

SZP/UE/3/2018

Załącznik nr 1 do SIWZ
Zmodyfikowany: 22-10-2018

Opis przedmiotu zamówienia (OPZ)

Informatyzacja oraz wdrożenie e-usług
W Samodzielnym Publicznym Zakładzie Opieki
Zdrowotnej w Lubartowie

Spis treści

Spis treści.....	2
1. Wstęp.....	4
2. Informacja o Zamawiającym.....	7
3. Założenia i wymagania ogólne dla systemu.....	9
4. Wymagania dla funkcjonalności Systemu.....	14
4.1 Wymagania dla modułu e-platformy	14
4.1.1. e-Rejestracja	15
4.1.2. e-Badanie.....	18
4.1.3. e-Powiadomienia.....	19
4.1.4. e-Dokumentacja	20
4.1.5. e-Archiwum	21
4.1.6. e-Kolejka	21
4.1.7. e-Wywiad/e-Ankieta.....	23
4.2. Wymagania podsystemu RDM/EDM	24
4.3. Wymagania dla oprogramowania do digitalizacji dokumentacji medycznej papierowej.....	25
5. Założenia i wymagania dla środowiska infrastruktury sprzętowej i prac modernizacyjnych	27
5.1 Wykaz sprzętu i oprogramowania	27
5.1.1 Serwery na potrzebę wirtualizacji – 3 sztuki.....	27
5.1.2. Oprogramowanie dostępne użytkownika do środowiska CAL – 150 sztuk	32
5.1.3. Oprogramowanie do wirtualizacji dla serwerów wirtualizacji - Licencja na min 3 hosty po min 2 CPU 33	
5.1.4. Macierz – 1 sztuka.....	35
5.1.5. Serwer na potrzebę systemu ochrony danych (backupu) – 1 sztuka	38
5.1.6. Biblioteka taśmowa – 1 sztuka	41
5.1.7. Przełącznik rdzeniowy – 1 sztuka	41
5.1.8. Przełącznik dostępowy 48 portowy PoE – 4 sztuki	42
5.1.9. Przełącznik dostępowy 24 portowy – 4 sztuki	43
5.1.10. Urządzenia UPS dla przełączników dostępowych – 3 sztuki	44
5.1.11. Szafa teletechniczna wraz z wyposażeniem – 1 sztuka	46
5.1.12. Urządzenie UPS do serwerowni – 1 sztuka	47
5.1.13. Oprogramowanie systemu ochrony danych (backupu) – 1 komplet.....	49
5.1.14. Kontroler WiFi – 1 sztuka.....	52
5.1.15. Punkty dostępne sieci WiFi – 30 sztuk.....	54

5.1.16.	Stacje robocze wraz z oprogramowaniem systemowym – 125 sztuk	56
5.1.17.	Monitory stacji roboczych – 125 sztuk.....	60
5.1.18.	Instalacja, konfiguracja i uruchomienie infrastruktury sprzętowej oraz oprogramowania systemowego, wirtualizacyjnego i narzędziowego	61
5.1.19.	Modernizacja sieci teleinformatycznej (szkielet światłowod).....	62
5.1.20.	Modernizacja serwerowni.....	62
5.1.21.	Skaner dokumentacji medycznej - 1 sztuka	64
5.1.22.	Przełącznik FC – 2 sztuki.....	64
6.	Wymagania dotyczące wdrożenia i przeszkolenia	66
6.1.	Wymagania dotyczące budowy środowiska chmury obliczeniowej.....	66
6.2.	Wymagania dotyczące zarządzenia projektem.....	67
6.3.	Wymagania dotyczące świadczenia serwisu gwarancyjnego dla Systemu.....	68
6.4.	Wymagania dotyczące przeszkolenia Administratorów i Użytkowników	69
6.4.1.	Szkolenia dla administratorów Systemu	69
6.4.2.	Szkolenia dla Użytkowników z obsługi funkcjonalności Systemu	69
6.5.	Wymagania dotyczące przygotowania dokumentacji.....	69
6.6.	Wymagania dotyczące testów penetracyjnych funkcjonalności e-platformy (EDM/RDM, e-usługi).....	70

1. Wstęp

W dokumencie przedstawiony został opis przedmiotu zamówienia systemu na potrzebę informatyzacji oraz wdrożenia e-usług w Samodzielnym Publicznym Zakładzie Opieki Zdrowotnej w Lubartowie.

W ramach struktur SPZOZ w Lubartowie działają następujące placówki medyczne:

1. Szpital Specjalistyczny, Przychodnia Specjalistyczna, Ratownicze Zespoły Wyjazdowe – ul. Cicha 14, 21-100 Lubartów
2. Centrum Medycyny Rodzinnej – ul. 1-go Maja 3, 21-150 Kock
3. Centrum Medycyny Rodzinnej – ul. Partyzantów 12, 21-110 Ostrów Lubelski

Wszystkie wyżej wymienione placówki stanowią jeden podmiot gospodarczy stanowiący Zamawiającego, natomiast projektem objęta jest jedynie placówka przy ul. Cichej 14 w Lubartowie.

Celem głównym projektu jest informatyzacja w sektorze ochrony zdrowia poprzez rozbudowę oraz zakupy infrastruktury informatycznej służącej zwiększeniu stopnia cyfryzacji, w tym aplikacji i systemów bazodanowych zapewniających poprawę efektywności zarządzania oraz upowszechnienia komunikacji elektronicznej w sektorze ochrony zdrowia, oraz rozwój elektronicznych usług publicznych, poprzez rozbudowę istniejącego u Zamawiającego systemu informatycznego zapewniającego dostępność, integrację oraz cyfryzację nowych usług i poprawę funkcjonalności istniejących usług publicznych świadczonych drogą elektroniczną w zakresie e-zdrowia. Celem bezpośrednim projektu jest zapewnienie pacjentom szpitala dostępu do szerokiego zakresu wysokiej jakości usług publicznych świadczonych drogą elektroniczną. Efektem realizacji projektu będzie wyposażenie wnioskodawcy w narzędzia i usługi przyczyniające się do efektywniejszych działań w zakresie ochrony zdrowia. Działania objęte projektem pozwolą rozszerzyć istniejącą ofertę e-usług świadczonych przez wnioskodawcę, co przyczyni się do zwiększenia stopnia ich wykorzystania. Wzrost liczby e - usług stanowi wsparcie działań na rzecz rozwoju społeczeństwa informacyjnego, a co za tym idzie zwiększenie uczestnictwa obywateli w życiu publicznym. Cel bezpośredni projektu zostanie osiągnięty poprzez wzrost liczby e- usług oraz zwiększenie stopnia cyfryzacji procesów realizowanych przez wnioskodawcę. Projekt przyczyni się do poprawy dostępu do informacji medycznej dla pacjentów wnioskodawcy, poprawy jakości procesu leczenia i zwiększenie bezpieczeństwa pacjentów, podniesienia efektywności ekonomicznej wnioskodawcy, a także usprawnienia procesu bieżącego zarządzania ochroną zdrowia.

W ramach projektu należy wykonać następujące prace:

1. instalacja, konfiguracja i uruchomienie infrastruktury sprzętowej oraz oprogramowania systemowego, wirtualizacyjnego i narzędziowego, a także przeprowadzenie testów penetracyjnych funkcjonalności e-platformy.
2. dostawa serwerów:
 - serwerów na potrzebę wirtualizacji
 - serwera na potrzebę systemu ochrony danych
3. dostawa zestawów komputerowych - stacji roboczych z systemem operacyjnym wraz z monitorami;
4. dostawa urządzeń:
 - macierzy dyskowej,
 - przełączników sieciowych rdzeniowych,
 - przełączników sieciowych dostępowych 48 portowych PoE+,

- przełączników sieciowych dostępowych 24 portowych,
 - biblioteki taśmowej,
 - urządzeń UPS dla przełączników dostępowych,
 - szafy teletechnicznej wraz z wyposażeniem,
 - UPS do serwerowni,
 - kontrolera sieci WiFi,
 - punktów dostępowych sieci WiFi,
 - skanera dokumentacji medycznej,
 - przełączników FC.
5. dostawa oprogramowania narzędziowego:
- licencji oprogramowania backup,
 - licencji dostępowych do serwera,
 - licencji oprogramowania do wirtualizacji.
6. Modernizacja
- sieci teleinformatycznej,
 - serwerowni
7. dostawa licencji i wdrożenie oprogramowania e-usług:
- RDM/EDM,
 - e-rejestracja,
 - e-badanie,
 - e-powiadomienia,
 - e-dokumentacja,
 - e-kolejka,
 - e-wywiad/e-ankieta,
 - e-archiwum,
 - oprogramowania do digitalizacji dokumentacji medycznej papierowej
8. Przeprowadzenie instruktażu dla pracowników i szkolenia dla administratorów systemu.
9. Sporządzenie dokumentacji technicznej i powykonawczej.

Szczegółowy wykaz ilościowy:

L.p.	Pozycja	kategoria kosztu	J.m.	liczba jednostek
1.	przeprowadzenie szkoleń dla administratorów systemu	usługi	komplet	1
2.	rdm/edm	zakupy	licencja	1
3.	e-rejestracja	zakupy	licencja	1
4.	e-badanie	zakupy	licencja	1
5.	e-powiadomienia	zakupy	licencja	1
6.	e-dokumentacja	zakupy	licencja	1
7.	e-kolejka	zakupy	licencja	1
8.	e-wywiad/e-ankieta	zakupy	licencja	1
9.	e-archiwum	zakupy	licencja	1
10.	oprogramowanie do digitalizacji dokumentacji medycznej papierowej	zakupy	licencja	1
11.	instalacja, konfiguracja i uruchomienie e-platformy wraz z instruktażem (szkoleniem) dla użytkowników, testy penetracyjne funkcjonalności e-	usługi	usługa	1

	platformy			
12.	instalacja, konfiguracja i uruchomienie infrastruktury sprzętowej oraz oprogramowania systemowego, wirtualizacyjnego i narzędziowego	usługi	usługa	1
13.	wyposażenie serwerowni - zakup serwera na potrzebę wirtualizacji	zakupy	sztuka	3
14.	wyposażenie serwerowni - zakup serwera na potrzebę systemu ochrony danych	zakupy	sztuka	1
15.	wyposażenie stanowisk pracowniczych - zakup stacji roboczych z systemem operacyjnym	zakupy	sztuka	125
16.	wyposażenie stanowisk pracowniczych - zakup monitorów do stacji roboczych	zakupy	sztuka	125
17.	wyposażenie serwerowni - zakup macierzy dyskowej	zakupy	sztuka	1
18.	wyposażenie serwerowni - zakup przełączników sieciowych rdzeniowych	zakupy	sztuka	1
19.	wyposażenie serwerowni - zakup przełączników sieciowych dostępowych 48 portowych poe+	zakupy	sztuka	4
20.	wyposażenie serwerowni - zakup przełączników sieciowych dostępowych 24 portowych	zakupy	sztuka	4
21.	wyposażenie serwerowni - zakup biblioteki taśmowej	zakupy	sztuka	1
22.	wyposażenie serwerowni - zakup ups dla przełączników dostępowych	zakupy	sztuka	3
23.	wyposażenie serwerowni - zakup szafy teletechnicznej wraz z wyposażeniem	zakupy	sztuka	1
24.	wyposażenie serwerowni - zakup ups do serwerowni	zakupy	sztuka	1
25.	wyposażenie serwerowni - zakup kontrolera sieci wifi	zakupy	sztuka	1
26.	wyposażenie serwerowni - zakup punktów dostępowych sieci wifi	zakupy	sztuka	30
27.	wyposażenie stanowisk pracowniczych - zakup skanera dokumentacji medycznej	zakupy	sztuka	1
28.	wyposażenie serwerowni - zakup przełącznika fc	zakupy	sztuka	2
29.	wyposażenie serwerowni - zakup licencji oprogramowania backup	zakupy	sztuka	1
30.	wyposażenie serwerowni - zakup licencji dostępowych do serwera	zakupy	sztuka	150
31.	wyposażenie serwerowni - zakup licencji oprogramowania do wirtualizacji	zakupy	sztuka	1
32.	modernizacja sieci teleinformatycznej	usługi	usługa	1
33.	modernizacja serwerowni	usługi	usługa	1

2. Informacja o Zamawiającym

W skład SPZOZ w Lubartowie wchodzi:

1. Szpital Specjalistyczny, Przychodnia Specjalistyczna, Ratownicze Zespoły Wyjazdowe – ul. Cicha 14, 21-100 Lubartów
 - Izba Przyjęć
 - Oddział chirurgiczny ogólny
 - Oddział pediatryczny
 - Oddział intensywnej terapii i anestezjologii
 - Oddział ginekologiczno - położniczy
 - Oddział neonatologiczny
 - Oddział urologiczny
 - Oddział chorób wewnętrznych
 - Oddział neurologiczny
 - Pododdział Udarowy Oddziału Neurologicznego
 - Pododdział Rehabilitacji Neurologicznej Oddziału Neurologicznego
 - Oddział chorób płuc
 - Apteka zakładowa
 - Pracownia diagnostyki obrazowej
 - Blok operacyjny
 - Poradnia diabetologiczna
 - Poradnia endokrynologiczna
 - Poradnia gastroenterologiczna
 - Poradnia kardiologiczna
 - Poradnia nefrologiczna
 - Poradnia neurologiczna
 - Poradnia rehabilitacyjna
 - Poradnia neonatologiczna
 - Poradnia ginekologiczno-położnicza
 - Poradnia chirurgii ogólnej
 - Poradnia chirurgii urazowo- ortopedycznej
 - Poradnia preluksacyjna
 - Poradnia urologiczna
 - Poradnia reumatologiczna
 - Poradnia chorób płuc
 - Poradnia zdrowia psychicznego dla dorosłych
 - Poradnia terapii uzależnienia od alkoholu
 - Poradnia Medycyny Pracy
 - Gabinet lekarza POZ
 - Zespół wyjazdowy reanimacyjny R
 - Zespół wyjazdowy reanimacyjny W
 - Zespół transportu sanitarnego
 - Pracownia endoskopii przewodu pokarmowego
 - Pracownia tomografii komputerowej
 - Pracownia EEG

- Pracownia Diagnostyki Kardiologicznej
 - Pracownia bronchoskopowa
 - Gabinet medycyny szkolnej
 - Dział Fizjoterapii
 - Gabinet położnej POZ
 - Gabinet pielęgniarstwa POZ
 - Gabinet diagnostyczno-zabiegowy przy Poradni Chirurgii Urazowo-Ortopedycznej
 - Gabinet diagnostyczno-zabiegowy przy Poradni Chirurgii Ogólnej
 - Gabinet diagnostyczno-zabiegowy przy Poradni Ginekologiczno-Położniczej
 - Gabinet nocnej i świątecznej opieki zdrowotnej
2. Centrum Medycyny Rodzinnej – ul. 1-go Maja 3, 21-150 Kock
- Zespół wyjazdowy reanimacyjny R
 - Gabinet lekarza POZ
 - Poradnia ginekologiczna
 - Gabinet medycyny szkolnej
 - Gabinet położnej POZ
 - Gabinet pielęgniarstwa POZ
 - Gabinet diagnostyczno-zabiegowy przy Poradni Ginekologiczno-Położniczej
3. Centrum Medycyny Rodzinnej – ul. Partyzantów 12, 21-110 Ostrów Lubelski
- Zespół wyjazdowy reanimacyjny W
 - Gabinet lekarza POZ
 - Poradnia
 - Gabinet medycyny szkolnej
 - Gabinet pielęgniarstwa środowiskowej POZ
 - Gabinet położnej POZ

3. Założenia i wymagania ogólne dla systemu

Wykonawca w ramach realizacji przedmiotu umowy, tj. rozbudowy istniejącego u Zamawiającego systemu HIS (system WMS Mediquis firmy Gabos Software Sp. z o.o., ul. Generała Leona Berbeckiego 6, 44-100 Gliwice, działający w oparciu o system relacyjnej bazy danych IBM DB2), dostarczy i wdroży system e-usług, udostępniający e-usługi dla Pacjentów i Personelu medycznego placówek Zamawiającego. W ramach systemu e-usług Wykonawca dostarczy rozwiązanie posiadające:

- podsystem (oprogramowanie) do digitalizacji dokumentacji medycznej papierowej,
- podsystem (oprogramowanie) e-platformy, udostępniający usługi elektroniczne (e-usługi),
- podsystem (oprogramowanie) RDM/EDM, umożliwiające prowadzenie dokumentacji medycznej pacjenta.

Zamawiający oczekuje rozbudowy istniejącego u Zamawiającego systemu HIS o funkcjonalności umożliwiające prowadzenie dokumentacji medycznej pacjenta (EDM/RDM), dostawy i uruchomienia specjalistycznego oprogramowania mającego na celu wdrożenie nowoczesnych e-usług (e-platformy) oraz oprogramowania do digitalizacji dokumentacji medycznej papierowej w taki sposób, by podsystemy EDM/RDM. e-platformy i digitalizacji pracowały z tym systemem HIS bezpośrednio (online), to jest bez konieczności uruchamiania dodatkowego oprogramowania pośredniczącego, przesyłającego dane w postaci osobnych zbiorów (plików) danych między HIS i dowolnym z podsystemów.

Zamawiający informuje, że nie posiada praw do kodów źródłowych w/w oprogramowania – tym samym nie ma możliwości ich udostępnienia wykonawcom na potrzeby wykonywania zamówienia. Zamawiający nie posiada informacji w zakresie standardów umożliwiających przesyłanie informacji pomiędzy przedmiotem zamówienia, a systemem szpitalnym klasy HIS, jak również nie posiada wiedzy na temat struktury bazy danych do której dane powinny być przekazywane. Zamawiający oczekuje, że Wykonawca celem zapewnienia współdziałania z oferowanymi e-usługami, przy użyciu posiadanej wiedzy oraz doświadczenia, o ile będzie to konieczne, w celu ustalenia, jak użytkowany u Zamawiającego system klasy HIS działa, dokona szczegółowej analizy przy pomocy inżynierii wstecznej na etapie analizy przedwdrożeniowej w ramach przygotowania Projektu Wykonawczego.

Zamawiający na etapie realizacji umowy zapewni Wykonawcy dostęp do bazy danych obecnie użytkowanego systemu HIS. Zamawiający zastrzega, że nie jest twórcą programu WMS Mediquis, jak i dokumentacji tegoż systemu i nie może odpowiadać za jej kompletność. Zamawiający zastrzega, że ewentualne luki w ogólnodostępnej dokumentacji silnika bazy danych nie stanowią podstawy dla Wykonawcy dla zaprzestania lub zmniejszenia zakresu integracji użytkowanego systemu HIS ani do przesunięcia wymaganych terminów realizacji zadania. Wykonawca nie może ingerować w przechowywane dane medyczne obecnie użytkowanego systemu HIS w celu przeprowadzenia procesu integracji systemu z oferowanymi e-usługami.

Szczegółową informację uwzględniającą powiązanie z istniejącą infrastrukturą Zamawiającego Wykonawca przygotuje i przedstawi do akceptacji Zamawiającego w trakcie analizy przedwdrożeniowej w Projektu Wykonawczym. W ramach konfiguracji środowiska systemu Wykonawca będzie odpowiedzialny za konfigurację serwerów i systemów zgodnie z uzgodnionym projektem technicznym integracji.

Dane z modułów obsługi pacjenta i obiegu informacji medycznej HIS będą stanowiły wsad informacyjny, stanowiący podstawę działania dostarczanych podsystemów. Informacje z dostarczanych podsystemów będą trafiały do systemu HIS. Dla zachowania spójności przetwarzanych danych i uniknięcia dublowania danych (niezasadne wykorzystanie zasobów sprzętowych), zbiory informacji przechowywanych przez ww. elementy oprogramowania muszą stanowić wspólną bazę danych, z której poszczególne usługi

Systemu będą korzystać. System w wyżej wymienionym zakresie musi więc posiadać jeden spójny zbiór danych, do którego dostęp mają osoby posiadające odpowiednie uprawnienia.

Wykonawca na podstawie informacji i danych przekazanych przez Zamawiającego na etapie opracowywania Projektu Wykonawczego przygotowuje konfigurację dostarczanych podsystemów w taki sposób, aby spełniał on wszystkie wymagania zdefiniowanych w OPZ i przez to umożliwiał rozpoczęcie pracy personelu Zamawiającego z dostarczonymi podsystemami bez zakłócania pracy jednostek Zamawiającego.

Kolumna „Próbka” oznaczona wyrazem „TAK” oznacza konieczność zademonstrowania tejże funkcjonalności w trakcie prezentacji próbki systemu o której mowa w Załączniku nr 3 do SIWZ

Wymagania ogólne dla systemu e-usług

Lp.	Wymagania	Próbka
1	Podsystemy e-usług, digitalizacji i EDM/RDM muszą działać na tej samej bazie danych co system obsługi pacjenta i obiegu informacji medycznej HIS. Podsystemy te muszą stanowić rozbudowę istniejącego u Zamawiającego systemu HIS.	
2	System musi być zgodny z normami dotyczącymi służby zdrowia: <ul style="list-style-type: none"> • 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 „Technika informatyczna - Zarządzanie usługami - Część 1: Wymagania dla systemu zarządzania usługami”, • PN ISO/IEC 27001 „Technika informatyczna - Techniki bezpieczeństwa - Systemy zarządzania bezpieczeństwem informacji - Wymagania”, • PN-ISO/IEC 27005 "Technika informatyczna - Techniki bezpieczeństwa - Zarządzanie ryzykiem w bezpieczeństwie informacji", 	
3	Podsystemy muszą spełniać zasady interoperacyjnego współdziałania na trzech poziomach: semantycznym, organizacyjnym oraz technologicznym zgodnie z Rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. 2012 poz. 526, z późn. zm.).	
4	Podsystemy muszą być przystosowane do uruchomienia na platformie wirtualizacyjnej w chmurze.	
5	Podsystemy muszą mieć możliwość pracy użytkowej przez 24 godziny na dobę, 7 dni w tygodniu, 365 dni w roku.	
6	Dostarczane podsystemy muszą posiadać dwa stworzone przez Wykonawcę w ramach wdrożenia środowiska: środowisko produkcyjne, środowisko testowo-szkoleniowe. Środowisko produkcyjne przeznaczone będzie do eksploatacji produkcyjnej, a środowisko testowo-szkoleniowe dla prowadzenia testów poprawek programowych oprogramowania przed jego instalacją w środowisku produkcyjnym, oraz do prowadzenia szkoleń użytkowników.	
7	Podsystemy muszą umożliwiać tworzenie, archiwizowanie oraz udostępnianie elektronicznej dokumentacji medycznej wg zasad określonych w ustawie o z dnia 28 kwietnia 2011r. o systemie informacji w ochronie zdrowia (Dz. U. 2011 nr 113 poz. 657, z późn. zm.).	
8	Podsystemy muszą umożliwiać ich integrację z platformami P1 i P2.	
9	Podsystemy muszą być zintegrowane z systemami NFZ w zakresie niezbędnym do realizacji opisanych w dokumencie funkcjonalności.	

