie ustawień lokalizacji (CLI) Liczba portów (gniazd) RJ-45 Ethernet - 12 10G Ethernet (100/1000/10000) Liczba zainstalowanych modułów SFP- 3 Złącze światłowodowe QSFP28 Złącze zasilania Gniazdo wejściowe AC Sieć komputerowa Obsługa sieci VLAN Typ przełączników modułów optycznych - 100 Gigabit Ethernet Przepustowość rutowania/przełączania - 840 Gbit/s Przepustowość - 630 Mpps Latency (10-100 Mbps) - 2500 µs Funkcje Multicast Obsługa Multicast Możliwości montowania w stelażu Liczba wentylatorów - 3 wentylatory Do produktu dołączono zasilacz. Zasilacz dołączony Ilość jednostek zasilania - 2 Napięcie prądu elektrycznego. Napięcie wejściowe AC 100 - 240 V Częstotliwość wejściowa AC 50 - 60 Hz Pobór mocy 120 W Maksymalne zużycie mocy 200 W Minimalna i maksymalna temperatura, w której można bezpiecznie używać urządzenia. Zakres temperatur (eksploatacja): 0 - 45 °C Zakres wilgotności względnej: 10 - 85%

7. Skaner – 1 szt.

Nazwa komponentu	Wymagane minimalne parametry techniczne
Typ urządzenia	Urządzenie skanujące wielofunkcyjne kolorowe A3
Główne funkcje	Skanowanie, wysyłanie, przechowywanie, opcja drukowania, kopiowania
Procesor	Dwurdzeniowy procesor o częstotliwości 1,75 GHz
Panel sterowania	Kolorowy ekran dotykowy LCD TFT WSVGA o przekątnej 10,1 cala
Pamięć	3,0 GB pamięci RAM
Dysk twardy	320 GB (dostępne miejsce na dysku: 250 GB)
Interfejsy podłączeniowe	SIEĆ 1000Base-T/100Base-TX/10Base-T, bezprzewodowa sieć LAN (IEEE 802.11 b/g/n) 1 port USB 2.0 (host), 1 port USB 3.0 (host) 1 port USB 2.0 (urządzenie)
Pojemność zasobników papieru	(arkusze A4, 80 g/m²) Standardowo: 1200 arkuszy 2 kasety o pojemności 550 arkuszy każda Taca wielofunkcyjna na 100 arkuszy Maksymalnie: 2300 arkuszy (z modułem kasety podajnika AP1)
Pojemność tacy odbiorczej	(arkusze A4, 80 g/m²) 250 arkuszy
Formaty obsługiwanych nośników	Taca wielofunkcyjna: Rozmiar standardowy: SRA3, A3, A4, A4R, A5, A5R, A6R, B4, B5, B5R Kaseta górna: Rozmiar standardowy: A4, A5, A5R, A6R, B5 Kaseta dolna: Rozmiar standardowy: A3, A4, A4R, A5, A5R, A6R, B4, B5, B5R
Obsługiwana gramatura nośników	Taca wielofunkcyjna: 52–300 g/m²* Kasety na papier (górna/dolna): 52–220 g/m² Druk dwustronny: 52–220 g/m²
Czas rozgrzewania	Tryb szybkiego uruchamiania: maks. 4 s*
Wymiary (szer. × dł. × wys.)	Z pokrywą płyty szklanej Y2: 565 × 692 × 777 mm Z jednoprzebiegowym podajnikiem DADF C1: 565 × 722 × 887 mm (do ustalenia) Z podajnikiem DADF BA1: 565 × 719 × 880 mm
Masa	max. 80 kg
Typ skanowania	Standardowo: kolorowy (płyta) Opcjonalnie: pokrywa płyty, jednoprzebiegowy podajnik DADF C1 lub DADF B1 (2-stronny na 2-stronny; automatyczny z podajnikiem DADF)* * Automatyczny dwustronny podajnik dokumentów DADF
Pojemność podajnika dokumentów (80 g/m²)	Jednoprzebiegowy podajnik DADF C1: do 200 arkuszy DADF BA1: maks. 100 arkuszy
Akceptowane oryginały i gramatury	Płyta: arkusz, książka i obiekty trójwymiarowe Gramatura nośników – podajnik dokumentów: Jednoprzebiegowy podajnik: Skanowanie jednostronne: 38–220 g/m² (cz.-b., kol.) Skanowanie dwustronne: 38–220 g/m² (cz.-b., kol.) Skanowanie jednostronne: 38–128 g/m² (cz.-b.) / 64–128 g/m² (kol.) Skanowanie jednostronne: 50–128 g/m² (cz.-b.) / 64–128 g/m² (kol.)
Formaty obsługiwanych nośników	Płyta szklana: maks. rozmiar skanowania: 297,0 × 431,8 mm Jednoprzebiegowy podajnik A3, A4, A4R, A5, A5R, A6R, B4, B5, B5R, B6R Rozmiar niestandardowy: od 70,0 × 139,7 mm do 304,8 × 431,8 mm A3, A4, A4R, A5, A5R, B4, B5, B5R, B6 Rozmiar niestandardowy: od 139,7 × 128 mm do 297,0 × 431,8 mm