10	<p>Podsystemy muszą umożliwić tworzenie elektronicznych dokumentów medycznych oraz prowadzenie rejestru świadczeń opieki zdrowotnej, o którym mowa w Rozporządzeniu Ministra Zdrowia z dnia 20 czerwca 2008r. 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 w sprawie rodzajów Elektronicznej Dokumentacji Medycznej z dnia 8 maja 2018 r. (Dz.U. z 2018 r. poz. 941) oraz dokumentach opublikowanych przez Centrum Systemów Informacyjnych Ochrony Zdrowia.</p>	
11	<p>Podsystemy muszą generować dokumenty medyczne w standardzie HL7 CDA i/lub PDF.</p>	
12	<p>Podsystemy muszą umożliwić przesłanie do P1 informacji o trzech obszarach:</p> <ul style="list-style-type: none"> • informacja o zdarzeniu medycznym, tzw. ExtPLHealthcareEvent, • indeksy dokumentów medycznych wytworzonych w ramach tego zdarzenia, tzw. XDSDocumentEntry, • informacja o bieżącej komunikacji, tzw. XDSSubmissionSet, 	
13	<p>Podsystemy w zakresie gromadzenia i udostępniania, za pośrednictwem P1, informacji o zdarzeniach medycznych oraz wytworzonej podczas zdarzenia medycznego elektronicznej dokumentacji medycznej, powinny posiadać następujące grupy funkcjonalne:</p> <ul style="list-style-type: none"> • dodawania i edycji danych medycznych, • importu/migracji danych zewnętrznych, • tworzenia dokumentacji medycznej, • autoryzacji, • wersjonowania, • archiwizacji, • uprawnień, • dostępu. 	
14	<p>Podsystemy muszą działać w architekturze Klient – Serwer, w której baza danych znajduje się na serwerze centralnym obsługującym zarządzanie i przetwarzanie danych. Poszczególne aplikacje pracując na stacjach roboczych otrzymują z serwera wyniki obliczeń jednak również same mogą wykonywać indywidualne zadania lub obliczenia nie angażując serwera.</p>	
15	<p>Podsystemy muszą posiadać mechanizmy umożliwiające przeprowadzenie centralnej aktualizacji oprogramowania, zarówno w środowisku produkcyjnym jak i testowo-szkoleniowym, bez konieczności ręcznej aktualizacji na każdej stacji roboczej i tablecie z osobna.</p>	
16	<p>Podsystemy muszą działać i udostępniać wszystkie wymagane funkcjonalności na infrastrukturze sprzętowej Zamawiającego, z uwzględnieniem również komponentów tej infrastruktury dostarczanych w ramach niniejszego projektu.</p>	
17	<p>Podsystemy muszą posiadać mechanizmy umożliwiające użycie bezpiecznego podpisu elektronicznego weryfikowanego przy pomocy ważnego kwalifikowanego certyfikatu w rozumieniu rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylającego dyrektywę 1999/93/WE (Dz. Urz. UE L 257 z 28.08.2014, str. 73) lub podpisu potwierdzonego profilem zaufanym ePUAP w rozumieniu ustawy z dnia 17 lutego 2005r. o informatyzacji działalności podmiotów realizujących zadania publiczne. Powyższe dotyczy:</p> <p>elektronicznej dokumentacji medycznej,</p> <p>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,</p> <p>wniosku o dostęp do danych przetwarzanych w SIM umożliwiającym wymianę między usługodawcami danych zawartych w elektronicznej dokumentacji medycznej.</p>	

18	Podsystemy muszą spełniać wymagania bezpieczeństwa na poziomie wysokim opisanym w Załączniku do rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.	
19	Podsystemy muszą posiadać zaimplementowane mechanizmy kontroli dostępu do danych.	
20	Podsystemy muszą działać w oparciu o rejestrowany odrębny identyfikator dla każdego użytkownika, przy czym nie jest dopuszczalna sytuacja, w której którykolwiek z podsystemów wymaga od użytkownika logowania się innym identyfikatorem, niż ten, który dla tego użytkownika jest zdefiniowany w systemie HIS Zamawiającego.	
21	Podsystemy muszą posiadać spójny z systemem HIS mechanizm kontroli dostępu. Dostęp do danych będzie możliwy wyłącznie po dokonaniu uwierzytelnienia.	
22	Podsystemy muszą posiadać ochronę przed zagrożeniami pochodzącymi z sieci publicznej opartą na fizycznych lub logicznych zabezpieczeniach chroniących przed nieuprawnionym dostępem.	
23	Dane z podsystemów przesyłane w sieci publicznej muszą być zaszyfrowane. Certyfikaty do szyfrowania danych nie stanowią przedmiotu zamówienia.	
24	Podsystemy muszą być zabezpieczone przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego oraz przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.	
25	Podsystemy muszą umożliwiać ograniczenie dostępu do danych, funkcji systemu, procesów systemowych stosownie do danej roli użytkownika, tj. według zasady „w Systemie widzę tylko to co muszę, aby wypełniać swoje obowiązki”.	
26	Podsystemy muszą w logu systemowym współdzielonym z systemem HIS składować informacje (datę i godzinę z dokładnością do sekundy; adres IP stacji, unikalny identyfikator użytkownika; jeżeli dane w podsystemie uległy zmianie, to również informacje o tym, z jakiej wartości i na jaką wartość została dokonana zmiana), rejestrując w szczególności: zapisy o zalogowaniu do podsystemu i wylogowaniu z podsystemu każdego z użytkowników, zmianę parametrów konta każdego użytkownika, w szczególności zmianę uprawnień użytkownika, każdą inną zmianę danych zgromadzonych w podsystemie i dopisanie nowych danych do Systemu (wartość początkowa danych powinna być wówczas pusta) Funkcjonalność dodatkowa	
27	W podsystemach musi zostać odwzorowana struktura organizacyjna każdej z placówek Zamawiającego.	
28	Podsystemy muszą blokować fizyczne usunięcie wpisu dokonanego w dokumentacji medycznej. Usunięcie wpisu oznacza jedynie jego dezaktywację, tj. przełączanie w tryb nieaktywny od daty i godziny pobranej automatycznie w momencie dezaktywacji. Usunięcia (tj. dezaktywacji) lub modyfikacji wpisu może dokonać osoba dokonująca wpisu lub osoba posiadająca specjalne wyodrębnione uprawnienie do tych operacji. Fakt ten musi zostać odnotowany w podsystemie wraz z zachowaniem historii zmiany to jest: oznaczenia osoby dokonującej zmiany, czasu dokonania zmiany oraz zachowania wersji sprzed dokonania zmiany. Jako spełnienie wymogu nie będzie uważane jedynie zapisywanie logu transakcji i wyszukiwanie zmian na poziomie administratora bazy danych.	
29	Wszystkie udostępniane w podsystemach funkcjonalności użytkownika muszą być w języku polskim.	
30	W oprogramowaniu podsystemów pola wymagane (obligatoryjne) muszą być jednoznacznie rozróżnialne (np.: inny kolor, kształt).	
31	W miejscach interfejsu użytkownika oprogramowania, w których prezentowane są dane w formie tabelarycznej, musi istnieć możliwość sortowania poszczególnych kolumn po nagłówkach.	
32	Oprogramowanie podsystemów musi umożliwiać wyszukiwanie elementów po fragmencie frazy bez uwzględniania wielkości znaków.	
33	Wszystkie dane słownikowe i rejestry wykorzystywane w podsystemach muszą być spójne z danymi słownikowymi i rejestrami systemu HIS i definiowane w jednym miejscu, którym jest baza danych	

	systemu HIS - funkcjonalność dodatkowa	
34	Proces zarządzania użytkownikami w tym logowanie, polityka haseł w systemie HIS i wdrażanych podsystemach musi być jednolity dla wszystkich podsystemów i systemu HIS Zamawiającego - funkcjonalność dodatkowa	

4. Wymagania dla funkcjonalności Systemu

W ramach projektu Wykonawca uruchomi e-platformę wraz z szeregiem usług elektronicznych (e-usług), dla których wymagania zostały opisane poniżej.

4.1 Wymagania dla modułu e-platformy

Wdrożony System musi posiadać moduł e-platformy. Funkcjonalności systemu e-platformy dostępne muszą być z poziomu strony WWW Zamawiającego dla pacjentów Zamawiającego. Moduł e-platformy musi posiadać następujące funkcjonalności i cechy:

Wymagania dla modułu e-platformy

Lp.	Wymagania	Próbka
1.	Moduł e-platformy, musi posiadać funkcjonalności umożliwiające zdefiniowanie trzech rodzajów kont dostępowych: dla pacjentów, dla osób personelu medycznego Zamawiającego	
2.	Dostęp do modułu e-platformy musi być możliwy ze strony WWW, zarówno z sieci Internet jak i sieci wewnętrznej placówki (Intranet), także z poziomu stacji roboczych dostarczonych w ramach projektu.	
3.	Moduł e-platformy musi udostępniać pacjentom formularz rejestracyjny umożliwiający samodzielne założenie konta dostępowego do e-usług.	
4.	W procesie rejestracji do modułu e-platformy, w formularzu rejestracyjnym, pacjent musi zostać zobligowany do wprowadzenia następujących informacji: <ul style="list-style-type: none"> danych niezbędnych do założenia wpisu w rejestrze pacjentów, tj.: nazwisko, imię, PESEL, adres; adresu email i numeru telefonu komórkowego dla celów wysyłania powiadomień. 	
5.	Formularz rejestracyjny pacjenta musi mieć wbudowany mechanizm walidacji, jako ochrona przed robotami (szkodliwym oprogramowaniem).	
6.	Dostęp do e-usług musi być chroniony hasłem i dostępny poprzez szyfrowane połączenie (https) tylko dla kont użytkowników zarejestrowanych w e-platformie.	
7.	Formularz rejestracyjny musi walidować poprawność numeru PESEL.	
8.	Formularz rejestracyjny musi walidować adres email.	
9.	Podczas zakładania konta pacjenta, wprowadzone dane muszą być walidowane przez System z rejestrem pacjentów jednostki znajdującym się w bazie danych Systemu, tj.: jeżeli dane pacjenta znajdują się już w rejestrze pacjentów, to konto w module e-platforma powinno być z tą osobą automatycznie powiązane – tzn. dane takiej osoby nie są dopisywane do rejestru; jeżeli dane pacjenta, nie znajdują się w rejestrze, to osoba taka musi zostać automatycznie dopisana do rejestru pacjentów, a konto w e-platformie automatycznie musi zostać powiązane z tą osobą.	
10.	Moduł musi realizować proces aktywacji konta pacjenta w następujący sposób: Pacjent rejestruje się do e-platformy poprzez formularz rejestracyjny; Po wypełnieniu i wysłaniu formularza rejestracyjnego System musi zwrócić pacjentowi, na podany w procesie rejestracji email, potwierdzenie o założeniu konta wraz z linkiem aktywacyjnym; Wybranie (kliknięcie) przez pacjenta linka aktywacyjnego w emailu, musi przenieść pacjenta do okienka udostępnianego przez moduł e-platformy, w którym (w celu aktywacji konta) będzie zobligowany do podania i potwierdzenia hasła. Zapisanie hasła musi spowodować aktywację konta dostępowego do e-usług w e-platformie.	

	Po wykonaniu powyższych kroków pacjent musi mieć możliwość korzystania z e-usług Systemu.	
11.	Podsystem, w procesie rejestracji pacjenta, musi wymuszać podanie hasła o właściwej składni – wymaganej przepisami prawa dotyczącymi systemów informatycznych przetwarzających dane osobowe w tym dane medyczne.	
12.	Pacjent rejestrujący się do e-platformy musi zostać poinformowany przez System z ilu i jakich znaków musi być złożone hasło logowania do e-usług (hasło aktywacyjne).	
13.	Podsystem musi udostępniać Administratorowi Systemu, funkcjonalność definiowania okresu ważności hasła dostępowego do e-usług Systemu. Użycie funkcjonalności musi wymuszać na Użytkownikach modułu e-platformy dokonania zmiany hasła po upływie okresu jego ważności. Przy pierwszym logowaniu do e-usługi po okresie ważności hasła, System musi wymusić na Użytkowniku dokonanie zmiany hasła.	
14.	Moduł musi umożliwiać pacjentowi, użytkownikowi e-platformy założenie dodatkowego konta dostępowego do e-usług wyłącznie do swoich danych w celu ich udostępnienia osobie trzeciej. Konto takie musi być tworzone na określony okres czasu, tj. na okres czasu wskazany przez właściciela danych oraz musi być związane tylko i wyłącznie z kontem pacjenta wnioskującego. Dla założenia konta, System musi wymuszać na osobie podanie daty ważności konta, a po upływie czasu aktywności, konto musi zostać automatycznie wyłączone.	
15.	Moduł musi umożliwiać założenie przez Administratora Systemu lub uprawnioną przez Zamawiającego osobę, konta w module e-platformy dla osoby personelu medycznego Zamawiającego, np. dla lekarza.	
16.	Konto dla osoby personelu medycznego w module e-platformy może zostać założone wyłącznie dla osoby posiadającej aktywne konto w module obsługi pacjenta i obiegu dokumentacji medycznej.	
17.	Przy zakładaniu konta dla osoby personelu medycznego System musi wymuszać podanie adresu email tej osoby - pracownika	
18.	Logowanie osoby personelu medycznego do modułu e-platformy musi odbywać się z wykorzystaniem parametrów logowania (loginu i hasła), tych samych, którymi osoba posługuje się logując do modułu obsługi pacjenta i obiegu dokumentacji medycznej.	
19.	Moduł musi umożliwiać założenie przez Administratora Systemu lub uprawnioną przez Zamawiającego osobę, konta w module e-platformy dla osoby reprezentującej placówkę współpracującą. Takie konto może zostać założone wyłącznie dla partnera zaewidencjonowanego w Systemie jako podmiot medyczny.	
20.	Przy zakładaniu konta dla osoby partnera moduł musi wymuszać podanie następujących danych: jednostkę (partnera) – wartość słownikowa, użytkownika i hasło, adres email. Moduł musi wymuszać zmianę hasła przy pierwszym logowaniu do modułu e-platformy osoby partnera Zamawiającego.	
21.	System musi umożliwiać Administratorowi Systemu wykonanie dezaktywacji dowolnego konta utworzonego w module e-platforma.	
22.	Administrator musi mieć możliwość aktywowania konta nieaktywnego.	
23.	System musi posiadać funkcjonalność zmiany/resetowania hasła dostępu do modułu e-platformy przez użytkownika.	

4.1.1. e-Rejestracja

Usługa e-rejestracji dedykowana jest dla pacjentów, uprawnionych pracowników Zamawiającego i uprawnionych kontrahentów. Ma zapewnić pacjentowi możliwości sprawdzenia dostępności terminów przyjęć przez lekarzy w poszczególnych poradniach / gabinetach oraz dokonania rezerwacji dogodnego terminu.

Usługa musi być dostępna z poziomu strony internetowej Zamawiającego, po zalogowaniu się pacjenta indywidualnym profilem do modułu e-platformy. Usługa udostępniona będzie także z poziomu stacji roboczych dostarczonych w ramach projektu.

Moduł udostępni również usługi dla uprawnionego personelu Przychodni w celu systematycznego definiowania grafików dostępności świadczonych usług w aktualnie używanym systemie do obsługi medycznej - HIS. Wykorzystując mechanizmy integracji pomiędzy systemem HIS a systemem e-platformy, informacje nt. wolnych terminów, w których możliwe jest świadczenie usług, będą dostępne w module e-Rejestracji. W przypadku rezerwacji usług świadczonych bezpośrednio z poziomu e-platformy, ich dostępność definiowana będzie bezpośrednio w e-platformie. Pracownik Przychodni będzie miał możliwość udostępnienia informacji nt. terminów świadczenia usług, dla których płatnikiem jest Narodowy Fundusz Zdrowia.

Wymagany sposób działania:

1. Pacjent nie posiadający konta w e-platformie będzie miał możliwość sprawdzenia dostępności usług w placówce.
2. W celu rezerwacji terminu realizacji usługi, Pacjent będzie musiał stworzyć swoje indywidualne konto w e-platformie. Konta dla Kontrahentów tworzone będą przez uprawniony personel placówki.
3. Po zalogowaniu do e-platformy pacjent wskaże, w spisie dostępnych gabinetów, ten gabinet, do którego zamierza się udać.
4. Po wybraniu poradni specjalistycznej, pacjentowi zostanie zaprezentowany aktualny grafik pracy, pokazujący godziny pracy lekarzy przyjmujących w wybranym gabinecie.
5. Pacjentowi zostaną przedstawione tylko rzeczywiste wolne terminy uwzględniające rezerwacje w systemie z innych kanałów (rejestracja, telefon itp.).
6. Zarezerwowany termin zostanie zaprezentowany pacjentowi na liście wykonanych przezeń rezerwacji. Z poziomu tej listy pacjent będzie mógł anulować wykonaną rezerwację lub zmienić jej termin, klikając na odpowiednie przyciski z odnośnymi funkcjami.
7. Do zarezerwowanej w ten sposób wizyty pacjent będzie mógł, drogą elektroniczną, dołączyć posiadane dokumenty medyczne (usługa e-Dokumentacja) i ankiety (usługa e-Ankieta) za pomocą osobnych funkcjonalności.
8. Informacja nt. rezerwacji terminu automatycznie przesyłana jest do systemu HIS lub w przypadku rezerwacji e-usługi udostępnianej z e-platformy do odpowiedniego pracownika medycznego Przychodni jeśli jest to wymagane.
9. Po poprawnie zakończonym procesie rezerwacji, Pacjent otrzyma wiadomość SMS z potwierdzeniem tego faktu.

Wymagania szczegółowe dla usługi e-Rejestracja

Lp	Wymagania	Próbka
1.	Usługa musi umożliwić świadczeniobiorcom umawianie się drogą elektroniczną na wizyty, monitorowanie statusu na liście oczekujących na udzielenie świadczenia oraz powiadamianie o terminie udzielenia świadczenia zgodnie z wymaganiami art. 23a ust. 1 Ustawy z dnia 27 sierpnia 2004r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych (Dz. U. 2004 nr 210 poz. 2135, z późn. zm.) oraz Rozporządzeniem Ministra Zdrowia w sprawie minimalnej funkcjonalności dla systemów teleinformatycznych umożliwiających realizację usług związanych z prowadzeniem przez świadczenioborców list oczekujących na udzielenie świadczenia opieki zdrowotnej z dnia 7 lipca 2017 r. (Dz.U. z 2017 r. poz. 1404).	TAK

2.	Usługa musi zostać udostępniona w module e-platformy na stronie WWW Zamawiającego i być dostępna zarówno w sieci Internet jak i wewnętrznej każdej placówki Zamawiającego.	TAK
3.	Usługa musi być dostępna dla każdego pacjenta posiadającego konto w module e-platformy.	TAK
4.	Dostępność usługi e-Rejestracji musi być możliwa z poziomu stacji roboczych i urządzeń mobilnych, w tym tabletów.	
5.	Usługa, po zalogowaniu pacjenta do modułu e-platformy, musi zapewniać wyszukiwanie i wybór poradni/specjalizacji i/lub lekarza, do której / którego na wizytę chce się umówić pacjent.	TAK
6.	Usługa po dokonaniu wyboru poradni/specjalizacji i/lub lekarza musi prezentować wolne terminy wizyt oraz musi zapewnić możliwość wybrania przez pacjenta dogodnego dla siebie terminu spośród dostępnych, w którym chce skorzystać z wizyty oraz możliwość dokonania rezerwacji terminu. Informacja o dokonanej rezerwacji terminu wizyty oraz dane pacjenta muszą być dostępne w module obsługi pacjenta i obiegu dokumentacji medycznej.	TAK
7.	Usługa musi umożliwiać wprowadzenie informacji ze skierowania w zakresie: <ul style="list-style-type: none"> • kodu chorobowego (ICD10), • jednostki kierującej (REGON, VII i VIII część kodu resortowego), • lekarza kierującego (Nr prawa wykonywania zawodu), • daty skierowania. funkcjonalność dodatkowa	
8.	Terminarz dostępnych wizyt w poszczególnych poradniach/specjalizacjach i/lub lekarzy na e-platformie musi wskazywać wolne terminy zgodnie z aktualnym stanem ewidencjonowanym w module obsługi pacjenta i obiegu dokumentacji medycznej.	TAK
9.	Usługa musi na bieżąco (online) weryfikować dostępność wolnych terminów.	TAK
10.	Dokonując rezerwacji terminu wizyty usługa Systemu musi umożliwiać pacjentowi wprowadzenie uwag do wizyty (np. powód wizyty). Wprowadzone uwagi muszą być dostępne w odpowiednich funkcjach systemu w module obsługi pacjenta i obiegu dokumentacji medycznej.	TAK
11.	Usługa musi umożliwiać wymuszenie wypełnienia e-Ankiety przez pacjenta dla wybranych specjalizacji i/lub lekarzy jako informacja (wywiad wstępny) przed wizytą. Wynik tak wypełnionej e-Ankiety musi być dostępny w systemie dla lekarza w trakcie wizyty i może stanowić element dokumentacji medycznej – funkcjonalność dodatkowa	
12.	Usługa musi wyróżniać (dać możliwość wyboru) typu wizyty, tj. NFZ lub rozliczanej przez innych płatników.	TAK
13.	Usługa musi udostępniać terminarz w układzie dziennym lub tygodniowym lub miesięcznym.	
14.	W ramach usługi musi istnieć możliwość rejestracji pacjenta do Poradni Medycyny Pracy wraz z możliwością wyboru czynników szkodliwych lub uciążliwych znajdujących się na skierowaniu.	
15.	W ramach usługi musi istnieć możliwość uzupełnienia danych ze skierowania podczas rejestracji na badania profilaktyczne Medycyny Pracy w tym: Nazwa firmy, NIP oraz REGON pracodawcy.	TAK
16.	System musi posiadać możliwość automatycznego planowania badań powiązanych z wybranymi przez pacjenta czynnikami szkodliwymi podczas rejestracji do Poradni Medycyny Pracy.	
17.	Usługa musi udostępniać możliwość wyszukania pierwszego wolnego terminu do danej poradni/specjalizacji lub lekarza.	
18.	Pacjent musi mieć możliwość wglądu do listy swoich zaplanowanych wizyt zarówno tych zarezerwowanych online jak również zaplanowanych w module obsługi pacjenta i obiegu dokumentacji medycznej – wizyty umówione poprzez personel rejestracji placówki.	TAK
19.	Pacjent musi mieć możliwość zmiany online terminu zaplanowanej wcześniej wizyty poprzez wskazanie nowego terminu spośród dostępnych, a informacja o dokonanej zmianie terminu przez Pacjenta musi być dostępna w module obsługi pacjenta i obiegu dokumentacji medycznej.	TAK
20.	Usługa musi automatycznie wysłać do pacjenta potwierdzenie zmiany terminu wizyty na adres email i/lub SMS.	

21	Usługa musi umożliwiać pacjentowi dokonanie odwołania zaplanowanej wizyty, a informacja o odwołaniu wizyty musi być dostępna w module obsługi pacjenta i obiegu dokumentacji medycznej,	TAK
22	Usługa musi zapewniać, dla uprawnionego personelu Zamawiającego, możliwość definiowania i aktualizacji grafików dostępności świadczonych usług medycznych, w tym możliwość ograniczenia rejestracji online do wybranych poradni, ograniczenia do wybranych godzin w grafiku każdego lekarza oraz ograniczenia liczby jednocześnie wprowadzanych przez pacjenta rezerwacji w trybie rejestracji online (rejestracji w przód).	
23	System musi prowadzić dziennik logowań użytkowników do usługi e-Rejestracji - funkcjonalność dodatkowa	
24	System musi umożliwić bieżące śledzenie terminów rezerwowanych wizyt przez uprawnionego pracownika Zamawiającego.	TAK
25	System musi udostępniać terminarz dokonanych rejestracji, zmian terminu i odwołania wizyty na e-platformie dla każdej placówki indywidualnie.	

4.1.2. e-Badanie

Usługa e-Badanie dostępna będzie dla Pacjentów Przychodni, posiadających konta w e-platformie i udostępniać będzie usługę udostępnienia wyników wykonanych badań diagnostycznych i laboratoryjnych. Dzięki temu Pacjent będzie miał szybki dostęp do informacji o swoim stanie zdrowia.

Wymagany sposób działania:

1. System HIS/EDM będzie umożliwiał wprowadzanie danych opisujących badania wykonane przez diagnostykę: ręcznie (opisy będą wprowadzane z klawiatury) lub jako skany dokumentów papierowych. System będzie również zawierał narzędzia i mechanizmy umożliwiające integrację z systemami LIS (aktualnie system informatyczny e-Lab firmy Eclipse Spółka z ograniczoną odpowiedzialnością sp.k., ul. Prof. M. Życzkowskiego 16, Kraków) i RIS/PACS (aktualnie użytkowany system firmy PIXEL Technology Sp. z o. o. z siedzibą w Łodzi, ul. Piękna 1), umożliwiające wysyłanie do tych systemów zleceń elektronicznych i odbiór wyników takiej samej formie. Wszystkie te wyniki będą powiązane z historią choroby pacjenta.
2. Pacjent po zalogowaniu się do e-platformy będzie mógł w module e-Badanie wybrać z listy jeden z udostępnionych mu dokumentów z wynikiem badania.
3. Wybrany dokument będzie mógł zostać wyświetlony, wydrukowany lub pobrany w postaci pliku PDF i zapisany na lokalnym nośniku danych.

Wymagania szczegółowe dla usługi e-Badanie

Lp	Wymagania	Próbka
1.	Usługa e-Badanie dostępna będzie dla Pacjentów oraz uprawnionych pracowników medycznych Przychodni posiadających konta w e-platformie	
2.	Dostęp do usługi e-Badanie musi być możliwy z poziomu e-platformy za pośrednictwem strony WWW Zamawiającego, w sieci Internet oraz w sieci wewnętrznej (intranet). Dostęp do usługi będzie możliwy wyłącznie po zalogowaniu się użytkownika do e-platformy – użytkownik musi posiadać konto w e-platformie.	
3.	Dostępność usługi musi być możliwa z poziomu stacji roboczych i urządzeń mobilnych, w tym tabletów.	
4.	Poprzez usługę musi istnieć dostęp dla pacjenta do wyników badań diagnostycznych i laboratoryjnych zgromadzonych w placówkach Zamawiającego i przechowywanych w Systemie.	TAK



5.	Usługa musi umożliwiać pacjentowi przeszukanie historii wizyt i wyświetlenie informacji o wynikach badań wykonanych w związku z wybraną wizytą, udostępnionych w ramach wskazanej wizyty - funkcjonalność dodatkowa	
6.	Usługa musi umożliwiać pobranie przez pacjenta wyników badań w postaci pliku co najmniej PDF oraz jej wydrukowanie.	TAK
7.	Usługa musi umożliwiać opatrzenie udostępnianych wyników badań bezpiecznym podpisem elektronicznym weryfikowanym kwalifikowanym certyfikatem.	

4.1.3. e-Powiadomienia

Usługa e-Powiadomienia dostępna jest dla pacjentów oraz uprawnionych pracowników medycznych Zamawiającego, posiadających konta w e-platformie i udostępniać będzie funkcjonalności informowania pacjenta lub pracownika medycznego o zbliżającym się terminie realizacji usługi zarejestrowanej w Systemie.

Wymagany sposób działania:

1. Użytkownik korzystający z usługi e-Powiadomienia, powiadamiany będzie przy pomocy wiadomości poczty elektronicznej i/lub wiadomości SMS o zbliżających się terminach związanych z prowadzonym leczeniem w danej placówce.
2. Działanie usługi musi spełniać obowiązek wynikający wprost z art. 23a ust. 1 Ustawy z dnia 27 sierpnia 2004r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych (Dz. U. 2004 nr 210 poz. 2135, z późn. zm.). Zgodnie z nim: Świadczeniodawca, o którym mowa w art. 20, jest obowiązany umożliwić świadczeniobiorcom umawianie się drogą elektroniczną na wizyty, monitorowanie statusu na liście oczekujących na udzielenie świadczenia oraz powiadamianie o terminie udzielenia świadczenia. Minimalną funkcjonalność usługi określa Rozporządzenie Ministra Zdrowia w sprawie minimalnej funkcjonalności dla systemów teleinformatycznych umożliwiających realizację usług związanych z prowadzeniem przez świadczeniobiorców list oczekujących na udzielenie świadczenia opieki zdrowotnej z dnia 7 lipca 2017 r. (Dz.U. z 2017 r. poz. 1404).

Wymagania szczegółowe dla usługi e-Powiadomienia

Lp	Wymagania	Próbka
1.	Usługa musi zostać udostępniona w module e-platformy na stronie WWW Zamawiającego i być dostępna zarówno w sieci Internet jak i wewnętrznej każdej placówki Zamawiającego.	
2.	Usługa musi być dostępna dla pacjentów oraz uprawnionych pracowników medycznych Zamawiającego posiadających konta w e-platformie.	
3.	Usługa musi udostępniać funkcjonalność przekazywania pacjentom informacji przypominającej o planowanej wizycie, zmianie jej terminu lub jej odwołaniu za pomocą wybranego medium komunikacyjnego (SMS, mail, dwoma sposobami równocześnie) w zależności od preferencji użytkownika (parametru profilu użytkownika).	
4.	Poprzez usługę musi istnieć możliwość przekazywania pacjentom innych informacji na żądanie uprawnionego przedstawiciela Zamawiającego. Adresatami powiadomienia mogą być: wskazany pacjent, grupa pacjentów wybrana z użyciem filtra daty i godziny oraz/lub jednostki organizacyjnej, wszyscy pacjenci - funkcjonalność dodatkowa	
5.	Powiadomienia drogą elektroniczną przesyłane muszą być za pomocą wiadomości (email, SMS i/lub email), w zależności od preferencji użytkownika, zapisanych jako parametr konfiguracyjny w jego profilu.	
6.	Powiadomienia będą generowane automatycznie przez poszczególne e-usługi. Dodatkowo uprawniony użytkownik będzie mógł wysłać powiadomienia do osoby lub grup osób „na żądanie”.	

7.	Musi istnieć możliwość określania, przez Administratora Systemu, treści korespondencji email i SMS-owej do pacjentów, którzy mają zarejestrowaną wizytę.	
----	--	--

4.1.4. e-Dokumentacja

Usługa e-Dokumentacja dostępna będzie dla Pacjentów posiadających konto w e-platformie i udostępniała będzie usługi pozwalające na dostęp Pacjenta do zgromadzonej i udostępnionej przez placówkę dokumentacji medycznej, tj. wystanie i odbiór dokumentacji indywidualnej w postaci elektronicznej, jako alternatywę postaci papierowej.

Wymagany sposób działania:

1. Zakres udostępnianej dokumentacji wynikać będzie z konfiguracji usługi. Pacjenci muszą mieć możliwość dostępu do własnej dokumentacji, a lekarze Zamawiającego dostęp do dokumentacji tych pacjentów, którzy byli przez nich leczeni w tej placówce. Lekarze współpracujący (z innych podmiotów) muszą mieć dostęp do dokumentacji tych pacjentów, do których dostęp został im indywidualnie przyznany przez pacjenta.
2. Po zalogowaniu do e-platformy osoba chcąca mieć dostęp do dokumentacji będzie widziała listę tych dokumentów, do których dostęp wynika z powyższych zasad. Pozycje na liście będą opisane parametrami, pozwalającymi jednoznacznie określić wizytę (data, gabinet, lekarz) i dokument wystawiony w ramach tej wizyty. Docelowo usługa będzie zintegrowana z Platformą P1.
3. Po wskazaniu dokumentu na liście użytkownik po kliknięciu na odpowiedni przycisk będzie mógł wskazać dokument: wyświetlić, wydrukować, pobrać w postaci pliku PDF i zapisać na lokalnym nośniku danych.

Wymagania szczegółowe dla usługi e-Dokumentacja

Lp	Wymagania	Próbka
1.	Usługa musi zostać udostępniona w module e-platformy na stronie WWW Zamawiającego i być dostępna zarówno w sieci Internet jak i wewnętrznej każdej placówki Zamawiającego.	
2.	Usługa musi być dostępna dla pacjentów oraz uprawnionych pracowników medycznych Zamawiającego posiadających konta w e-platformie po zalogowaniu do e-platformy.	
3.	Dostępność usługi musi być możliwa z poziomu stacji roboczych i urządzeń mobilnych, w tym tabletów.	
4.	Poprzez usługę musi istnieć dostęp dla pacjenta lub lekarza placówki współpracującej do dokumentacji zgromadzonej w placówkach Zamawiającego i przechowywanej w Systemie, tj.: zapisów historii choroby, zaleceń lekarskich, orzeczeń, opisów wyników badań, opisów dawkowania leków, historii wizyt, informacji o schorzeniach przewlekłych itp.	

5.	Poprzez usługę musi istnieć możliwość wysłania i odbioru dokumentacji indywidualnej w postaci elektronicznej, jako alternatywy postaci papierowej, tj.: <ul style="list-style-type: none"> informacja dla lekarza kierującego/POZ, orzeczenie, opinia, wyniki badań diagnostycznych, dokumenty dostarczane do przychodni, deklaracja wyboru - deklaracja wyboru – Podstawowa Opieka Zdrowotna, oświadczenie o upoważnieniu innej osoby do uzyskiwania informacji o stanie zdrowia, skierowanie (do czasu uruchomienia platformy P1), dokumenty własne pacjenta. 	
6.	Usługa musi umożliwiać pacjentowi przeszukanie historii wizyt we wskazanym ośrodku i wyświetlenie informacji medycznych udostępnionych przez ten ośrodek w ramach wskazanej wizyty.	TAK
7.	Usługa musi umożliwiać pobranie przez pacjenta dokumentacji w postaci pliku co najmniej PDF oraz jej wydrukowanie.	TAK
8.	Usługa musi umożliwiać opatrzenie udostępnianych dokumentów bezpiecznym podpisem elektronicznym weryfikowanym kwalifikowanym certyfikatem.	
9.	Usługa musi umożliwiać przekazanie przez pacjenta dostępu do swojej dokumentacji dowolnemu lekarzowi.	
10	Usługa musi udostępniać możliwość dołączenia przez pacjenta posiadanej dokumentacji medycznej, oświadczeń i ankiet do wizyty, której termin pacjent uprzednio zarezerwował.	TAK
11	Usługa e-Dokumentacja umożliwiać będzie udostępnienie pacjentowi dokumentów innych niż medyczne (np. instrukcja przygotowania się do badania) – funkcjonalność dodatkowa	
12	Dostęp do dokumentacji archiwalnej pacjenta będzie możliwy po złożeniu formalnego wniosku przez pacjenta, kierownika zainteresowanej placówki medycznej lub innej uprawnionej osoby lub instytucji zgodnie z ustawą o Prawach Pacjenta i Rzeczniku Praw Pacjenta.	

4.1.5. e-Archiwum

Usługa e-Archiwum będzie dostępna dla pacjentów oraz jednostek współpracujących i finansujących świadczenia medyczne, posiadających konto dostępu do e-usług. Zadaniem usługi e-archiwum będzie udostępnianie na żądanie ucyfrowionej dokumentacji medycznej pierwotnie wytworzonej w postaci papierowej (np. dokumentacji medycznej wytworzonej w placówce przed uruchomieniem systemu HIS). Skany dokumentacji papierowej zostaną dołączone do rekordu pacjenta i będą gromadzone i przechowywane w module EDM. Usługa zapewni możliwość przeglądania przez pacjenta tak zdigitalizowanej dokumentacji. Usługa będzie umożliwiała dostęp do pełnej dokumentacji medycznej, w tym archiwalnej, zeskanowanej papierowej dokumentacji medycznej sporządzonej przed okresem wprowadzenia dokumentacji elektronicznej, zawierającej m.in.: historię choroby, archiwalne wyniki badań diagnostycznych, karty zabiegowe, oświadczenia, skierowania.

Wymagany sposób działania usługi:

Usługa e-Archiwum będzie działała w zakresie udostępniania dokumentacji archiwalnej w sposób analogiczny do działania usługi e-Dokumentacja.

4.1.6. e-Kolejka

Usługa będzie dostępna będzie dla Pacjentów, uprawnionych pracowników medycznych Zamawiającego posiadających konta w e-platformie i udostępniać będzie możliwość sprawdzenie miejsca w kolejce do lekarza. Obowiązek umożliwienia pacjentom monitorowanie swojego miejsca w kolejce oczekujących wynika

wprost z art. 23a Ustawa z dnia 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych (Dz.U. 2004 nr 210 poz. 2135, z późn. zm.). Zgodnie z nim Świadczeniodawca, o którym mowa w art. 20, jest obowiązany umożliwić świadczeniobiorcom umawianie się drogą elektroniczną na wizyty, monitorowanie statusu na liście oczekujących na udzielenie świadczenia oraz powiadamianie o terminie udzielenia świadczenia. Minimalną funkcjonalność usługi określa Rozporządzenie Ministra Zdrowia w sprawie minimalnej funkcjonalności dla systemów teleinformatycznych umożliwiających realizację usług związanych z prowadzeniem przez świadczeniobiorców list oczekujących na udzielenie świadczenia opieki zdrowotnej z dnia 7 lipca 2017 r. (Dz.U. z 2017 r. poz. 1404).

Sposób korzystania z usługi:

1. Po zalogowaniu się do e-platformy i wybraniu funkcjonalności e-Kolejki:
 - pacjent widzi listę wizyt, na które jest umówiony na wizytę w poradniach Zamawiającego;
 - uprawniony pracownik Zamawiającego lub jego partnera widzi listę zaplanowanych wizyt, z którymi jest powiązany.
2. Po wybraniu wizyty z listy wyświetlane jest okno z podstawowymi informacjami o tej wizycie wraz z informacją o miejscu w kolejce do wybranego lekarza.
3. Pacjent może zrezygnować z umówionej wizyty (wykreślenie z kolejki). Informacja o rezygnacji pacjenta z wizyty (zwolnienie terminu) jest dostępna w podsystemie obsługi pacjenta i obiegu dokumentacji medycznej Zamawiającego.

Wymagania szczegółowe dla usługi e-Kolejka

Lp	Wymagania	Próbka
1.	Usługa udostępniona musi zostać w module e-platformy za pośrednictwem Portalu Informacyjnego Placówki.	
2.	Dostęp do usługi musi być możliwy zarówno z sieci Internet jak i Intranet (sieć wewnętrzna Zamawiającego).	
3.	Dostęp do usługi musi być możliwy wyłącznie dla posiadaczy konta na e-platformie.	
4.	Dostęp do usługi musi wymagać logowania do e-platformy poprzez podanie parametrów dostępowych (użytkownik i hasło).	
5.	Usługa musi być dostępna dla pacjentów umówionych na wizytę w poradni Zamawiającego	
6.	Usługa musi umożliwić sprawdzenie miejsca w kolejce do wybranego lekarza zgodnie z art. 23a Ustawy z dnia 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych (Dz.U. 2004 nr 210 poz. 2135, z późn. zm.).	
7.	Usługa musi umożliwiać pacjentowi rezygnację z umówionej wizyty - wykreślenie z kolejki. Informacja o rezygnacji pacjenta z wizyty (zwolnienie terminu) musi być dostępna w podsystemie obsługi pacjenta i obiegu dokumentacji medycznej Zamawiającego.	
8.	Informacja o rezygnacji z umówionej wizyty musi być udostępniana w terminarzu wizyt poszczególnych pracowników medycznych Zamawiającego.	
9.	Terminarz dla poszczególnych pracowników musi być udostępniany poprzez konto do e-platformy dla pracowników medycznych Zamawiającego.	
10	W przypadku rezygnacji pacjenta z umówionej wizyty, usługa musi wysłać do pacjenta potwierdzenie rezygnacji z wizyty (kolejki) na adres email i/lub SMS.	



11	Usługa musi umożliwiać administratorowi systemu zdefiniowanie treści komunikatów wysyłanych do pacjenta w sytuacji rezygnacji z kolejki.	
----	--	--

4.1.7. e-Wywiad/e-Ankieta

E-Ankieta będzie dostępna dla Pacjentów posiadających konto w e-platformie i umożliwiać będzie pacjentom wypełnienie i wysłanie ankiet – zarówno związanych z procesem leczenia (np. elementy wywiadu) jak i innych (np. ankieta zadowolenia z jakości udzielonych świadczeń).

Ankieta wywiadu będzie dostępna dla Pacjentów po zalogowaniu przy pomocy parametrów dostępowych. Usługa będzie umożliwiać pacjentom wypełnienie i wysłanie do Zamawiającego informacji wymaganych w związku z planowanym procesem leczenia. Pacjent po zalogowaniu się za pomocą indywidualnego profilu i uruchomieniu usługi e-Ankieta zobaczy listę ankiet możliwych do wypełnienia oraz ankiet wypełnionych dotychczas przez niego. Będzie mógł wskazać odpowiednią ankietę wywiadu z listy - po wskazaniu jej zostanie mu wyświetlony formularz powiązany z tą ankietą. Pacjent będzie mógł wypełnić go odpowiednimi danymi zgodnie z wymuszonym przez formularz schematem postępowania.

Po wypełnieniu formularza System poprosi pacjenta o potwierdzenie poprawności wprowadzonych informacji. Po otrzymaniu takiego potwierdzenia System zapisze ankietę w bazie danych systemu HIS. Taka ankieta/wywiad będzie automatycznie dołączona do danych pacjenta w podsystemie ewidencji pacjentów i obiegu dokumentacji.

Wskazanie na liście ankiet jednej z już wcześniej wypełnionych i kliknięcie na odpowiedni przycisk umożliwi pacjentowi wyświetlenie (bez prawa modyfikacji), wydruk lub zapisanie do pliku PDF wskazanej ankiety. Dzięki wydrukowi zaoszczędzony zostanie czas na sporządzanie ankiet w ośrodku.

Usługa e-Ankieta poprzez e-platformę będzie umożliwiać także wysyłanie indywidualnej korespondencji mailowej do pacjenta. W przypadku, gdy skutkiem oceny ankiety ma być wizyta lub hospitalizacja, powiadomienie o tym zostanie przesłane pacjentowi za pomocą usługi e-Powiadomienia.

Formularze ankiet będą definiowane przez administratora Systemu. Możliwe będzie używanie w ankietach elementów typu radio button i checkbox oraz list wyboru. Reguły obligatoryjności i walidacji poprawności wprowadzanych danych będą stanowiły element definicji formularza ankiety. Administrator Systemu będzie miał też możliwość określenia, czy dana ankieta będzie dotyczyć pacjenta ogólnie, czy też będzie powiązana z konkretnym miejscem wykonania usługi (z dokładnością do poradni i /lub lekarza) oraz czy ma być elementem dokumentacji medycznej.

Usługa w pełnym zakresie będzie dla pacjentów możliwa do uruchomienia z poziomu stacji roboczych i urządzeń mobilnych, w tym tabletów.

Sposób korzystania z usługi:

1. Pacjent po zalogowaniu się za pomocą indywidualnego profilu uruchamia usługę e-Ankieta
2. System wyświetla listę ankiet możliwych do wypełnienia oraz listę ankiet wypełnionych dotychczas przez niego.
3. Pacjent wskazuje ankietę z listy możliwych do wypełnienia.
4. System wyświetla zdefiniowany przez Administratora formularz, powiązany z wybraną ankietą.

5. Pacjent wypełnia ankietę zgodnie z opisami w niej zawartymi. Obligatoryjność i poprawności wprowadzanych danych są sprawdzane zgodnie z regułami wprowadzonymi w definicji formularza na etapie jego tworzenia.
6. Pacjent zapisuje wypełnioną ankietę, klikając na przycisk „Zapisz”.
7. System prosi o potwierdzenie poprawności wprowadzonych informacji.
8. Po otrzymaniu potwierdzenia System zapisuje ankietę w bazie danych.
9. System powraca do głównego okna usługi, wyświetlając zaktualizowaną listę ankiet możliwych do wypełnienia i ankiet dotychczas wypełnionych przez pacjenta.

Wymagania szczegółowe dla usługi e-Ankieta

Lp	Wymagania	Próbka
1.	Usługa udostępniona musi zostać w module e-platformy za pośrednictwem Portalu Informacyjnego Placówki.	
2.	Dostęp do usługi możliwy musi być zarówno z sieci Internet jak i Intranet (sieć wewnętrzna Zamawiającego).	
3.	Dostęp do usługi musi być możliwy wyłącznie dla posiadaczy konta na e-platformie.	
4.	Dostęp do usługi musi wymagać logowania do e-platformy poprzez podanie parametrów dostępowych (użytkownik i hasło).	
5.	Usługa musi umożliwić pacjentom wypełnienie i wysłanie do Zamawiającego dowolnej ankiety zdefiniowanej przez Administratora systemu.	
6.	Usługa musi umożliwić pacjentom wydrukowanie każdej wypełnionej i wysłanej ankiety.	
7.	Musi istnieć funkcjonalność dostępna dla administratora systemu umożliwiająca tworzenie ankiet medycznych, powiązanie ich z jednostkami organizacyjnymi, nadawanie im okresu ważności (udostępnienia pacjentom).	
8.	System musi umożliwiać łączenie danych wprowadzonych przez pacjenta za pośrednictwem usługi e-Ankiety z historią choroby tego pacjenta - funkcjonalność dodatkowa	
9.	Dane zebrane w usłudze e-ankiety muszą być dostępne dla personelu medycznego Zamawiającego.	
10.	Usługa musi umożliwić wysyłanie indywidualnej i zbiorczej korespondencji mailowej do uczestników ankiet medycznych.	
11.	Musi istnieć możliwość określania przez administratora systemu treści korespondencji email do uczestników ankiet medycznych i warunki jej zastosowania.	
	Usługa udostępniona musi zostać w module e-platformy za pośrednictwem Portalu Informacyjnego Placówki.	