Szybkość skanowania (obr./min: cz.-b./kol., A4)	Jednoprzebiegowy podajnik Skanowanie jednostronne: 135/135 (300 × 300 dpi, wysyłanie) 51/51 (600 × 600 dpi, kopiowanie) Skanowanie dwustronne: 270/270 (300 × 300 dpi, wysyłanie) 51/51 (600 × 600 dpi, kopiowanie) Skanowanie jednostronne: 70/70 (300 × 300 dpi, wysyłanie) 51/51 (600 × 600 dpi, kopiowanie) Skanowanie dwustronne: 35/35 (300 × 300 dpi, wysyłanie) 25,5/25,5 (600 × 600 dpi, kopiowanie)
Rozdzielczość skanowania (dpi)	Skanowanie z kopiowaniem: 600 × 600 Skanowanie z wysyłaniem: (tryb Push) maks. 600 × 600 (SMB/FTP/WebDAV/IFAX), (tryb Pull) 600 × 600 Skanowanie z faksowaniem: 600 × 600
Dane techniczne trybu Pull	Colour Network ScanGear2. Dla opcji TWAIN i WIA Obsługiwane systemy operacyjne: Windows® 7 / 8.1 / 10 / Server2008 / Server2008 R2 / Server2012 / Server2012 R2 / Server2016
Metoda skanowania	Skanowanie w trybie Push i Pull, skanowanie do usługi Box, skanowanie do Advanced Space, skanowanie do sieci, skanowanie do pamięci USB, skanowanie do urządzenia przenośnego, skanowanie do chmury (uniFLOW Online – opcjonalnie)
Szybkość drukowania (cz.-b./kol.)	Do 20 str./min (A4, A5, A5R, A6R), do 15 str./min (A3), do 20 str./min (A4R)
Rozdzielczość drukowania (dpi)	600 × 600, 1200 × 1200 (połowa prędkości)
Języki opisu strony	Standardowo: UFR II, PCL6, Adobe® PostScript®3TM
Drukowanie bezpośrednie	Obsługiwane typy plików: PDF, EPS, TIFF/JPEG i XPS
Szybkość kopiowania (cz.-b./kol.)	Do 20 str./min (A4, A5, A5R, A6R), do 15 str./min (A3) Maks. 20 str./min (A4R)
Czas druku pierwszej kopii (A4, cz.-b./kol.)	Około 5,9/8,2 s lub mniej
Rozdzielczość kopiowania (dpi)	600 × 600
Kopiowanie wielokrotne	Do 999 kopii
Gęstość kopii	Automatyczne lub ręczne (9 poziomów)
Powiększenie	Zmienne powiększenie: 25–400% (przyrost o 1%) Zaprogramowane ustawienia zmniejszenia/powiększenia: 25%, 50%, 70%, 110% (1:1), 141%, 200%, 400%