4.2. Wymagania podsystemu RDM/EDM

Dostarczone oprogramowanie musi posiadać funkcjonalności wspomagające zarządzanie zbiorem dokumentacji elektronicznej poprzez funkcjonalności i cechy przedstawione poniżej. Ponadto Wykonawca

wraz z oprogramowaniem dostarczy Repozytorium Dokumentacji Medycznej (RDM) jako zasób, w którym gromadzone i przechowywane będą (w sposób bezpieczny) obrazy zeskanowanej dokumentacji medycznej oraz elektroniczna dokumentacja medyczna przetwarzana w systemie.

Wymagania szczegółowe obszaru RDM/EDM

Lp.	Wymagania	Próbka
1.	Przechowywanie drukowanych dokumentów w formie PDF wraz z informacjami pozwalającymi na zidentyfikowanie osoby generującej dany wydruk.	TAK
2.	W przypadku dokonania ponownego wydruku dokumentu, tworzony jest nowy PDF odkładany jako kolejna wersja dokumentu przechowywana w module EDM.	TAK
3.	Możliwość podpisania certyfikatem elektronicznym (kwalifikowanym lub niekwalifikowanym) wygenerowanego dokumentu PDF.	TAK
4.	Możliwość wyszukiwania dokumentów PDF.	TAK
5.	Brak możliwości modyfikowania zarejestrowanych dokumentów w module EDM.	TAK
6.	Możliwość ewidencjonowania archiwum papierowego.	TAK
7.	Możliwość nadania statusu dokumentacji medycznej (wypożyczenie, zwrot, zniszczenie/odnalezienie, stworzenie kopii, planowe zniszczenie, archiwizacja).	TAK
8.	Ewidencję adnotacji o osobie wypożyczającej wydającej dokumentację medyczną.	TAK
9.	Automatyczny druk dokumentu PDF podczas wydruków z przypisaniem go do historii choroby.	TAK
10.	Przechowywanie dokumentów elektronicznych wraz z wersjonowaniem.	TAK
11.	Możliwość podpisu elektronicznego dokumentu PDF.	TAK

4.3. Wymagania dla oprogramowania do digitalizacji dokumentacji medycznej papierowej

Wdrożony podsystem musi posiadać moduł obsługi digitalizacji dokumentacji medycznej papierowej, który musi posiadać funkcjonalności i cechy przedstawione poniżej.

Wymagania szczegółowe oprogramowania do digitalizacji dokumentacji medycznej papierowej

Lp.	Wymagania	Próbka
1.	Oprogramowanie będzie współpracowało z dostarczonym w ramach projektu urządzeniem skanującym.	
2.	Tylko uprawnieni pracownicy Zamawiającego będą mieli dostęp do funkcjonalności w zakresie skanowania dokumentacji zgromadzonej przez Zamawiającego oraz bieżącej dokumentacji papierowej dostarczanej przez Pacjentów do ośrodka, indeksowania, archiwizowania i przeglądania dokumentacji RDM.	
3.	Oprogramowanie musi umożliwiać zasilenie RDM cyfrową wersją dokumentacji wytworzonej w postaci papierowej;	
4.	Oprogramowanie musi umożliwiać skanowanie i indeksowanie dokumentów, archiwalnych i wypisywanych odręcznie bezpośrednio na panelach dotykowych urządzeń skanujących wpiętych do systemu	
5.	Zeskanowane i przekazane do RDM dokumenty muszą posiadać odpowiednią nazwę określającą typ dokumentu i być przypisane do przyjmującego oddziału/jednostki organizacyjnej placówki i być dostępne z poziomu aplikacji HIS/RDM.	
6.	Wszystkie dokumenty przetwarzane przez oprogramowanie muszą być przekazywane do modułu RDM wraz z opatrzeniem ich informacją o osobie skanującej.	

7.	Oprogramowanie musi współpracować z modułem RDM w zakresie współdzielenia słowników: typów dokumentów, jednostek organizacyjnych, pacjentów, personelu.	
8.	Oprogramowanie musi posiadać wbudowanym mechanizmom OCR tekstu i odczytu kodów jedno i dwu wymiarowych przeznaczony do automatycznego przetwarzania i odczyt danych z dokumentów.	
9.	Musi istnieć funkcjonalność usuwania pustych stron z przetwarzanych dokumentów.	
10.	Oprogramowanie musi posiadać modułu administratora dający możliwość konfigurowania użytkowników i działania systemu.	
11.	Oprogramowanie musi posiadać wbudowane narzędzia zabezpieczające bazę danych przed wprowadzeniem do niej dokumentów z błędnymi danymi. Informacje o ewentualnych błędach i niezgodnościach w przetwarzaniu, zapisie lub odczycie danych z dokumentów muszą być wyświetlane w postaci komunikatów co najmniej na panelach urządzeń skanujących.	
12.	Musi istnieć możliwość regulacji stopnia kompresji archiwizowanych plików.	
13.	Musi istnieć możliwość automatycznego dzielenia kompletów dokumentów podawanych seryjnie do podajnika urządzenia skanującego i zapisanie ich jako odrębne pliki oraz archiwizacji dokumentacji wraz z załącznikami – z dziedziczeniem przez załączniki danych odczytanych z dokumentu głównego.	
14.	<p>Oprogramowanie musi umożliwiać realizację poniższego procesu na urządzeniu skanującym:</p> <ol style="list-style-type: none"> 1 Pracownik na urządzeniu skanującym wprowadza nr PESEL lub nr kartoteki pacjenta lub na podstawie kodu kresowego umieszczonego na dokumentacji (np. w formie naklejki), urządzenie skanujące identyfikuje pacjenta – „sięga” po informacje do bazy pacjentów systemu HIS; 2 Po identyfikacji pacjenta, na wyświetlaczu urządzenia skanującego wyświetlane jest Imię i Nazwisko pacjenta którego PESEL/nr Kartoteki lub kod kreskowy został zidentyfikowany; 3 Pracownik weryfikuje, wyświetlane na wyświetlaczu urządzenia skanującego, dane pacjenta z danymi na dokumentacji papierowej. 4 Pracownik potwierdza poprawność danych identyfikacyjnych na ekranie urządzenia skanującego. 5 Pracownik odpowiednio do skanowanego dokumentu: <ol style="list-style-type: none"> 5.1 wybiera rodzaj/typ dokumentacji (ze słownika) oraz komórkę organizacyjną placówki które ona dotyczy (ze słownika), 5.2 wprowadza datę lub przedział dat których dotyczy skanowana dokumentacja. 6 Następuje skanowanie dokumentu i zapisanie jego odwzorowania cyfrowego z odpowiednimi parametrami w Repozytorium Dokumentacji Medycznej. 	
15.	<p>Oprogramowanie musi umożliwiać realizację poniższego procesu na urządzeniu skanującym:</p> <ol style="list-style-type: none"> 1. Pracownik na urządzeniu skanującym wprowadza nr PESEL lub nr Kartoteki pacjenta lub na podstawie kodu kresowego umieszczonego na dokumentacji (np. w formie naklejki), urządzenie skanujące identyfikuje pacjenta - „sięga” po informacje do bazy pacjentów systemu HIS; 2. Po identyfikacji pacjenta na wyświetlaczu urządzenia skanującego wyświetlane jest Imię i Nazwisko pacjenta, którego PESEL/nr Kartoteki lub kod kreskowy został zidentyfikowany. 3. Pracownik weryfikuje wyświetlane na wyświetlaczu urządzenia skanującego dane pacjenta z danymi na dokumentacji papierowej. <ol style="list-style-type: none"> a. Pracownik potwierdza poprawność danych identyfikacyjnych na ekranie urządzenia skanującego. b. Nie są wykonywane czynności związane z zaklasyfikowaniem dokumentu i określeniu jego daty; c. Następuje skanowanie dokumentu i zapisanie jego odwzorowania cyfrowego w Repozytorium Dokumentacji Medycznej jako dokumentacja ogólna z nieokreśloną datą – bez parametrów. <p>W tym przypadku zawsze musi istnieć możliwość uporządkowania zeskanowanej dokumentacji poprzez opatrzenie jej właściwymi parametrami – z wykorzystaniem dostępu do modułu RDM.</p>	

16.	<p>Oprogramowanie musi umożliwiać realizację poniższego procesu na urządzeniu skanującym:</p> <ol style="list-style-type: none"> 1 Pracownik przy pomocy urządzenia skanującego skanuje dokumenty medyczne pacjentów. Zeskanowane dokumenty nie są powiązane z konkretnym pacjentem. 2 Zeskanowane dokumenty umieszczane są w tymczasowym zasobie modułu RDM. <p>W tym przypadku Pracownik korzystając z modułu RDM, zawsze musi dla każdego zeskanowanego dokumentu, wybrać pacjenta, określić typ dokumentu, komórkę organizacyjną oraz przedział dat których dotyczy wybrana dokumentacja pacjenta.</p>	
-----	--	--

Założenia i wymagania dla środowiska infrastruktury sprzętowej i prac modernizacyjnych

5.1 Wykaz sprzętu i oprogramowania

Wykonawca dostarczy w ramach realizacji zamówienia sprzęt i oprogramowanie w ilości i o parametrach przedstawionych poniżej.

5.1.1 Serwery na potrzebę wirtualizacji – 3 sztuki

Serwer	
Nazwa komponentu	Wymagane minimalne parametry techniczne
Obudowa	<p>Obudowa Rack o wysokości max 2U z możliwością instalacji min. 8 dysków wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli.</p> <p>Obudowa musi mieć możliwość wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej (Android/ Apple iOS) przy użyciu jednego z protokołów NFC/ BLE/ WIFI w technologii pozwalającej na zdalne konfigurowanie oraz monitoring najważniejszych komponentów serwera poprzez przeglądarkę internetową która dostępna jest na każdym urządzeniu mobilnym typu notebook, tablet czy smartfon.</p>
Płyta główna	Płyta główna z możliwością zainstalowania minimum dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.
Chipset	Dedykowany przez producenta procesora do pracy w serwerach dwuprocessorowych
Procesor	Zainstalowane dwa procesory dziesięciordzeniowe klasy x86 dedykowane do pracy z zaferowanym serwerem umożliwiający osiągnięcie wyniku min. 99 punktów w teście SPECrate2017_int_peak dostępnym na stronie www.spec.org dla dwóch procesorów.
RAM	384GB DDR4 RDIMM 2666MT/s w kościach min. 32GB, na płycie głównej powinno znajdować się minimum 24 slotów przeznaczonych do instalacji pamięci. Płyta główna powinna obsługiwać do 3TB pamięci RAM.
Zabezpieczenia pamięci RAM	Memory Rank Sparing, Memory Mirror, SDDC.
Gniazda PCI	Min. 2 sloty x8 generacji 3 oraz 2 sloty x16 generacji 3.
Interfejsy	Wbudowane cztery interfejsy sieciowe 1Gb Ethernet w standardzie BaseT.

sieciowe/FC/SAS	<p>Możliwość instalacji wymiennie modułów udostępniających:</p> <ul style="list-style-type: none"> - dwa interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz dwa interfejsy sieciowe 10Gb Ethernet ze złączami w standardzie SFP+. - cztery interfejsy sieciowe 10Gb Ethernet w standardzie SFP+. - cztery interfejsy sieciowe 1Gb Ethernet w standardzie BaseT - dwa interfejsy sieciowe 25Gb Ethernet ze złączami SFP28. <p>Dodatkowo zainstalowana jedna karta dwuportowa 10Gb Ethernet w standardzie SFP+ oraz jedna karta dwuportowa FC 8Gb.</p>
Napęd optyczny	DVD-RW
Dyski twarde	<p>Zainstalowany moduł dedykowany dla hypervisora wirtualizacyjnego, wyposażony w 2 jednakowe nośniki typu flash o pojemności min. 32GB z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnek na dyski twarde.</p> <p>Zainstalowane dwa dyski SAS 15k o pojemności min. 300GB skonfigurowane w RAID 1.</p>
Kontroler RAID	Sprzętowy kontroler dyskowy, posiadający min. 2GB nieulotnej pamięci cache, możliwe konfiguracje poziomów RAID: 0, 1, 5, 6, 10, 50, 60.
Karty GPU	Nie wymagane.
Serwerowy System Operacyjny SSO	Zainstalowany Windows Server 2016 Std z pełną licencją na oferowany serwer. Licencje mają uprawniać do uruchamiania serwerowego systemu operacyjnego SSO na minimum 4 maszynach wirtualnych.
Wbudowane porty	min. 1 porty USB 2.0, 2 porty USB 3.0 oraz 1 port Micro-usb, 4 porty RJ45, 2 porty VGA (1 na przednim panelu obudowy, drugi na tylnym), min. 1 port RS232
Video	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200.
Wentylatory	Redundantne
Zasilacze	Redundantne, Hot-Plug minimalnie 750W każdy.
Bezpieczeństwo	TPM 2.0.
Karta Zarządzania	<p>Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet umożliwiające:</p> <ul style="list-style-type: none"> • zdalny dostęp do graficznego interfejsu Web karty zarządzającej • zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera) • szyfrowane połączenie (SSLv3) oraz autentykację i autoryzację użytkownika • możliwość podmontowania zdalnych wirtualnych napędów • wirtualną konsolę z dostępem do myszy, klawiatury • wsparcie dla IPv6 • wsparcie dla SNMP; IPMI2.0, VLAN tagging, Telnet, SSH • możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer • możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer • integracja z Active Directory • możliwość obsługi przez dwóch administratorów jednocześnie • wsparcie dla dynamic DNS • wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej • możliwość podłączenia lokalnego poprzez złącze RS-232. • Producent systemu musi posiadać dedykowane rozwiązanie które będzie

	<p>przeciwdziało automatycznym skryptom konfiguracyjnym działającym w sieci. Jest niedopuszczalne aby konsole zarządzające serwerów miały identyczne dane dostępowe.</p> <ul style="list-style-type: none"> • Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych • Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta • Wsparcie dla protokołów– WMI, SNMP, IPMI, Linux SSH • Możliwość oskryptowywania procesu wykrywania urządzeń • Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram • Szczegółowy opis wykrytych systemów oraz ich komponentów • Możliwość eksportu raportu do CSV, HTML, XLS • Grupowanie urządzeń w oparciu o kryteria użytkownika • Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach • Automatyczne skrypty CLI umożliwiające dodawanie i edycję grup urządzeń • Szybki podgląd stanu środowiska • Podsumowanie stanu dla każdego urządzenia • Szczegółowy status urządzenia/elementu/komponentu • Generowanie alertów przy zmianie stanu urządzenia • Filtry raportów umożliwiające podgląd najważniejszych zdarzeń • Możliwość przejęcia zdalnego pulpitu • Możliwość podmontowania wirtualnego napędu • Automatyczne zaplanowanie akcji dla poszczególnych alertów w tym automatyczne tworzenie zgłoszeń serwisowych w oparciu o standardy przyjęte przez producentów oferowanych w tym postępowaniu sprzętu • Kreator umożliwiający dostosowanie akcji dla wybranych alertów • Możliwość importu plików MIB • Możliwość definiowania ról administratorów • Możliwość zdalnej aktualizacji sterowników i oprogramowania wewnętrznego serwerów • Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania) • Możliwość instalacji sterowników i oprogramowania wewnętrznego bez potrzeby instalacji agenta • Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów <ul style="list-style-type: none"> ▪ Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie gwarancji, adresy IP kart sieciowych ▪ Możliwość automatycznego przywracania ustawień serwera ,kart sieciowych, BIOS, wersji firmware w przypadku awarii i wymiany któregoś z komponentów (w tym kontrolera RAID, kart sieciowych, płyty głównej)
<p>Certyfikaty</p>	<p>Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2008 oraz ISO-14001. Serwer musi posiadać deklaracja CE. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów, Microsoft Windows 2012 x64, Microsoft Windows 2012R2 x64, Windows Server 2016 x64.</p>
<p>Wyposażenie dodatkowe</p>	<p>Dołączone dwie sztuki kabli SFP+ to SFP+ 10GbE do łączenia bezpośredniego o długości min. 3m.</p>
<p>Warunki</p>	<p>Trzy lata gwarancji realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii poprzez ogólnopolską</p>

gwarancji	linię telefoniczną producenta. W przypadku awarii dyski twarde pozostają własnością Zamawiającego. Możliwość rozszerzenia gwarancji przez producenta do siedmiu lat.
Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim lub angielskim. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.

Serwerowy System Operacyjny (SSO) – opis równoważności:

Wymagane minimalne parametry techniczne	
Licencja ma mieć charakter wieczysty i nie narażać Zamawiającego na dodatkowe koszty w przyszłym użytkowaniu. Zamawiający wymaga licencji grupowej (jeden klucz na wszystkie produkty). Zamawiający wymaga, aby wszystkie elementy systemu oraz jego licencja pochodziły od tego samego producenta. Licencja ma umożliwiać downgrade do poprzednich wersji systemu operacyjnego oraz 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.	
1	Posiada możliwość wykorzystania 320 logicznych procesorów oraz 4 TB pamięci RAM w środowisku fizycznym
2	Posiada możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności 64TB przez każdy wirtualny serwerowy system operacyjny.
3	Posiada możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania do 7000 maszyn wirtualnych.
4	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.
5	Posiada wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.
6	Posiada wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.
7	Posiada automatyczną weryfikację cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
8	Posiada możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy.
9	Wbudowane wsparcie instalacji i pracy na wolumenach, które: <ul style="list-style-type: none"> • 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).
10	Posiada wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
11	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.
12	Posiada możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET
13	Posiada możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
14	Posiada wbudowaną zaporę internetową (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.

15	Graficzny interfejs użytkownika.
16	Zlokalizowane w języku polskim, następujące elementy: <ul style="list-style-type: none"> • menu, • przeglądarka internetowa, • pomoc, • komunikaty systemowe.
17	Posiada wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
18	Posiada możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
19	Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
20	Pochodzący od producenta systemu serwis zarządzania polityką konsumpcji informacji w dokumentach (Digital Rights Management).
21	Posiada możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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, • Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza. • Zdalna dystrybucja oprogramowania na stacje robocze. • Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej • Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego umożliwiające: <ul style="list-style-type: none"> • 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. Wirtualne 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: <ul style="list-style-type: none"> • 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.
22	Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath).
23	Posiada możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
24	Posiada mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
25	Posiada możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.

5.1.2. Oprogramowanie dostępne użytkownika do środowiska CAL – 150 sztuk

LICENCJA SSO - CAL	
Nazwa komponentu	Wymagane minimalne parametry techniczne
Oprogramowanie	MS Windows 2016 Device CAL lub równoważne
Inne	Wykonawca zapewni dostęp do spersonalizowanej strony producenta produktów pozwalającej upoważnionym osobom ze strony Zamawiającego na: <ul style="list-style-type: none"> - Pobieranie zakupionego oprogramowania, - Pobieranie kluczy aktywacyjnych do zakupionego oprogramowania, - Sprawdzanie liczby zakupionych licencji w wykazie zakupionych produktów.
Sposób licencjonowania	Zamawiający nie dopuszcza licencji OEM Licencja ma mieć charakter wieczysty i nie narażać Zamawiającego na dodatkowe koszty w przyszłym użytkowaniu. Zamawiający wymaga typu licencji MOLP (Microsoft Open License Program) w licencjonowaniu dla jednostek rządowych. Licencja ma umożliwiać downgrade do wcześniejszej wersji licencji (2012, 2008) oraz uprawniać do dostępu do zasobów serwera dla określonej liczby urządzeń.
Kompatybilność	Zamawiający wymaga, aby licencja była kompatybilna z Serwerowym Systemem Operacyjnym SSO opisanym powyżej

Licencje dostępne dla SSO – opis równoważności:

Komponent	Minimalne wymagania
Sposób licencjonowania	Zamawiający nie dopuszcza licencji OEM Licencja ma mieć charakter wieczysty i nie narażać Zamawiającego na dodatkowe koszty w przyszłym użytkowaniu. Zamawiający wymaga licencji grupowej (jeden klucz na wszystkie produkty). Zamawiający wymaga, aby wszystkie elementy systemu oraz jego licencja pochodziły od tego samego producenta. Licencja ma umożliwiać downgrade do poprzednich wersji licencji oraz uprawniać do dostępu do zasobów serwera dla określonej liczby urządzeń.
Cechy	Licencja powinna zapewnić (w zgodzie z wymaganiami licencyjnymi producenta) możliwość równoległego zarządzania wybranymi usługami przez administratorów serwera, a także dostęp do zasobów serwera dla określonej liczby urządzeń.
Kompatybilność	Zamawiający wymaga, aby licencja była kompatybilna z systemem operacyjnym opisanym powyżej

5.1.3. Oprogramowanie do wirtualizacji dla serwerów wirtualizacji - Licencja na min 3 hosty po min 2 CPU

Oprogramowanie do wirtualizacji	
Nazwa komponentu	Wymagane minimalne parametry techniczne
Oprogramowanie do wirtualizacji	Licencje muszą umożliwiać uruchamianie wirtualizacji na serwerach fizycznych o łącznej liczbie 6 procesorów fizycznych oraz jednej konsoli do zarządzania całym środowiskiem. Wszystkie licencje powinny być dostarczone wraz z 3-letnim wsparciem, świadczonym przez producenta będącego licencjodawcą oprogramowania na pierwszym, drugim i trzecim poziomie, które powinno umożliwiać zgłaszanie problemów 5 dni w tygodniu przez 12h na dobę.
Konsolidacja	<ul style="list-style-type: none"> • Warstwa wirtualizacji musi być rozwiązaniem systemowym tzn. musi być zainstalowana bezpośrednio na sprzęcie fizycznym i nie może być częścią innego systemu operacyjnego. • Warstwa wirtualizacji nie może dla własnych celów alokować więcej niż 200MB pamięci operacyjnej RAM serwera fizycznego. • Rozwiązanie musi zapewnić możliwość obsługi wielu instancji systemów operacyjnych na jednym serwerze fizycznym. Wymagana jest możliwość przydzielenia maszynie większej ilości wirtualnej pamięci operacyjnej niż jest zainstalowana w serwerze fizycznym oraz większej ilości przestrzeni dyskowej niż jest fizycznie dostępna. • Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością dostępu do 4TB pamięci operacyjnej. • Oprogramowanie do wirtualizacji musi zapewnić możliwość przydzielenia maszynom wirtualnym do 128 procesorów wirtualnych. • Rozwiązanie musi umożliwiać łatwą i szybką rozbudowę infrastruktury o nowe usługi bez spadku wydajności i dostępności pozostałych wybranych usług. • Rozwiązanie musi w możliwie największym stopniu być niezależne od producenta platformy sprzętowej. • Rozwiązanie musi wspierać następujące systemy operacyjne: Windows XP, Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows Server 2016, SLES, RHEL, Solaris 10 x86, NetWare 6.5, Debian, CentOS, FreeBSD, Ubuntu, SCO OpenServer, SCO Unixware, Mac OS X • Rozwiązanie musi zapewniać sprzętowe wsparcie dla wirtualizacji zagnieżdżonej, w szczególności w zakresie możliwości zastosowania trybu XP mode w Windows 7 a także instalacji wszystkich funkcjonalności w tym Hyper-V pakietu Windows Server 2012/2012R2 na maszynie wirtualnej. • Rozwiązanie musi posiadać centralną konsolę graficzną do zarządzania środowiskiem serwerów wirtualnych. Konsola graficzna musi być dostępna poprzez dedykowanego klienta lub za pomocą przeglądark, minimum IE i Firefox. • Dostęp przez przeglądarkę do konsoli graficznej musi być skalowalny tj. powinien umożliwiać rozdzielenie komponentów na wiele instancji w przypadku zapotrzebowania na dużą liczbę jednoczesnych dostępów administracyjnych do środowiska. • Rozwiązanie musi zapewniać zdalny i lokalny dostęp administracyjny do wszystkich serwerów fizycznych poprzez protokół SSH, z możliwością nadawania uprawnień do takiego dostępu nazwanym użytkownikom bez konieczności wykorzystania konta root. • Rozwiązanie musi umożliwiać składowanie logów ze wszystkich serwerów fizycznych i konsoli zarządzającej na serwerze Syslog. Serwer Syslog w dowolnej implementacji musi stanowić integralną część rozwiązania.

- Rozwiązanie musi zapewnić możliwość monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej i zdefiniowania alertów informujących o przekroczeniu wartości progowych.
- Rozwiązanie musi umożliwiać integrację z rozwiązaniami antywirusowymi firm trzecich w zakresie skanowania maszyn wirtualnych z poziomu warstwy wirtualizacji.
- Rozwiązanie musi zapewniać możliwość konfigurowania polityk separacji sieci w warstwie trzeciej, tak aby zapewnić oddzielne grupy wzajemnej komunikacji pomiędzy maszynami wirtualnymi.
- Oprogramowanie do wirtualizacji musi zapewnić możliwość wykonywania kopii zapasowych instancji systemów operacyjnych oraz ich odtworzenia w możliwie najkrótszym czasie.
- Kopie zapasowe muszą być składowane z wykorzystaniem technik deduplikacji danych.
- Musi istnieć możliwość odtworzenia pojedynczych plików z kopii zapasowej maszyny wirtualnej przez osoby do tego upoważnione bez konieczności nadawania takim osobom bezpośredniego dostępu do głównej konsoli zarządzającej całym środowiskiem.
- Mechanizm zapewniający kopie zapasowe musi być wyposażony w system cyklicznej kontroli integralności danych. Ponadto musi istnieć możliwość przywrócenia stanu repozytorium kopii zapasowych do punktu w czasie, kiedy wszystkie dane były integralne w przypadku jego awarii.
- Oprogramowanie do wirtualizacji musi zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy z możliwością wskazania konieczności zachowania stanu pamięci pracującej maszyny wirtualnej.
- Oprogramowanie do wirtualizacji musi zapewnić możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi.
- Oprogramowanie zarządzające musi posiadać możliwość przydzielania i konfiguracji uprawnień z możliwością integracji z usługami katalogowymi, w szczególności: Microsoft Active Directory, Open LDAP.
- Platforma wirtualizacyjna musi umożliwiać zastosowanie w serwerach fizycznych procesorów o dowolnej ilości rdzeni.
- Rozwiązanie musi umożliwiać tworzenie jednorodnych wolumenów logicznych o wielkości do 62TB.
- Rozwiązanie musi zapewniać możliwość dodawania zasobów w czasie pracy maszyny wirtualnej, w szczególności w zakresie przestrzeni dyskowej.
- Rozwiązanie musi posiadać wbudowany interfejs programistyczny (API) zapewniający pełną integrację zewnętrznych rozwiązań wykonywania kopii zapasowych z istniejącymi mechanizmami warstwy wirtualizacyjnej.
- Rozwiązanie musi umożliwiać wykorzystanie technologii 10GbE w tym agregację połączeń fizycznych do minimalizacji czasu przenoszenia maszyny wirtualnej pomiędzy serwerami fizycznymi.
- Rozwiązanie musi zapewniać możliwość replikacji maszyn wirtualnych z dowolnej pamięci masowej w tym z dysków wewnętrznych serwerów fizycznych na dowolną pamięć masową w tym samym lub oddalonym ośrodku przetwarzania.
- Rozwiązanie musi gwarantować współczynnik RPO na poziomie minimum 5 minut
- Czas planowanego przestoju usług związany z koniecznością prac serwisowych (np. rekonfiguracja serwerów, macierzy, switchy) musi być ograniczony do minimum.

	<ul style="list-style-type: none"> Oprogramowanie do wirtualizacji musi obsługiwać przełączenie ścieżek SAN (bez utraty komunikacji) w przypadku awarii jednej ze ścieżek. Oprogramowanie do wirtualizacji musi obsługiwać przełączenie ścieżek LAN (bez utraty komunikacji) w przypadku awarii jednej ze ścieżek. System musi umożliwiać udostępnianie pojedynczego urządzenia fizycznego (PCIe) jako logicznie separowane wirtualne urządzenia dedykowane dla poszczególnych maszyn wirtualnych.
Wysoka dostępność	<ul style="list-style-type: none"> Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy serwerami fizycznymi, niezależnie od dostępności współdzielonej przestrzeni dyskowej, różnymi rodzajami wirtualnych przełączników sieciowych. Musi zostać zapewniona odpowiednia redundancja i nadmiarowość zasobów tak by w przypadku awarii np. serwera fizycznego usługi na nim świadczone zostały automatycznie przełączone na inne serwery infrastruktury. Rozwiązanie musi umożliwiać łatwe i szybkie ponowne uruchomienie systemów/usług w przypadku awarii poszczególnych elementów infrastruktury. Rozwiązanie musi zapewnić bezpieczeństwo danych mimo poważnego uszkodzenia lub utraty sprzętu lub oprogramowania. Rozwiązanie musi zapewniać mechanizm bezpiecznego, bezprzerwowego i automatycznego uaktualniania warstwy wirtualizacyjnej wliczając w to zarówno poprawki bezpieczeństwa jak i zmianę jej wersji. Rozwiązanie musi posiadać co najmniej 2 niezależne mechanizmy wzajemnej komunikacji między serwerami oraz z serwerem zarządzającym, gwarantujące właściwe działanie mechanizmów wysokiej dostępności na wypadek izolacji sieciowej serwerów fizycznych lub partycjonowania sieci. Decyzja o próbie przywrócenia funkcjonalności maszyny wirtualnej w przypadku awarii lub niedostępności serwera fizycznego powinna być podejmowana automatycznie, jednak musi istnieć możliwość określenia przez administratora czasu po jakim taka decyzja jest wykonywana.
Równoważenie obciążenia i przestoje serwisowe	<ul style="list-style-type: none"> Czas planowanego przestoju usług związany z koniecznością prac serwisowych (np. rekonfiguracja serwerów, macierzy, switchy) musi być ograniczony do minimum. Konieczna jest możliwość przenoszenia usług pomiędzy serwerami fizycznymi, bez przerywania pracy usług. System musi mieć wbudowany mechanizm kontrolowania i monitorowania ruchu do pamięci masowych oraz ustalania priorytetów dostępu do nich na poziomie konkretnych wirtualnych maszyn.

5.1.4. Macierz – 1 sztuka

Macierz	
Nazwa komponentu	Wymagane minimalne parametry techniczne
Obudowa	Do instalacji w standardowej szafie RACK 19". Wysokość maksymalnie 2U wraz z kompletem szyn do montażu w szafie Rack z możliwością instalacji minimum 24 dysków 2.5" Hot Plug.
Kontrolery	Dwa kontrolery posiadające łącznie minimum cztery porty FC minimum 16 Gb/s wraz z wkładkami SFP do podłączenia serwerów, pracujące w trybie active-active. Wymagane poziomy zabezpieczenia RAID: 0,1,5,6,10. Minimum 4GB na kontroler, pamięć cache zapisu mirrorowana między kontrolerami, z opcją zapisu na dysk lub inną pamięć nieulotną lub podtrzymywana bateryjnie przez min. 72h w

	razie awarii
Dyski twarde	<p>Zainstalowane dyski :</p> <p>24 dyski o pojemności minimum 1.2TB SAS 10k RPM Hot-Plug 2.5" każdy.</p> <p>Możliwość rozbudowy przez dokładanie kolejnych dysków/półek dyskowych, możliwość obsługi łącznie minimum 190 dysków, wydajnych dysków SAS,SSD, ekonomicznych dysków typu SATA (lub NearLine SAS), samoszyfrujących dysków SED dostępnych w ofercie producenta macierzy, możliwość mieszania typów dysków w obrębie macierzy oraz półki.</p>
Oprogramowanie	<p>Zarządzające macierzą w tym powiadamianie mailem o awarii, umożliwiające maskowanie i mapowanie dysków.</p> <p>Dostarczyć licencję umożliwiającą utworzenie minimum 512 LUN'ów oraz 32 kopii migawkowych na LUN.</p> <p>Licencja zaoferowanej macierzy powinna umożliwiać podłączanie minimum 32 hostów bez konieczności zakupu dodatkowych licencji.</p> <p>Zarządzanie macierzą poprzez minimum oprogramowanie zarządzające lub przeglądarkę internetową.</p> <p>Dodatkowe oprogramowanie umożliwiające wspólne zarządzanie oferowanymi serwerami oraz oferowaną macierzą poprzez sieć spełniające minimalne wymagania:</p> <ul style="list-style-type: none"> - Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych - Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta - Wsparcie dla protokołów– WMI, SNMP, IPMI, WSMAN, Linux SSH - Możliwość oskryptowywania procesu wykrywania urządzeń - Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram - Szczegółowy opis wykrytych systemów oraz ich komponentów - Możliwość eksportu raportu do CSV, HTML, XLS - Grupowanie urządzeń w oparciu o kryteria użytkownika - Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach - Automatyczne skrypty CLI umożliwiające dodawanie i edycję grup urządzeń - Szybki podgląd stanu środowiska - Podsumowanie stanu dla każdego urządzenia - Szczegółowy status urządzenia/elementu/komponentu - Generowanie alertów przy zmianie stanu urządzenia - Filtry raportów umożliwiające podgląd najważniejszych zdarzeń - Integracja z service desk producenta dostarczonej platformy sprzętowej - Możliwość przejścia zdalnego pulpitu - Możliwość podmontowania wirtualnego napędu - Automatyczne zaplanowanie akcji dla poszczególnych alertów w tym automatyczne tworzenie zgłoszeń serwisowych w oparciu o standardy przyjęte przez producentów oferowanego w tym postępowaniu sprzętu - Kreator umożliwiający dostosowanie akcji dla wybranych alertów - Możliwość importu plików MIB - Przesyłanie alertów „as-is” do innych konsol konsol firm trzecich - Możliwość definiowania ról administratorów - Możliwość zdalnej aktualizacji sterowników i oprogramowania wewnętrznego serwerów - Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania) - Możliwość instalacji sterowników i oprogramowania wewnętrznego bez potrzeby instalacji agenta - Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów - Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne

	sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie gwarancji, adresy IP kart sieciowych
Bezpieczeństwo	<p>Ciągła praca obu kontrolerów nawet w przypadku zaniku jednej z faz zasilania. Zasilacze, wentylatory, kontrolery RAID redundantne.</p> <p>Możliwość przydzielenia większej przestrzeni dyskowej dla serwerów niż fizycznie dostępna (Thin Provisioning)</p> <p>Fizyczne zabezpieczenie dedykowane przez producenta serwera uniemożliwiające wyjęcie dysków twardych umieszczonych na froncie obudowy przez nieuprawnionych użytkowników.</p>
Dokumentacja	Zamawiający wymaga dokumentacji w języku polskim lub angielskim
Certyfikaty	<p>Macierz wyprodukowana zgodnie z normą ISO 9001 oraz 14001</p> <p>Zgodność z systemami operacyjnymi: Microsoft® Windows®, VMware®, Microsoft Hyper-V®, Citrix® XenServer®, Red Hat® oraz SUSE</p>
Gwarancja	<p>Trzy lata gwarancji realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 24x7x365 poprzez ogólnopolską linię telefoniczną producenta. Możliwość rozszerzenia gwarancji przez producenta do 7 lat.</p> <p>W przypadku awarii dyski twarde pozostają własnością Zamawiającego.</p> <p>Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia, oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji macierzy.</p>

5.1.5. Serwer na potrzebę systemu ochrony danych (backupu) – 1 sztuka

Serwer	
Nazwa komponentu	Wymagane minimalne parametry techniczne
Obudowa	Obudowa Rack o wysokości max 2U z możliwością instalacji do min. 12 dysków 3,5" oraz min. 4 dysków 2,5". Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych. Obudowa wyposażona w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej (Android/ Apple iOS) przy użyciu jednego z protokołów NFC/ BLE/ WIFI.
Płyta główna	Płyta główna z możliwością zainstalowania minimum dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.
Chipset	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych
Procesor	Zainstalowane dwa procesory dziesięciordzeniowe klasy x86 dedykowane do pracy z zaferowanym serwerem umożliwiający osiągnięcie wyniku min. 99 punktów w teście SPECrate2017_int_peak dostępnym na stronie www.spec.org dla dwóch procesorów.
RAM	64GB DDR4 RDIMM 2666MT/s, na płycie głównej powinno znajdować się minimum 24 slotów przeznaczonych do instalacji pamięci. Płyta główna powinna obsługiwać do 3TB pamięci RAM.
Zabezpieczenia pamięci RAM	Memory Rank Sparing, Memory Mirror, SDDC.
Gniazda PCI	Min. 3 sloty x8 generacji 3 oraz 1 slot x16 generacji 3.
Interfejsy sieciowe/FC/SAS	Wbudowane cztery interfejsy sieciowe 1Gb Ethernet w standardzie BaseT. Możliwość instalacji wymiennie modułów udostępniających: - dwa interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz dwa interfejsy sieciowe 10Gb Ethernet ze złączami w standardzie SFP+. - cztery interfejsy sieciowe 10Gb Ethernet w standardzie SFP+. - cztery interfejsy sieciowe 1Gb Ethernet w standardzie BaseT - dwa interfejsy sieciowe 25Gb Ethernet ze złączami SFP28. Dodatkowo zainstalowana jedna karta dwuportowa 10Gb Ethernet w standardzie SFP+ oraz jedna karta dwuportowa FC 8Gb.
Napęd optyczny	Brak
Dyski twarde	Zainstalowane dyski: 6x4TB NearLine SAS interfejsem SAS 12Gb/s 4x600GB SAS 10k z interfejsem SAS 12Gb/s. 2x300GB SAS 15k z interfejsem SAS 12Gb/s. Możliwość instalacji modułu dedykowanego dla hypervisora wirtualizacyjnego, możliwość instalacji 2 jednakowych nośników typu flash o pojemności min. 64GB z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnek na dyski twarde. Możliwość zainstalowania dwóch dysków M.2 o pojemności min. 240, możliwość

	konfiguracji RAID1.
Kontroler RAID	Sprzętowy kontroler dyskowy, posiadający min. 2GB nieulotnej pamięci cache, możliwe konfiguracje poziomów RAID: 0, 1, 5, 6, 10, 50, 60.
Karty GPU	Nie wymagane.
Serwerowy System Operacyjny	Zainstalowany Windows Server 2016 Std z pełną licencją na oferowany serwer.
Wbudowane porty	min. 1 porty USB 2.0, 2 porty USB 3.0 oraz 1 port Micro-usb, 4 porty RJ45, 1 port VGA min. 1 port RS232.
Video	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200.
Wentylatory	Redundantne
Zasilacze	Redundantne, Hot-Plug minimalnie 750W każdy.
Bezpieczeństwo	TPM 2.0.
Karta Zarządzania	<p>Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet umożliwiające:</p> <ul style="list-style-type: none"> • zdalny dostęp do graficznego interfejsu Web karty zarządzającej • zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera) • szyfrowane połączenie (SSLv3) oraz autentykację i autoryzację użytkownika • możliwość podmontowania zdalnych wirtualnych napędów • wirtualną konsolę z dostępem do myszy, klawiatury • wsparcie dla IPv6 • wsparcie dla SNMP; IPMI2.0, VLAN tagging, Telnet, SSH • możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer • możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer • integracja z Active Directory • możliwość obsługi przez dwóch administratorów jednocześnie • wsparcie dla dynamic DNS • wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej • możliwość podłączenia lokalnego poprzez złącze RS-232. • Producent systemu musi posiadać dedykowane rozwiązanie które będzie przeciwdziałało automatycznym skryptom konfiguracyjnym działającym w sieci. Jest niedopuszczalne aby konsole zarządzające serwerów miały identyczne dane dostępowe. • możliwość zarządzania bezpośredniego poprzez złącze USB umieszczone na froncie obudowy. • możliwość konfiguracji przepływu powietrza na każdym slotcie PCIe, jak również musi posiadać możliwość konfiguracji wyłączenia lub włączania poszczególnych wentylatorów. • możliwość zablokowania konfiguracji oraz odnowienia oprogramowania karty zarządzającej poprzez jednego z administratorów. Podczas trwania blokady musi być ona wyświetlana dla wszystkich administratorów którzy obecnie korzystają z karty. <p>Dodatkowe oprogramowanie umożliwiające zarządzanie poprzez sieć, spełniające minimalne wymagania:</p> <ul style="list-style-type: none"> • Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych • Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta

	<ul style="list-style-type: none"> • Wsparcie dla protokołów– WMI, SNMP, IPMI, , Linux SSH • Możliwość oskryptowywania procesu wykrywania urządzeń • Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram • Szczegółowy opis wykrytych systemów oraz ich komponentów • Możliwość eksportu raportu do CSV, HTML, XLS • Grupowanie urządzeń w oparciu o kryteria użytkownika • Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach • Automatyczne skrypty CLI umożliwiające dodawanie i edycję grup urządzeń • Szybki podgląd stanu środowiska • Podsumowanie stanu dla każdego urządzenia • Szczegółowy status urządzenia/elementu/komponentu • Generowanie alertów przy zmianie stanu urządzenia • Filtry raportów umożliwiające podgląd najważniejszych zdarzeń • Integracja z service desk producenta dostarczonej platformy sprzętowej • Możliwość przejęcia zdalnego pulpitu • Możliwość podmontowania wirtualnego napędu • Automatyczne zaplanowanie akcji dla poszczególnych alertów w tym automatyczne tworzenie zgłoszeń serwisowych w oparciu o standardy przyjęte przez producentów oferowanego w tym postępowaniu sprzętu • Kreator umożliwiający dostosowanie akcji dla wybranych alertów • Możliwość importu plików MIB • Przesyłanie alertów „as-is” do innych konsol firm trzecich • Możliwość definiowania ról administratorów • Możliwość zdalnej aktualizacji sterowników i oprogramowania wewnętrznego serwerów • Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania) • Możliwość instalacji sterowników i oprogramowania wewnętrznego bez potrzeby instalacji agenta • Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów <ul style="list-style-type: none"> ▪ Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie gwarancji, adresy IP kart sieciowych ▪ Możliwość automatycznego przywracania ustawień serwera ,kart sieciowych, BIOS, wersji firmware w przypadku awarii i wymiany któregoś z komponentów (w tym kontrolera RAID, kart sieciowych, płyty głównej)
<p>Certyfikaty</p>	<p>Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2008 oraz ISO-14001. Serwer musi posiadać deklaracja CE. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów, Microsoft Windows 2012 x64, Microsoft Windows 2012R2 x64, Windows Server 2016 x64.</p>
<p>Wyposażenie dodatkowe</p>	<p>Dołączone dwie sztuki kabli SFP+ to SFP+ 10GbE do łączenia bezpośredniego o długości min. 3m.</p>
<p>Warunki gwarancji</p>	<p>Trzy lata gwarancji realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii poprzez ogólnopolską linię telefoniczną producenta. W przypadku awarii dyski twarde pozostają własnością</p>

	Zamawiającego. Możliwość rozszerzenia gwarancji przez producenta do siedmiu lat.
Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim lub angielskim. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.

5.1.6. Biblioteka taśmowa – 1 sztuka

Biblioteka taśmowa	
Nazwa komponentu	Wymagane minimalne parametry techniczne
Obudowa	Do zamontowania w szafie rack, maksymalnie 2U
Napęd	LTO-6 FC – 1 szt.
Liczba slotów	24 w tym minimum jeden slot we/wy, jeżeli licencjonowana jest liczba slotów - wymagane aktywowanie wszystkich slotów
Dodatkowe	interfejs do zarządzania poprzez przeglądarkę WWW oraz możliwość zarządzania bezpośrednio z użyciem wbudowanych klawiszy i wyświetlacza LCD wyjmowane magazynki kieszeni na taśmy w celu łatwego zarządzania większą ilością taśm wsparcie dla nośników LTO WORM (Write Once, Read Many), umożliwiającym spełnienie norm prawnych dotyczących odpowiednio długiego przechowywania nienaruszonych danych (archiwizacja) Obsługa SNMP Wsparcie dla technologii szyfrowania backupowanych danych Wymagane dostarczenie 21 taśm w tym minimum: 20 taśm LTO-6 Media, 1 taśma czyszcząca. Wymagane dostarczenie 60 etykiet na taśmy.
Warunki gwarancji	Trzy lata gwarancji producenta realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia. Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta serwera – dokumenty potwierdzające załączyć do oferty.

5.1.7. Przełącznik rdzeniowy – 1 sztuka

Przełącznik rdzeniowy	
Nazwa komponentu	Wymagane minimalne parametry techniczne
Obudowa	Umożliwiająca montaż w szafie rack 19"
Liczba gniazd	wbudowane 24x 10G BASE-T oraz 24x1000/10GBASE-X SFP+ port

Rodzaj urządzenia	przełącznik warstwy L3
Przepustowość przełączania	Min. 950 Gbit/s
Przepustowość	Min. 702 Mpps
Pamięć flash	Min. 256 MB
MAC addresses	128 000
Zasilacz	Wewnętrzny redundantny
Inne	obsługa ssl/ssh; pełny duplex, protokół drzewa rozpinającego, klient DHCP, obsługa sieci VLAN, lista kontroli dostępu (ACL).
Stos	Minimalna ilość przełączników w stosie: 8 Możliwość łączenia w stos przełączników z dominującymi portami 10Gb/s oraz 1Gb/s Możliwość łączenia w stos za pomocą interfejsów 10Gb/s Możliwość łączenia przełączników w stos w konfiguracji: pierścień, podwójny pierścień, mesh
Akcesoria	Zamawiający wymaga dostarczenia wraz z przełącznikiem: 8 x Transceiver 10GBASE-SR 8 x kabel LC-LC min. 5 metrów

5.1.8. Przełącznik dostępowy 48 portowy PoE – 4 sztuki

Przełącznik dostępowy 48 portowy PoE	
Nazwa komponentu	Wymagane minimalne parametry techniczne
Obudowa	Umożliwiająca montaż w szafie rack 19"
Liczba gniazd	48 portów 1GBaseT PoE+, 2 x SFP+ oraz 2 x 10GBaseT niezależne
Rodzaj urządzenia	przełącznik warstwy L3
Budżet PoE	480W
Zasilacz	Możliwość instalacji drugiego wewnętrznego zasilacza
Przepustowość przełączania	Min. 175 Gbit/s
Przepustowość	Min. 130 Mpps
Pamięć RAM	Min. 1 GB
Pamięć flash	Min. 256 MB
Bufor	16 Mb
MAC addresses	16 000

Inne	obsługa ssl/ssh; pełny duplex, protokół drzewa rozpinającego, klient DHCP, obsługa sieci VLAN, lista kontroli dostępu (ACL).
Stos	Minimalna ilość przełączników w stosie: 8 Możliwość łączenia w stos przełączników z dominującymi portami 10Gb/s oraz 1Gb/s Możliwość łączenia w stos za pomocą interfejsów 10Gb/s Możliwość łączenia przełączników w stos w konfiguracji: pierścień, podwójny pierścień, mesh
Akcesoria	Zamawiający wymaga dostarczenia wraz z przełącznikiem: 2 x Transceiver 10GBASE-SR 2 x kabel LC-LC min. 5 metrów

5.1.9. Przełącznik dostępowy 24 portowy – 4 sztuki

Przełącznik dostępowy 24 portowy	
Nazwa komponentu	Wymagane minimalne parametry techniczne
Obudowa	Umożliwiająca montaż w szafie rack 19"
Liczba gniazd	24 porty 1GBaseT, 2 x SFP+ oraz 2 x 10GBaseT niezależne
Rodzaj urządzenia	przełącznik warstwy L3
Przepustowość przełączania	Min. 128 Gbit/s
Przepustowość	Min. 95 Mpps
Pamięć RAM	Min. 1 GB
Pamięć flash	Min. 256 MB
Bufor	16 Mb
MAC addresses	16 000
Inne	obsługa ssl/ssh; pełny duplex, protokół drzewa rozpinającego, klient DHCP, obsługa sieci VLAN, lista kontroli dostępu (ACL).
Stos	Minimalna ilość przełączników w stosie: 8 Możliwość łączenia w stos przełączników z dominującymi portami 10Gb/s oraz 1Gb/s Możliwość łączenia w stos za pomocą interfejsów 10Gb/s Możliwość łączenia przełączników w stos w konfiguracji: pierścień, podwójny pierścień, mesh
Akcesoria	Zamawiający wymaga dostarczenia wraz z przełącznikiem: 1 x Transceiver 10GBASE-SR 1 x kabel LC-LC min. 5 metrów

5.1.10. Urządzenia UPS dla przełączników dostępowych – 3 sztuki

Zasilacz UPS dla przełączników dostępowych	
Nazwa komponentu	Wymagane minimalne parametry techniczne
Moc pozorna	1000VA
Moc czynna	900W
Napięcie wejściowe	230V
Zakres napięcia wejściowego	160/140/120/110V – 300V dla obciążenia 100-80%/80-70%/70-60%/60-0%
Częstotliwość wejściowa	45-55Hz lub 56-65Hz
Wejściowy współczynnik mocy	0,99 (nominalne napięcie, pełne obciążenie)
Napięcie wyjściowe	208V, 220V, 230V, 240V
Tolerancja napięcia wyjściowego	±1%
Częstotliwość wyjściowa	50/60Hz ±0,1%
Czas przełączania	0 ms
Tryb pracy	true on-line
Kształt napięcia wyjściowego	Czysta sinusoida
Zniekształcenia napięcia wyjściowego	≤2% THD przy liniowym obciążeniu ≤4% THD przy nieliniowym obciążeniu
Współczynnik szczytu	3:1
Gniazda wyjściowe	8 x IEC 320 (10A)
Komunikacja	port RS 232, USB, karta sieciowa SNMP
Zdalne wyłączenie	złącze EPO (ppoz.)
Poziom hałasu	< 50dB(A) / 1m
Baterie	Szczelne, bezobsługowe, ołowiono-kwasowe
Czas ładowania do 90%	4 godziny
Prąd ładowania	1,5A (max.)
Wykonanie	Wersja RACK
Czas podtrzymania	3 minut dla 100% obciążenia/6 minut dla 50% obciążenia
Wymiary (szer x gł x wys)	UPS - 438 x 410 x 88 [2U] mm
Sprawność	91% - tryb AC-AC 90% - tryb baterii 97% - tryb ECO
Dodatkowe cechy zasilacza	- wyświetlacz LCD - sterowanie mikroprocesorowe

	<ul style="list-style-type: none"> - funkcja Cold Start – załączanie obciążonego urządzenia bez napięcia w sieci - system automatycznego ładowania baterii - podział gniazd wyjściowych na zarządzalne grupy - ochrona przepięciowa linii tel/fax/modem - możliwość pracy jako konwerter częstotliwości z 50Hz na 60Hz lub z 60Hz na 50Hz - współpraca z agregatami prądotwórczymi - opcjonalna możliwość zdalnego włączania i wyłączenia zasilacza UPS bez użycia dodatkowego oprogramowania, karty sieciowej SNMP oraz karty styków bezpotencjałowych - opcjonalna możliwość monitorowania w trybie on-line pracy każdego akumulatora z osobną, pomiar napięcia na każdym z akumulatorów oraz skuteczne ostrzeżenie o wykrytych problemach w badanych akumulatorach - zwiększone bezpieczeństwo podczas transportu (użycie złącza ANNEN) - opcjonalna możliwość podłączenia czujnika zasilania - opcjonalna możliwość zdalnego nadzoru przez autoryzowany serwis UPS - zabezpieczenie przed głębokim rozładowaniem baterii akumulatorów
Wskaźniki ostrzeżenia na wyświetlaczu LCD	<ul style="list-style-type: none"> - niski poziom baterii - przeciążenie - akumulator nie jest podłączony - przeładowanie baterii - błędne podłączenie kabli zasilających - aktywacja EPO - przegrzanie - awaria ładowarki - awaria baterii - wyjście poza zakres napięcia linii bypassu - niestabilna częstotliwość linii bypassu - błąd EEPROM - awaria wentylatora - wymiana baterii
Tryby pracy	<ul style="list-style-type: none"> - online - ECO - AECO (zaawansowany tryb ECO) - konwertera częstotliwości - baterii - obejścia serwisowego - czuwania
Certyfikat	CE
Gwarancja	36 miesięcy UPS i 24 miesiące akumulatory

5.1.11. Szafa teletechniczna wraz z wyposażeniem – 1 sztuka

Szafa teletechniczna wraz z wyposażeniem	
Nazwa komponentu	Wymagane minimalne parametry techniczne
Wysokość wewnętrzna	42 U
Wysokość	Min. 2000 mm
Szerokość	800 mm
Głębokość	1000 mm
Maksymalna nośność	800 kg
Dodatkowe informacje	<ul style="list-style-type: none"> • Drzwi przednie stalowe perforowane z zamkiem • Drzwi boczne demontowane na zatrzaskach z możliwością montażu zamka • Wyposażenie: 4 wentylatory, 3 półki, listwa zasilająca, 40 koszyków ze śrubami • Zgodne z standardami ANSI / EIA RS-310-D, DIN 41491 • Zgodność z normami PART1, IEC297-2, DIN41494 • Zgodność z normami PART7, GB/T3047.2-92 • Kompatybilne ze standardami: metrycznym, ETSI oraz międzynarodowym 19" • Szkielet o nośności do 800kg • Stalowa blacha zimnowalcowana • Wykończenie pow.: odtłuszczenie, wytrawianie, fosfatowanie, malowanie proszkowe • Zabezpieczona przed rdzą, utlenianiem, porysowaniem, korozją • Dwa przepusty kablowe - szczotkowy w suficie , kablowy w podłodze • Grubość ramy: 1.5 mm • Grubość szyn montażowych: 2.0 mm • Grubość paneli bocznych: 1.2 mm • Grubość przednich drzwi: 1.2 mm • Regulowane nóżki i kółka o dużej wytrzymałości • Dobry poziom wentylacji i rozpraszania ciepła • Kolor - RAL9004 • Stopień ochrony: IP20 • Kompatybilność ze sprzętem różnych producentów
Dodatkowe wyposażenie	<ul style="list-style-type: none"> • Dwa pionowe organizery kabli do szafy 42U • Przełącznik KVM (1U) rack 19" • Listwa zarządzalna 19" 1U 8xIEC320 C13, wtyk zasilający IEC320 C20 16A/250V (wbudowany) – <ul style="list-style-type: none"> ○ Monitorowanie <ul style="list-style-type: none"> ▪ Całkowitego obciążenia prądowego

	<ul style="list-style-type: none"> ▪ Napięcia zasilania listwy ▪ Stanu gniazda włączone/wyłączone ▪ Stanu czujnika temperatury i wilgotności ○ Załączenie/wyłączenie – gniazda oraz grupy gniazd ○ Kontrola – Wizualna załączenia/wyłączenia gniazda ○ Komunikacja <ul style="list-style-type: none"> ▪ Interfejs web – dostęp za pomocą przeglądarek ▪ Ethernet TCP/IP ▪ SNMP, Telnet
Gwarancja	36 miesięcy

5.1.12. Urządzenie UPS do serwerowni – 1 sztuka

Urządzenie UPS do serwerowni	
Nazwa komponentu	Wymagane minimalne parametry techniczne
Technologia	VFI (true on-line, podwójne przetwarzanie energii)
Moc znamionowa	6 kVA / 6 kW
Wyjściowy współczynnik mocy (PF)	1.0
Napięcie wejściowe	230 Vac
Tolerancja napięcia wejściowego przy obciążeniu 70-100%; bez przechodzenia na baterie	138– 299 Vac
Tolerancja napięcia wejściowego przy obciążeniu mniejszym od 70%; bez przechodzenia na baterie	110 – 299 Vac
Częstotliwość wejściowa	Wymagana 40-70 Hz
Sprawność AC-AC w trybie pracy on-line z obciążeniem 100%	nie mniejsza niż 95%
Sprawność AC-AC w trybie pracy Oszczędzania energii Eco Mode	nie mniejsza niż 99%
Tryb pracy z konwersją częstotliwości	Wymagana praca ze stałą częstotliwością wyjściową 50Hz, przy zasilaniu 60Hz lub odwrotnie.
Napięcie wyjściowe	230 Vac
Częstotliwość wyjściowa	50/60Hz (programowalna)
Automatyczny układ doładowywania baterii i ciągłego sprawdzania stanu naładowania oraz zabezpieczenie chroniące baterie przed głębokim rozładowaniem	Wymagane
Czas podtrzymania	25 minut dla obciążenia 2,5kW
Baterie	Szczelne, bezobsługowe, w technologii AGM, o projektowanej żywotności min. 10-12 lat i pojemności minimalnej 2160 V*Ah.

Szafa baterii	Zamknięta szafa bateryjna
Stabilizacja napięcia wyjściowego w stanie ustalonym	$\pm 1\%$
Stabilizacja napięcia wyjściowego w stanie niestabilnym	$\pm 3\%$
Współczynnik szczytu	3:1
Panel sterujący z wyświetlaczem ciekłokrystalicznym LCD w języku polskim oraz sygnalizacją akustyczną	Wymagane
Złącze interfejsów	RS232, USB, REPO
Karta sieciowa SNMP	Wymagana
Interfejs EPO (do wyłącznika ppoż.)	Wymagane
Diagnostyka parametrów urządzenia UPS i baterii	Automatyczna diagnostyka parametrów urządzenia UPS i baterii na panelu UPS-a i z wykorzystaniem oprogramowania do zarządzania i monitorowania UPS
Oprogramowanie zapewniające pełny monitoring, zarządzanie i automatyczny shut-down systemu operacyjnego	Wymagane
Poziom hałasu w odległości 1m,	< 50 dBA Wentylatory o regulowanej prędkości obrotowej w zależności od obciążenia i temperatury
Możliwość regulacji z panelu sterującego tolerancji napięcia wejściowego i częstotliwości wejściowej w linii bypassu	Wymagane
Bypass zewnętrzny serwisowy	Wymagane
Spełnienie wszystkich obowiązujących norm w zakresie bezpieczeństwa, kompatybilności elektromagnetycznej potwierdzone deklaracją zgodności CE	Wymagane
Producent zasilacza UPS z siedzibą w Polsce, posiadający biuro dystrybucji i serwisu na terenie kraju.	Wymagane
Certyfikat ISO 9001 oraz 14001 producenta zasilacza UPS	Wymagane
Wymiary zasilacza UPS w szafie rack 19"	Maks 5 U
Szyny do montażu w szafie rack	Wymagane
Instrukcja w języku polskim	Wymagane
Gwarancja	36 miesięcy

5.1.13. Oprogramowanie systemu ochrony danych (backupu) – 1 komplet

Szafa teletechniczna wraz z wyposażeniem	
Nazwa komponentu	Wymagane minimalne parametry techniczne
<p>Licencje muszą umożliwiać backup maszyn wirtualnych na serwerach fizycznych o łącznej liczbie min. 6 procesorów fizycznych. Licencja przeznaczona dla wykorzystywanego przez Wykonawcę środowiska wirtualizacji (3 serwery fizyczne opisane powyżej).</p> <p>Wszystkie licencje powinny być dostarczone wraz z 3-letnim wsparciem, świadczonym przez producenta oprogramowania, które powinno umożliwiać zgłaszanie problemów 5 dni w tygodniu przez 8h na dobę.</p>	
<ul style="list-style-type: none"> Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 4.1, 5.0, 5.1, 5.5, 6.0 oraz Microsoft Hyper-V 2012, 2012 R2 i 2016. 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 Manager, klastrami hostów oraz pojedynczymi hostami. Oprogramowanie musi zapewniać tworzenie kopii zapasowych wszystkich systemów operacyjnych maszyn wirtualnych wspieranych przez vSphere i Hyper-V 	
<ul style="list-style-type: none"> Oprogramowanie musi być licencjonowane w modelu "per-CPU". Wszystkie funkcjonalności zawarte w tym dokumencie powinny być zapewnione w tej licencji. Jakikolwiek dodatkowe licencjonowanie (per zabezpieczony TB, dodatkowo płatna deduplikacja) nie jest dozwolone 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 mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania Oprogramowanie musi zapewniać backup jednoprzebiegowy - nawet w przypadku wymagania granularnego odtworzenia Oprogramowanie musi zapewniać mechanizmy informowania o wykonaniu/błędzie zadania poprzez email lub SNMP. Oprogramowanie musi mieć możliwość uruchamiania dowolnych skryptów przed i po zadaniu backupowym lub przed i po wykonaniu zadania snapshota w środowisku VMware. 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. Oprogramowanie musi oferować zarządzanie kluczami w przypadku utraty podstawowego klucza Oprogramowanie musi wspierać backup maszyn wirtualnych używających współdzielonych dysków VHDX na Hyper-V (shared VHDX) 	
<ul style="list-style-type: none"> Oprogramowanie musi automatycznie wykrywać i usuwać snapshoty-sieroty (orphaned snapshots), które mogą zakłócić poprawne wykonanie backupu. Oprogramowanie musi wspierać kopiowanie backupów na taśmy wraz z pełnym śledzeniem wirtualnych maszyn Oprogramowanie musi mieć możliwość wydzielenia osobnej roli typu tape server Oprogramowanie musi mieć możliwość kopiowania backupów do lokalizacji zdalnej Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son) 	

- 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)
- Oprogramowanie musi umożliwić uruchomienie wielu maszyn wirtualnych bezpośrednio ze zduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana niezależnie od rodzaju storage'u użytego do przechowywania kopii zapasowych. Dla środowiska vSphere powinien być wykorzystany wbudowany w oprogramowanie serwer NFS. Dla Hyper-V powinna być zapewniona taka sama funkcjonalność realizowana wewnętrznymi mechanizmami oprogramowania
- Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków
- Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure.
- 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:
 - **Linux**
 - ext, ext2, ext3, ext4, ReiserFS (Reiser3), JFS, XFS, Btrfs
 - **BSD**
 - UFS, UFS2
 - **Solaris**
 - ZFS, UFS
 - **Mac**
 - HFS, HFS+
 - **Windows**
 - NTFS, FAT, FAT32, ReFS
 - **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.

- 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. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Windows oraz Linux.
 - Funkcjonalność ta nie może wymagać pełnego odtworzenia wirtualnej maszyny ani jej uruchomienia.
 - Oprogramowanie musi indeksować pliki Windows i Linux w celu szybkiego wyszukiwania plików w plikach backupowych.
 - Oprogramowanie musi używać mechanizmów VSS wbudowanych w system operacyjny Microsoft Windows
 - Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN
- 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.
 - Oprogramowanie musi mieć podobne mechanizmy dla replik w środowisku vSphere

Dla potrzeb serwera backupowego (1 licencja na 3 lata) oprogramowanie spełniające poniższe wymagania:

- Rozwiązanie musi wykonywać kopię zapasową systemu Windows wykorzystując agenta znajdującego się wewnątrz systemu operacyjnego
- Rozwiązanie musi być licencjonowane subskrypcyjnie, per agent, per rok – **Wykonawca zapewni licencję na 3 lata**
- Rozwiązanie musi wspierać Windows 7 SP1, lub nowsze oraz Windows Server 2008 R2 SP1 lub nowsze
- Rozwiązanie musi wspierać wykonywanie kopii zapasowych następujących systemów plików:
 - NTFS
 - ReFS
 - FAT32
- Rozwiązanie musi wspierać zabezpieczanie do oraz odzyskiwanie z urządzeń blokowych pozwalając na odzysk całej maszyny (tzw. bare metal recovery) wybranych wolumenów, oraz wybranych plików i folderów
- Kopia zapasowa całej maszyny oraz pojedynczych wolumenów musi być wykonywana na poziomie blokowym
- Rozwiązanie musi pozwalać na przechowywanie kopii zapasowych na:
 - Lokalnych (wewnętrznych) dyskach zabezpieczonej maszyny
 - Direct Attached Storage (DAS), takich jak zewnętrzne dyski USB, eSATA lub Firewire
 - Network Attached Storage (NAS) pozwalającym na wystawienie swoich zasobów poprzez SMB (CIFS) lub NFS.
 - Zcentralizowanym repozytorium danych
- Rozwiązanie musi wspierać deduplikację oraz kompresję na źródle. Dane wysyłane na repozytorium muszą być już odpowiednio przetworzone
- Rozwiązanie musi wspierać śledzenie zmienionych bloków podczas wykonywania blokowych kopii zapasowych
- Rozwiązanie musi wspierać technologię BitLocker
- Rozwiązanie musi wspierać uruchamianie z nośnika odtwarzania. Nośnik odtwarzania musi być automatycznie tworzony przez Rozwiązanie
- Rozwiązanie musi wspierać wgrywanie dodatkowych sterowników podczas odtwarzania z wykorzystaniem nośnika odtwarzania
- Rozwiązanie musi wspierać odzysk pojedynczych elementów aplikacji z jednoprzebiegowej kopii zapasowej

dla:

- Microsoft Exchange 2010 i nowszych
- Microsoft Active Directory 2003 i nowszych
- Microsoft Sharepoint 2010 i nowszych
- Microsoft SQL 2005 i nowszych
- Oracle for Windows 11g i nowszych
- Rozwiązanie musi wspierać odzysk do konkretnego punktu w czasie (point-in-time) dla wspieranych systemów bazodanowych
- Rozwiązanie musi wspierać odzysk obrazów kopii zapasowych bezpośrednio do Microsoft Azure
- Rozwiązanie musi wspierać szyfrowanie kopii zapasowych na źródle
- Rozwiązanie musi wspierać możliwość wykonywania kopii zapasowych lokalnie do repozytorium tymczasowego (cache) gdy połączenie sieciowe do głównego repozytorium kopii zapasowych jest niedostępne
- Rozwiązanie musi posiadać funkcjonalność indeksowania oraz przeszukiwania plików
- Rozwiązanie musi posiadać funkcjonalność automatycznego zmniejszenia szybkości przetwarzania danych, aby nie dopuścić do obniżenia wydajności systemu zabezpieczonego
- Rozwiązanie musi posiadać funkcjonalność ochrony przed ransomware dla nośników wymiennych wykorzystywanych, jako repozytorium kopii zapasowych
- Rozwiązanie musi wspierać tworzenie kopii zapasowych wykorzystując konsolę tekstową lub CLI na maszynie zabezpieczonej

5.1.14. Kontroler WiFi – 1 sztuka

Kontroler WiFi	
Nazwa komponentu	Wymagane minimalne parametry techniczne
Kontroler sieci bezprzewodowej obsługujący do 50 Punktów Dostępnych dostarczony z nieograniczoną żywotnością licencją do obsługi do 50 punktów dostępowych.	
Wymagania:	<ul style="list-style-type: none"> · Kontroler musi być zintegrowany z przełącznikiem zarządzanym Gigabit Ethernet z zasilaniem PoE · Musi posiadać minimum 8 portów 10/100/1000 Gigabit Ethernet PoE 802.3at/af o łącznym budżecie mocy min. 130W · Musi posiadać min. 2 złącza światłowodowe multimodowe zapewniającymi maksymalną odległość transmisji do 0,5km · Musi pozwalać na zasilanie innych urządzeń PoE niż Access Pointy bez użycia dodatkowego osprzętu (kontrolera, zasilacza itp.) np. kamery IP · Musi mieć możliwość podłączenia i zasilania minimum 7 punktów dostępowych PoE 802.3af bez dodatkowego źródła zasilania · Posiadać wbudowaną pamięć SDRAM minimum 256MB oraz FlashMemory minimum 32MB · Wbudowane narzędzia do zarządzania siecią · Pełna obsługa Warstwy 2 (Layer-2) · Kontroler Oprogramowanie do zarządzania punktami dostępowymi (bez ograniczeń czasowych i licencyjnych)

	<ul style="list-style-type: none"> · zarządzanie urządzeniem poprzez interfejs www (HTTP) · możliwość bezpłatnej aktualizacji oprogramowania urządzenia (np. poprzez pobranie ze strony producenta) · posiadać funkcjonalność umożliwiającą szybkie zapisanie/odtworzenie konfiguracji systemu · wydajność przełączania min. 20GB · Tablica MAC adresów – 8K · Funkcje VLAN: Voice VLAN, Max. 4094 grup statycznych · Kontroler zintegrowany z przełącznikiem musi umożliwiać montaż na ścianie zostać dostarczony z uchwytem montażowym oraz zestawem śrub do montażu. Musi być też dostarczony z zasilaczem oraz przewodem zasilającym. · Automatyczne wykrywanie i udostępnianie punktów dostępu · Automatyczne przypisanie adresu IP punktu dostępu · Zarządzanie klastrem dostępu · Musi umożliwiać umieszczenia na mapie geograficznej lokalizacji AP z dokładnością do budynku · Musi mieć możliwość wgrywania i umieszczenia na planie budynku rozmieszczenia AP na poszczególnych piętrach · Pokazywać graficznie na planie czy punkty dostępowe są online czy offline, MAC adres AP oraz nadaną nazwę AP. · Zapewniać wsparcie dla WEP, WPA / WPA2 Enterprise, WPA / WPA2 PSK · Port Mirroring; Port Trunking · 802.3ad Link Aggregation · 802.1D Spanning Tree (STP) · 802.1w Rapid Spanning Tree (RSTP) · 802.1s Multiple Spanning Tree (MSTP) · VLAN Tag / VLAN Pass-through · wpierać konfigurację poprzez www (http) · obsługa protokołu SNMP v1/ v2c/v3, MIB I/II · posiadać graficzny interfejs użytkownika (GUI) oraz CLI (Telnet) · Port Mirroring - One-to-One - Many-to-One · Monitorowanie stanu punktu dostępowego · Bezprzewodowa statystyka ruchu i użytkowania · Monitorowanie przepustowości w czasie rzeczywistym · Ponowne uruchamianie punktu dostępu zdalnego · Edytowanie nazw urządzeń Access Point · Posiadać zabezpieczenia przed atakami typu DoS · Powinien posiadać sygnalizacyjne diody LED: zasilania, błędu, PoE, trybu LAN, trybu PoE; · Kontroler musi być zintegrowany z przełącznikiem.
<p>oprogramowanie do zarządzania i kontroli wszystkich kontrolerów oraz AP</p>	
	<ul style="list-style-type: none"> · Musi zapewniać zdalną obsługę do min. 100 punktów dostępowych w różnych lokalizacjach do których jest dostęp przez sieć.

	<p>Oprogramowanie musi być dostarczone z nieograniczoną dożywotnią licencją do obsługi do min. 100 punktów dostępowych.</p> <ul style="list-style-type: none"> · Oprogramowanie musi mieć możliwość instalacji na MS Windows 7 lub nowszym na wirtualnej maszynie VirtualBox® 4.3.30 (lub nowszej) lub VMware® Player 7 (lub innej maszynie wirtualnej VMware®) · Oprogramowanie powinno posiadać wsparcie dla przeglądarek Internet Explorer 10 lub nowszej; Firefox 34.0 lub nowszej; Chrome 31.0 lub nowszej; · Oprogramowanie musi zarządzać centralnie wszystkimi access-pointami · Oprogramowanie do zarządzania kontrolerami i punktami dostępowymi musi mieć możliwość przejęcia głównych funkcjonalności kontrolera co umożliwia na pracę bez kontrolera. · Musi umożliwiać umieszczenia na mapie geograficznej lokalizacji AP z dokładnością do budynku · Musi mieć możliwość wgrywania i umieszczenia na planie budynku rozmieszczenia AP na poszczególnych piętrach · Pokazywać graficznie na planie czy punkty dostępowe są online czy offline, MAC adres AP oraz nadaną nazwę AP. · Automatyczne wykrywanie i udostępnianie punktów dostępu · Automatyczne przypisanie adresu IP punktu dostępu · Zarządzanie klastrem dostępu · Sprzęt do instalacji oprogramowania do zarządzania siecią bezprzewodową dostarcza zamawiający zgodnie z wytycznymi producenta · możliwość bezpłatnej aktualizacji oprogramowania urządzenia (np. poprzez pobranie ze strony producenta)
Gwarancja	36 miesięcy

5.1.15. Punkty dostępowe sieci WiFi – 30 sztuk

Punkty dostępowe sieci WiFi	
Nazwa komponentu	Wymagane minimalne parametry techniczne
<p>Urządzenie typu access-point przeznaczone do montażu wewnątrz budynku musi być zgodny ze standardami IEEE 802.11b, IEEE 802.11g oraz IEEE 802.11n w paśmie 2.4GHz oraz IEEE 802.11ac Wave2 w paśmie 5 GHz. Zarządzanie access-pointem musi odbywać się za pomocą dedykowanego kontrolera sprzętowego dostarczonego przed producenta access-pointa lub wirtualnego(zewnętrzne oprogramowanie tego samego producenta co punkt dostępowy.).Wyposażony w co najmniej wewnątrz dookólne anteny 2x2: 2 802.11ac/a/b/g/n/ac wave2</p>	

Wymagania:

- Obsługa multi-user Multiple Input Multiple Output
- Posiadać jedno gigabitowe złącza RJ45 służące do zasilania oraz transmisji łącza - 10/100/1000 BASE-T,
- Posiadać reset pozwalający przywrócić ustawienia fabryczne oraz wejście DC typu Jack.
- Musi być dostarczony z Adapterem dedykowanym do zasilania punktu dostępowego z wtykiem typu Jack 12V/1A
- Musi być dostarczony z uchwytyami montażowymi również z uchwytyami montażowymi na szyny typu T-Rail
- Zgodne ze standardem 802.3af,
- Obsługa min. 867 Mbps dla 5GHz 802.11ac oraz min. 400 Mbps dla 2.4GHz 802.11ac/a/b/g/n/,
- Obsługa 802.11ac w wersji Wave 2.0
- Moc wyjściowa anten dookólnych dwuradiowych nie mniejsza jak: 5dBi dla 2.4GHz, 5dBi dla 5GHz
- Moc transmisji dla 2.4Ghz oraz 5GHz nie mniejsza jak 26dBm
- Wsparcie dla minimum 8 niezależnych SSID
- Praca w zakresie temperatur 0°C do 40°C
- Praca w trybie meshowym,
- Punkty dostępowe muszą zapewnić ciągłość pracy tj. dostępu do sieci w przypadku uszkodzenia kontrolera lub zerwania z nimi połączenia.
- Musi wspierać Tx Beamforming (TxBF) - Zwiększenie niezawodności sygnału i odległości nadawania.
- Obsługa usługi do zarządzania:
 - captive portal,
 - sieć dla gości,
 - tagowany VLAN,
 - przypisanie VLAN do SSID,
 - zarządzanie VLAN (SSH, telnet, snmp),
 - filtrowanie adresów MAC,
 - lista klientów podłączonych do sieci bezprzewodowej,
 - obsługa RADIUS,
- Możliwość uruchomienia tunelu SSH,
- Musi mieć możliwość zarządzania przez dedykowane rozwiązanie producenta,
- Aktualizowanie konfiguracji z poziomu kontrolera poprzez jedno kliknięcie wszystkich punktów,
- Maksymalny pobór energii nie większy niż 11W
- Obsługiwać modulację typu
 - 802.11b: BPSK, QPSK, CCK
 - 802.11a/g/n: BPSK, QPSK, 16-QAM, 64-QAM
 - 802.11ac: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM
- Musi wspierać:
 - 802.11b: Direct-sequence spread-spectrum (DSSS)
 - 802.11ac/a/g/n: Orthogonal frequency-division multiplexing (OFDM)
 - 802.11n/ac: min. 2x2 MIMO

	<ul style="list-style-type: none"> ○ 802.11ac very high throughput (VHT) —VHT 20/40/80 MHz ○ 802.11n (HT) —HT 20/40 MHz ○ 802.11n very high throughput under the 2.4GHz radio – VHT40 ○ MHz (256-QAM) ○ 802.11n/ac packet aggregation: AMPDU, ASPDU <ul style="list-style-type: none"> • Posiadać certyfikaty • CE • EN 300 328 • EN 301 893 • EN 50385 • EN 60601-1-1 • EN 60601-1-2 • EN 55032 • EN 55024 • RED 2014/53/EU <p>Low Voltage Directive 2014/30/EU</p>
Gwarancja	36 miesięcy

5.1.16. Stacje robocze wraz z oprogramowaniem systemowym – 125 sztuk

Stacje robocze wraz z oprogramowaniem systemowym	
Nazwa komponentu	Wymagane minimalne parametry techniczne
Typ	Komputer stacjonarny.
Zastosowanie	Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna
Wydajność obliczeniowa	Procesor wielordzeniowy osiągający w teście Passmark CPU Mark wynik min. 7900 punktów według wyników ze strony http://www.cpubenchmark.net na dzień nie wcześniejszy niż 26/06/2018
Pamięć operacyjna RAM	8GB DDR4 2666MHz możliwość rozbudowy do min 32GB, min. 1 slot wolny
Parametry pamięci masowej	Min. 500 GB SATA 7200 obr./min
Wydajność grafiki	Grafika zintegrowana z procesorem powinna umożliwiać pracę dwumonitorową ze wsparciem DirectX 12, OpenGL 4.0, pamięć współdzielona z pamięcią RAM, dynamicznie przydzielana
Wyposażenie	Min 24-bitowa Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition,

multimedialne	wewnętrzny głośnik 2W w obudowie komputera.
Obudowa	<p>Typu Mini Tower z obsługą kart PCI Express tylko o pełnym profilu, możliwość instalacji minimum dwóch dysków 2,5" lub 3,5"</p> <p>Obudowa fabrycznie przystosowana do pracy w orientacji pionowej.</p> <p>Suma wymiarów obudowy nie może przekraczać 80cm, w tym głębokość max 30cm</p> <p>Zasilacz o mocy max. 260W 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%,</p> <p>Moduł konstrukcji obudowy w jednostce centralnej komputera powinien pozwalać na demontaż kart rozszerzeń, napędu optycznego bez konieczności użycia narzędzi (wyklucza się użycia wkrętów, śrub motylkowych).</p> <p>Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej (złącze blokady Kensingtona) oraz kłódki (oczeko w obudowie do założenia kłódki).</p> <p>Obudowa musi posiadać wbudowany wizualny system diagnostyczny, służący do sygnalizowania i diagnozowania problemów z komputerem i jego komponentami, sygnalizacja oparta na zmianie statusów diody LED przycisku POWER (tzn. barw i miganie)</p> <p>W szczególności musi sygnalizować: uszkodzenie lub brak pamięci RAM, uszkodzenie płyty głównej, uszkodzenie kontrolera video, awarię CMOS baterii, awarię BIOS'u, awarię procesora.</p> <p>Oferowany system diagnostyczny nie może wykorzystywać minimalnej ilości wolnych slotów wymaganych w specyfikacji,</p> <p>Każdy komputer powinien być oznaczony niepowtarzalnym numerem seryjnym umieszczonym na obudowie, oraz wpisanym na stałe w BIOS.</p>
Zgodność systemami operacyjnymi standardami	<p>z i</p> <p>Oferowane modele komputerów muszą posiadać certyfikat producenta oferowanego systemu operacyjnego, potwierdzający poprawną współpracę oferowanych modeli komputerów z oferowanym systemem operacyjnym (załączyć wydruk ze strony producenta oprogramowania)</p>
Bezpieczeństwo	<p>Zintegrowany z płytą główną dedykowany 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</p> <p>Zaimplementowany w BIOS system diagnostyczny z graficznym interfejsem użytkownika dostępny z poziomu szybkiego menu boot'owania, umożliwiający jednocześnie przetestowanie w celu wykrycia usterki zainstalowanych komponentów w oferowanym komputerze bez konieczności uruchamiania systemu operacyjnego.</p>
Wirtualizacja	Sprzętowe wsparcie technologii wirtualizacji realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu.
BIOS	<p>BIOS zgodny ze specyfikacją UEFI, wyprodukowany przez producenta komputera, zawierający logo lub nazwę producenta komputera lub nazwę modelu oferowanego komputera,</p> <p>Pełna obsługa BIOS za pomocą klawiatury i myszy.</p> <p>Funkcja blokowania wejścia do BIOS oraz blokowania startu systemu operacyjnego, (gwarantujący utrzymanie zapisanego hasła nawet w przypadku odłączenia wszystkich źródeł zasilania i podtrzymania BIOS)</p> <p>Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z zewnętrznymi</p>

		<p>urządzeń.</p> <p>Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych, ustawienia hasła na poziomie systemu, administratora oraz dysku twardego,</p> <p>Możliwość wyłączenia/włączenia karty sieciowej, z funkcją PXE,</p> <p>Możliwość włączenia/wyłączenia kontrolera SATA</p> <p>Możliwość włączenia/wyłączenia kontrolera audio,</p> <p>Możliwość włączenia/wyłączenia układu TPM.</p>
Certyfikaty standardy	i	<p>Certyfikat ISO9001: 2005 dla producenta sprzętu (załączyć dokument potwierdzający spełnianie wymogu)</p> <p>Deklaracja zgodności CE (załączyć do oferty)</p> <p>Certyfikat TCO dla oferowanego modelu – załączyć wydruk ze strony http://tcodevelopment.com/</p>
Warunki gwarancji		<p>Trzy lata gwarancja producenta świadczona na miejscu u klienta</p> <p>Czas reakcji serwisu - do końca następnego dnia roboczego</p> <p>Firma serwisująca musi posiadać ISO 9001: 2000 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta komputera – dokumenty potwierdzające załączyć do oferty.</p> <p>Długość gwarancji musi wynikać bezpośrednio z numeru seryjnego komputera i być weryfikowalna na stronie internetowej producenta sprzętu</p> <p>W przypadku awarii, dyski twarde zostają u Zamawiającego – do oferty należy załączyć oświadczenie podmiotu realizującego serwis lub producenta o spełnieniu tego warunku</p>
Wsparcie techniczne producenta		<p>Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej komputera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.</p> <p>Dostęp do najnowszych sterowników i uaktualnień na stronie producenta zestawu realizowany poprzez podanie na dedykowanej stronie internetowej producenta numeru seryjnego lub modelu komputera – do oferty należy dołączyć link strony.</p>
System operacyjny		<p>Zainstalowany system operacyjny Windows 10 Professional, klucz licencyjny Windows 10 Professional musi być zapisany trwale w BIOS.</p> <p><i>Opis równoważności</i></p> <p>Zainstalowany system operacyjny spełniający poniższe wymagania:</p> <ul style="list-style-type: none"> • Możliwość dokonywania aktualizacji i poprawek systemu przez Internet z możliwością wyboru instalowanych poprawek. • Możliwość dokonywania uaktualnień sterowników urządzeń przez Internet. • Darmowe aktualizacje w ramach wersji systemu operacyjnego przez Internet (niezbędne aktualizacje, poprawki, biuletyny bezpieczeństwa muszą być dostarczane bez dodatkowych opłat) – wymagane podanie nazwy strony serwera WWW. • Internetowa aktualizacja zapewniona w języku polskim. • Wbudowana zaporę internetową (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6. • Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimedialny, pomoc, komunikaty systemowe. • Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug & Play, Wi-Fi). • Funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do

której podłączony jest komputer.

- Interfejs użytkownika działający w trybie graficznym z elementami 3D, zintegrowana z interfejsem użytkownika interaktywna część pulpitu służąca do uruchamiania aplikacji, które użytkownik może dowolnie wymieniać i pobrać ze strony producenta.
- Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu.
- Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników.
- Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych.
- Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi.
- Wbudowany system pomocy w języku polskim.
- Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących).
- Możliwość zarządzania stacją roboczą poprzez polityki – przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji.
- Wdrażanie IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny.
- Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.
- Rozbudowane polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji.
- System posiada narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk.
- Wsparcie dla Sun Java i .NET Framework 1.1 i 2.0 i 3.0 lub programów równoważnych, tj. – umożliwiających uruchomienie aplikacji działających we wskazanych środowiskach.
- Wsparcie dla JScript i VBScript lub równoważnych – możliwość uruchamiania interpretera poleceń.
- Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem.
- Rozwiązanie służące do automatycznego zbudowania obrazu systemu wraz z aplikacjami. Obraz systemu służyć ma do automatycznego upowszechnienia systemu operacyjnego inicjowanego i wykonywanego w całości poprzez sieć komputerową.
- Rozwiązanie umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację.
- Graficzne środowisko instalacji i konfiguracji.
- Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe.
- Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe.
- Udostępnianie modemu.
- Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej.
- Możliwość przywracania plików systemowych.
- System operacyjny musi posiadać funkcjonalność pozwalającą na identyfikację sieci komputerowych, do których jest podłączony, zapamiętywanie ustawień i przypisywanie

	<p>do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.).</p> <ul style="list-style-type: none"> Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu). Zamawiający wymaga dostarczenia systemu operacyjnego w wersji 64-bit. Licencja i oprogramowanie musi być nowe, nieużywane.
Wymagania dodatkowe	<p>Wbudowane porty i złącza: VGA, HDMI, Display Port, min. 4 porty USB na przednim panelu obudowy (w tym min. 2 porty USB 3.0) i min. 4 porty USB na tylnym panelu obudowy (w tym min. 2 porty USB 3.0) wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp.; port słuchawkowo-mikrofonowy oraz czytnik kart na przednim panelu, port Line-out na tylnym panelu</p> <p>Karta sieciowa 10/100/1000 Ethernet RJ 45, zintegrowana z płytą główną, wspierająca obsługę WoL</p> <p>Karta sieci bezprzewodowej 802.11ac 2x2</p> <p>Płyta główna zaprojektowana i wyprodukowana na zlecenie producenta komputera, dedykowana dla danego urządzenia; wyposażona w min 1 złącze PCI Express x16 Gen.3, min. 3 wolne złącza PCI Express x 1, min. 2 złącza DIMM z obsługą do 32GB DDR4 pamięci RAM, min. 3 złącza SATA w tym 2 szt SATA 3.0; min. 1 złącze M.2 dla dysku SSD</p> <p>Klawiatura USB w układzie polski programisty</p> <p>Mysz USB</p> <p>Nagrywarka DVD +/-RW o prędkości min. 8x</p>

5.1.17. Monitory stacji roboczych – 125 sztuk

Monitory stacji roboczych	
Nazwa komponentu	Wymagane minimalne parametry techniczne
Typ ekranu	Ekran ciekłokrystaliczny z aktywną matrycą min. 23" (16:9)
Rozmiar plamki	0,265 mm
Jasność	250 cd/m ²
Kontrast	1000:1
Kąty widzenia (pion/poziom)	178/178 stopni
Czas reakcji matrycy	max 5ms gray to gray
Zużycie energii	Normalne działanie do 22W (typowe), do 25W (maksymalne), tryb wyłączenia aktywności mniej niż 0,5W
Powłoka powierzchni ekranu	Antyodblaskowa utwardzona
Podświetlenie	System podświetlenia LED
Bezpieczeństwo	Monitor musi być wyposażony w tzw. Kensington Slot - gniazdo zabezpieczenia przed kradzieżą.
Zakres regulacji Tilt	26 stopni

Obudowa	Kolor czarny
Złącze	Zgodne z oferowanym w komputerze stacjonarnym i umożliwiające prawidłową pracę monitora w max. rozdzielczości: 1x 15-stykowe złącze D-Sub - z dołączonym kablem 1xHDMI – z dołączonym kablem
Gwarancja	Trzy lata na miejscu u klienta Czas reakcji serwisu - do końca następnego dnia roboczego
Certyfikaty	<ul style="list-style-type: none"> • TCO , EPEAT Gold, Energy Star 5.2 lub nowszy. Do oferty należy dołączyć wydruk potwierdzający spełnienie tych wymogów. • Deklaracja zgodności oferowanego monitora z wymaganiami zasadniczymi (Deklaracja CE);
Inne	Zdejmowana podstawa oraz otwory montażowe w obudowie VESA 100mm

5.1.18. Instalacja, konfiguracja i uruchomienie infrastruktury sprzętowej oraz oprogramowania systemowego, wirtualizacyjnego i narzędziowego

W celu przygotowania infrastruktury serwerowej dla potrzeb systemów Elektronicznej Dokumentacji Medycznej oraz ePortalu należy wykonać następujące prace przygotowawcze:

1. Przedstawienie koncepcji połączeń oraz adresacji urządzeń serwerowo-sieciowych oraz uzgodnienie z Informatykami Zamawiającego akceptacji poniższych prac.
2. Montaż sprzętu serwerowego w szafie serwerowej.
3. Montaż pozostałego sprzętu typu: zasilacze awaryjne, przełączniki rdzeniowe, przełączniki SAN, KVM, biblioteka taśmowa, kontroler WiFi, punkty dostępne WiFi.
4. Podłączenie zasilania w sposób redundantny
5. Podłączenia logiczne urządzeń do przełączników rdzeniowych
6. Montaż przełączników sieciowych w Punktach dystrybucyjnych oraz montaż zasilaczy awaryjnych i podłączenia logiczne oraz elektryczne.
7. Podniesienie firmware na wszystkich urządzeniach serwerowo-sieciowych.
8. Nadanie adresacji dla przełączników sieciowych w Serwerowni oraz w pozostałych punktach dystrybucyjnych.
9. Nadanie adresacji dla pozostałych urządzeń tj. dla kart SNMP, zarządzania, sieci WiFi.
10. Konfiguracja VLAN-ów
11. Konfiguracja sieci Storage Area Network - SAN
12. Instalacja oprogramowania wirtualizacyjnego na serwerach, stworzenie klastra serwerów, instalacja oprogramowania do zarządzania maszynami wirtualnymi
13. Instalacja maszyn wirtualnych zgodnie z wytycznymi oprogramowania medycznego EDM oraz dla potrzeb ePortal
14. Instalacja i konfiguracja serwera backupu oraz oprogramowania do wykonywania kopii bezpieczeństwa

15. Instalacja patchów, update na serwerach fizycznych oraz na maszynach wirtualnych
16. Instalacja i konfiguracja oprogramowania do zarządzania i monitorowania sprzętu serwerowego oraz monitorowania określonych usług.
17. Instalacja i konfiguracja sieci Wi-Fi dla potrzeb tabletów medycznych
18. Wykonanie testów redundancji połączeń sieciowych i SAN-owych, zaniku napięcia, awarii serwera wirtualizacyjnego itp.

5.1.19. Modernizacja sieci teleinformatycznej (szkielet światłowod)

Wykonanie niezbędnych prac instalacyjnych polegających na ułożeniu kabla światłowodowego pomiędzy szafą główną serwerowni oraz szafami dystrybucyjnymi (3 szt.) i montażu i konfiguracji zakupionych urządzeń teleinformatycznych (przełączniki dostępowe, kontrolery Wi-Fi itp.).

5.1.20. Modernizacja serwerowni

Niezbędne prace instalacyjne wykonać zgodnie z kosztorysem na wykonanie modernizacji serwerowni.

Montaż podłogi teletechnicznej podniesionej

Montaż drzwi antywłamaniowych, przeciwpożarowych wraz z systemem kontroli dostępu

Montaż dwóch klimatyzatorów pracujących naprzemiennie.

Poniżej przedstawiono parametry techniczne urządzeń.

Wymagania techniczne dla systemu podłogi teletechnicznej podniesionej:

W pomieszczeniu serwerowni zostanie zamontowana podłoga techniczna, podniesiona na wysokość 30 cm.

Podłoga powinna charakteryzować się następującymi parametrami:

- wymiary płyt - 600x600x40 mm
- wysoko sprasowana płyta wiórowa klasy E1
- pokrycie górne / aplikacja / wykładzina PCV antyelektrostatyczna
- krawędzie boczne z listwą ochronną z twardego przewodzącego PCV
- pod szafami serwerowymi stosować płyty z kratką nawiewną
- pokrycie dolne wzmocnione blachą stalową ocynkowaną
- Konstrukcja wsporcza / ruszt / wysokość 300 mm
- stopy stalowe ocynkowane z płynną regulacją wysokości
- podstawy stop mocowane do podłoża za pomocą kleju lub kołków rozporowych

Parametry techniczne podłogi:

- obciążenie powierzchniowe - 25 kN/m²
- obciążenie skupione / punktowe / - 3 kN
- klasa odporności ogniowej – REI30

Powierzchnia serwerowni przewidziana do zabudowy podłogi technicznej: 8 m².

Wymagania dla drzwi do Serwerowni:

Pomieszczenie Serwerowni powinno być zabezpieczone przed dostępem osób niepowołanych. W tym celu zamontowane zostaną drzwi wejściowe do pomieszczenia Serwerowni. Istniejące drzwi do pomieszczenia zostaną zdemontowane wraz z ościeżnicą.

Drzwi atestowane przeciwpożarowe, o wymiarach 90x200.

Dane techniczne:

- zamek główny składający się z zamka centralnego,
- zawiasy wzmocnione,
- przeciwpożarowe – odporność ogniowa EI-60,
- dymoszczelność,
- antywłamaniowe klasy RC4,
- samozamykacz.

Wykonawca musi dostarczyć i zamontować drzwi antywłamaniowe. Drzwi muszą być sterowane przy pomocy skonfigurowanego systemu SSWiN z KD.

Wymagania dla systemu SSWiN z KD:

System alarmowy oraz kontroli dostępu obejmować będzie pomieszczenie serwerowni GPD.

Zaprojektowane rozwiązanie oparte o centralę alarmową zintegrowaną z systemem kontroli dostępu.

Powyższy system zostanie wyposażony również w czujki temperatury i zalania w celu monitoringu parametrów środowiskowych.

System SSWiN wraz z KD składać się będzie z następujących podzespołów (1 zestaw):

- Centrala systemu alarmowego, do 32 wejść i wyjść
- Klawiatura obsługi systemu alarmowego LCD z czytnikiem zbliżeniowym
- Moduł rozbudowy czytników kart/pastylek centrali systemu alarmowego
- Ethernetowy moduł komunikacyjny
- Przycisk awaryjnego wyjścia, zielony, podwójny, klapka zabezpieczająca
- Zwora 270kg z przekaźnikiem wraz z elementem mocowania
- Moduł rozbudowy centrali systemu alarmowego, komunikacyjny, monitoring GPRS/SMS wraz z

Anteną

- Sygnalizator optyczno-akustyczny, wewnętrzny
- Sygnalizator optyczno-akustyczny, zewnętrzny
- Obudowa central natynkowa
- Akumulator 12V, 18Ah
- Czujka ruchu dualna PIR+MW, wewnętrzna -2 sztuki
- Czujka zalania wody
- Czujka pożarowa systemu alarmowego, optyczno-temperaturowa – 2 sztuki
- Programowalna czujka temperatury
- Karta ISO UNIQUE – 10 sztuk

Wymagania minimalne dla klimatyzatorów – należy dostarczyć dwie sztuki pracujące naprzemiennie każdy o parametrach minimalnych:

1. Wydajność Chłodzenie kW 8,0, Grzanie kW 8,8
2. Pobór mocy Chłodzenie/Grzanie kW 2.33/2.41
3. Osuszanie 2,7 l/h
4. Przepływ powietrza Jedn. wew./ Jedn. zew. m³/h 1 380/3 600
5. Max długość przewodów Bez doładowania czynnika m 50 (20)
6. Max różnica poziomów 30m

7. Czynniki chłodnicze R410A
8. Inne funkcje Duży wymiennik ciepła, powiększona sprężarka DC, wysokosprawna inwerterowa płytka PCB. Tryb chłodzenia możliwy także przy niskiej temperaturze zewnętrznej i wilgotności powietrza.
9. Praca naprzemienna urządzeń, funkcja zabezpieczająca – w przypadku awarii jednego z nich drugie załączy się automatycznie. Funkcja wspierająca: oba urządzenia pracują jednocześnie, gdy w pomieszczeniu wzrasta temperatura
10. Gwarancja 3 lata – w cenie musi uwzględnić konieczne przeglądy w okresie gwarancji

5.1.21. Skaner dokumentacji medycznej - 1 sztuka

Skaner dokumentacji medycznej	
Nazwa komponentu	Wymagane minimalne parametry techniczne
Rodzaj czujnika skanowania obrazu	Kolorowe matryce CCD
Rozdzielczość optyczna	600 dpi
Wyjściowa głębi kolorów	Kolor: 24-bitowy, skala szarości: 8-bitów, monochromatyczny: 1-bit
Ultradźwiękowy czujnik	Tak
Źródło światła	Biała matryca LED
Prędkość skanowania A4	Jednostronny: 60 str./min, dwustronny: 120 obr./min
Pojemność ADF	Min. 80 arkuszy
Dzienna wydajność pracy	Min. 4.000 stron
Interfejs	Złącze USB 3.0
Podajniki	ADF, Podajnik Płaski
Funkcje procesowania obrazu / oprogramowanie	Wiele obrazów, pomijanie pustej strony, automatyczny kolor, prostowanie kadrowanie, usuwanie dziurek, kadrowanie tabulatur, oddzielanie góry i dołu, dyfuzja błędów, wahania, usuwanie efektu mory, podkreślanie obrazu, oczyszczanie kolorów, usuwanie kolorów (R, G, B, brak, biały, wskazany, nasycenie kolorów), naprawa krawędzi, redukcja pasów w pionie
Funkcje wykrywania pobrań	Ultradźwiękowy czujnik podwójnego pobrania, iSOP (Intelligent Sonic Paper Protection – inteligentna akustyczna ochrona skanowanych dokumentów), inteligentna funkcja podwójnego pobrania (pominięcie ręczne)
Inne funkcje	Obsługa skanowania wypukłych kart, skanowanie długich dokumentów, obsługa USB 3.0, automatyczne: rozpoznawanie kolorów, wykrywanie formatu papieru, korekta zakrzywień
Gwarancja	36 miesięcy

5.1.22. Przełącznik FC – 2 sztuki

Przełącznik FC	
Nazwa komponentu	Wymagane minimalne parametry techniczne
Obudowa	1U z możliwością montażu w szafie rack

<p>Funkcjonalność</p>	<ul style="list-style-type: none"> – Przełącznik FC musi być wykonany w technologii FC 16 Gb/s i posiadać możliwość pracy portów FC z prędkościami 16, 8, 4 Gb/s z funkcją autonegocjacji prędkości. – Przełącznik FC musi posiadać minimum 24 sloty na moduły FC. Wszystkie wymagane funkcje muszą być dostępne dla wszystkich portów FC przełącznika. – Przełącznik musi być dostarczony wraz z minimum 12 modułami SFP FC 16 Gb/s. – Rodzaj obsługiwanych portów: D_Port (ClearLink Diagnostic Port), E_Port, F_Port, M_Port (Mirror Port); – Przełącznik FC musi posiadać nadmiarowe wentylatory N+1. – Przełącznik FC musi być wykonany w tzw. architekturze „non-blocking” uniemożliwiającej blokowanie się ruchu wewnątrz przełącznika przy pełnej prędkości pracy wszystkich portów. – Przełącznik musi posiadać mechanizm balansowania ruchu między grupami połączeń tzw. „trunk” oraz obsługiwać grupy połączeń „trunk” o różnych długościach. – Przełącznik FC musi udostępniać usługę Name Server Zoning - tworzenia stref (zon) w oparciu bazę danych nazw serwerów. – Przełącznik FC musi posiadać możliwość wymiany i aktywacji wersji firmware’u (zarówno na wersję wyższą jak i na niższą) w czasie pracy urządzenia, bez wymogu ponownego uruchomienia urządzeń w sieci SAN. – Przełącznik FC musi posiadać wsparcie dla następujących mechanizmów zwiększających poziom bezpieczeństwa: <ul style="list-style-type: none"> • Listy Kontroli Dostępu definiujące urządzenia (przełączniki i urządzenia końcowe) uprawnione do pracy w sieci Fabric • Możliwość uwierzytelnienia (autentykacji) przełączników z listy kontroli dostępu w sieci Fabric za pomocą protokołów DH-CHAP i FCAP • Możliwość uwierzytelnienia (autentykacji) urządzeń końcowych z listy kontroli dostępu w sieci Fabric za pomocą protokołu DH-CHAP • Kontrola dostępu administracyjnego definiująca możliwość zarządzania przełącznikiem tylko z określonych urządzeń oraz portów • Szyfrowanie połączenia z konsolą administracyjną. Wsparcie dla SSHv2, • Wskazanie nadrzędnych przełączników odpowiedzialnych za bezpieczeństwo w sieci typu Fabric. • Konta użytkowników definiowane w środowisku RADIUS lub LDAP • Szyfrowanie komunikacji narzędzi administracyjnych za pomocą SSL/HTTPS • Obsługa SNMP v3 – Przełącznik FC musi posiadać możliwość konfiguracji przez komendy tekstowe w interfejsie znakowym oraz przez przeglądarkę internetową z interfejsem graficznym. – Przełącznik FC musi mieć możliwość instalacji jednomodowych SFP umożliwiających bezpośrednie połączenie (bez dodatkowych urządzeń pośredniczących) z innymi przełącznikami na odległość minimum 10km. – Przełącznik FC musi zapewnić możliwość jego zarządzania przez zintegrowany port Ethernet, RS232 oraz inband IP-over-FC – Przełącznik FC musi zapewniać wsparcie dla standardu zarządzającego SMI-S v1.1 (powinien zawierać agenta SMI-S zgodnego z wersją standardu v1.1) – Przełącznik FC musi zapewniać możliwość nadawania adresu IP dla zarządzającego portu Ethernet za pomocą protokołu DHCP – Maksymalny dopuszczalny pobór mocy przełącznika FC to 77W – Przełącznik FC musi zapewniać możliwość dynamicznego aktywowania portów za pomocą zakupionych kluczy licencyjnych. – Przełącznik FC musi zapewniać opóźnienie przy przesyłaniu ramek FC między dowolnymi
------------------------------	---

	<p>portami nie większe niż 700ns.</p> <ul style="list-style-type: none"> – Przełącznik FC musi zapewniać sprzętową obsługę zonu na podstawie portów i adresów WWN – Urządzenie musi wspierać mechanizm balansowania ruchem w połączeniach wewnątrz wielodomenowych sieci fabric w oparciu OXID. – Możliwość wymiany w trybie „na gorąco”: minimum w odniesieniu do modułów portów Fibre Channel (SFP). – Wsparcie dla N_Port ID Virtualization (NPIV). Obsługa co najmniej 255 wirtualnych urządzeń na pojedynczym porcie przełącznika.
Wyposażenie	Szyny do montażu w szafie rack.
Inne wymagania	Produkt musi być fabrycznie nowy i dostarczony przez autoryzowany kanał sprzedaży producenta na terenie kraju.
Gwarancja	Trzy lata gwarancji realizowanej w miejscu instalacji sprzętu, z czasem reakcji od przyjęcia zgłoszenia w następnym dniu roboczym, możliwość zgłaszania awarii w trybie 24x7x365 poprzez ogólnopolską linię telefoniczną producenta.

6. Wymagania dotyczące wdrożenia i przeszkolenia

6.1. Wymagania dotyczące budowy środowiska chmury obliczeniowej

W ramach realizacji przedmiotu zamówienia w obszarze budowy środowiska chmury obliczeniowej i dostawy sprzętu, Wykonawca zobowiązany będzie do realizacji poniższych zadań:

- W ramach opracowywanego Projektu wykonawczego szczegółowo opisać architekturę fizyczną wdrożenia systemu oraz jego konfigurację, zgodnie z którą przeprowadzone zostaną wdrożenia poszczególnych elementów Systemu.
- Opracowania harmonogramu dostaw i konfiguracji elementów środowiska.
- Dostawy wymaganego i opisanego powyżej sprzętu do lokalizacji głównej Zamawiającego.
- Instalacji wskazanego sprzętu w dostarczonej szafie serwerowej RACK.
- Uruchomienia i konfiguracji macierzy dyskowej na potrzeby wdrożenia wysokodostępnej wirtualizacji.
- Uruchomienia i konfiguracji dwóch serwerów fizycznych na potrzeby klastra wirtualizacji.
- Uruchomienia i konfiguracji system ochrony danych.
- Instalacji dostarczonych urządzeń sieciowych oraz konfiguracji sieci LAN.
- Wdrożenia wirtualizacji oraz konfiguracji wysokiej dostępności.
- Uruchomienia środowiska produkcyjnego i środowiska testowo-szkoleniowego Systemu. Nie jest wymagana konfiguracja środowiska testowo-szkoleniowego w trybie wysokiej dostępności.
- Opracowania dokumentacji powykonawczej.
- Przeszkolenia Administratorów z zakresu administrowania infrastrukturą i konfiguracją Systemu.

Ewentualne doposażenia elementów infrastruktury sprzętowej posiadanej przez Zamawiającego nie stanowią przedmiotu niniejszego zamówienia. A zatem jeżeli zajdzie taka potrzeba wówczas Wykonawca w Projekcie wykonawczym wskaże Zamawiającemu zakres takich wymaganych doposażeń.

6.2. Wymagania dotyczące zarządzania projektem

Dla zarządzania Projektem należy przyjąć metodykę PRINCE2 lub równoważną. Wykorzystanie stosownych wzorców zarządzania projektem oraz doświadczeń biznesowych i technicznych w zarządzaniu Projektem z wykorzystaniem metodyki PRINCE2 lub równoważnej winno zapewnić:

- dobre zaplanowanie i zarządzanie realizacją poszczególnych zadań projektu;
- właściwą diagnozę i minimalizację ryzyka projektowego,
- właściwe zarządzanie i monitorowanie procesu wytwarzania i dostarczania produktów projektu,
- dostarczenie produktów wysokiej jakości i właściwej konfiguracji spełniających wyspecyfikowane przez Zamawiającego wymagania.

Zarządzanie projektem musi zakładać ścisłą współpracę pomiędzy Wykonawcą a Zamawiającym od rozpoczęcia projektu aż do jego zakończenia.

Należy przyjąć, iż w ramach struktury organizacyjnej projektu wyodrębnione zostaną trzy poziomy zarządzania Projektem:

- Poziom 1 – Zarządzania strategiczne: obszar działania Komitetu Sterującego w Projekcie;
- Poziom 2 – Zarządzenie operacyjne: obszar działania Kierowników Projektu stron;
- Poziom 3 – Dostarczanie Produktów: obszar dziania Kierowników Zespołów i podległych im Członkom zespołów projektowych.

Należy przyjąć, iż Komitet Sterujący odpowiedzialny będzie za zatwierdzanie planów działań dotyczących projektu, monitorowanie stanu jego realizacji, podejmowanie strategicznych decyzji w projekcie oraz rozwiązywanie kwestii spornych, a w szczególności:

- sprawowanie nadzoru i kontroli nad realizacją projektu;
- podejmowanie decyzji o strategicznym znaczeniu dla realizacji projektu;
- stosownie do potrzeb, rekomendowanie i akceptacja zmiany harmonogramu realizacji i zakresu Umowy oraz ewentualne odstępstwa od innych jej postanowień;
- rozwiązywanie ewentualnych problemów powstających w wyniku realizacji Umowy.

Należy przyjąć, iż Kierownicy Projektu (przedstawiciele obu stron) odpowiedzialni będą za codzienne zarządzanie Projektem w granicach zdefiniowanych w zawartej przez strony Umowie. Obowiązkiem Kierowników Projektu w szczególności będzie:

- zapewnienie aby w ramach Projektu wytworzone i dostarczone zostały produkty zaplanowane w zamówieniu spełniające postawione przez Zamawiającego, wymagania;
- dbanie o terminowość i kompletność dostaw produktów;
- dbanie o jakość dostarczanych produktów;
- identyfikowanie i zarządzanie ryzykiem.

Członkowie zespołów Projektowych po stronie Wykonawcy odpowiedzialni będą za dostarczenie produktów projektu o odpowiedniej jakości w terminach zdefiniowanych w Harmonogramie. Członkowie zespołów projektowych po stronie Zamawiającego odpowiedzialni będą za przekazanie Wykonawcy informacji i danych niezbędnych dla dostarczenia produktów w terminie oraz wymaganych parametrach jakościowych a także wsparcie dla Członków Zespołu Projektowego po stronie Wykonawcy.

W celu właściwego zarządzania Projektem niezbędne jest zaplanowanie i opisanie:

- właściwej organizacji Projektu z uwzględnieniem uwarunkowań projektowych oraz potrzeby współdziałania stron;
- Harmonogramu Projektu;
- sposobu oraz terminów dostawy poszczególnych Produktów;

- sposobu podejścia do zarządzania i oceny jakości Produktów;
- sposobu identyfikowania, planowania i zarządzania ryzykiem;
- sposobu identyfikowania, planowania i zarządzania zmianą;
- sposobu monitorowania postępów.

Zarządzanie przebiegiem projektu winno koncentrować się na stałym delegowaniu, monitorowaniu i kontrolowaniu wszystkich aspektów Projektu oraz motywowaniu zaangażowanych osób, aby osiągnąć cele Projektu w granicach docelowych wskaźników wykonania w czasie (zgodnie z Harmonogramem Projektu), kosztów, jakości, zakresu, korzyści i ryzyka.

Wykonawca opracuje Dokument Zarządzania Projektem zawierający procedury i wytyczne dla sposobu realizacji projektu ujmujący założenia przedstawione powyżej. Dokument ten musi, zawierać następujące informacje:

- Opis celu dokumentu;
- Szczegółowy opis organizacji Projektu;
- Szczegółowy opis ról i obowiązków dla każdej ze stron Umowy;
- Plan komunikacji;
- Harmonogram Projektu;
- Wykaz produktów;
- Opis procedur stosowanych w procesie wdrażania Systemu oraz dostawy i odbioru poszczególnych typów produktów:
 - o Procedurę zmiany członków zespołów projektowych;
 - o Procedurę zgłaszania i zarządzania ryzykiem;
 - o Procedurę zgłaszania i zarządzania zagadnieniami projektowymi
 - o Procedurę zarządzania zmianą; o Procedurę dostawy i odbioru Dokumentacji
 - o Procedurę dostawy i odbioru Sprzętu; o Procedurę dostawy i odbioru Oprogramowania;
- Opis procedury zgłaszania i obsługi zgłoszeń serwisowych;

6.3. Wymagania dotyczące świadczenia serwisu gwarancyjnego dla Systemu

Wykonawca na potrzebę ewidencjonowania incydentów wymagających obsługi serwisowej oraz monitorowania obsługi zdiagnozowanych błędów i problemów w działaniu Systemu, udostępni Administratorom Systemu po stronie Zamawiającego dostęp do systemu internetowego Wykonawcy – ServiceDesk. Dzięki temu Administratorzy będą mieć możliwość bezpośredniego zdefiniowania takiego incydentu w systemie oraz bieżącego monitorowania stan jego obsługi.

Wykonawca zapewni zespół HelpDesk oraz numer telefonu i adres email do zgłaszania incydentów.

Wykonawca zapewni, że wszystkie zgłoszenia incydentu (bez względu na to, jakim kanałem zgłaszający dokona rejestracji zgłoszenia incydentu) będą rejestrowane w systemie ServiceDesk.

Wykonawca dla świadczenia usługi zapewni dedykowany zespół konsultantów.

Wykonawca przez cały okres trwania serwisu gwarancyjnego Systemu monitorował będzie zmieniające się przepisy prawa dotyczące działania wdrożonego u Zamawiającego Systemu, tak aby w terminach wymaganych prawem, wprowadzać i udostępniać Zamawiającemu niezbędne zmiany mające na celu zapewnienie Systemowi (w zakresie dostarczonych funkcjonalności) zgodność z przepisami prawa wg wymagań zdefiniowanych w Umowie i dokumentacji SIWZ.

6.4. Wymagania dotyczące przeszkolenia Administratorów i Użytkowników

Wykonawca w okresie wdrożenia oraz w okresie gwarancji przeprowadzi szkolenia dla Administratorów i Użytkowników systemu łącznie w wymiarze

- szkolenia dla administratorów Systemu – 24 godziny
- szkolenia z obsługi systemu informatycznego e-usług
-

Na etapie wdrożenia strony ustalą szczegółowy porządek i podział szkoleń z uwzględnieniem wymagań zawartych w niniejszym rozdziale które przyjęte zostaną w Planie szkoleń.

6.4.1. Szkolenia dla administratorów Systemu

W ramach realizacji zamówienia Wykonawca przeprowadzi szkolenia dla Administratorów (maksimum 2 osoby) z zakresu:

- Administrowania środowiskiem serwerowo-macierzowym:
 - o prezentacja dostarczonych produktów; o omówienie architektury wdrożonego środowiska;
 - o omówienie zasad i procedur administrowania w tym konfiguracji urządzeń i środowiska, wirtualizacji oraz monitorowania środowiska;
- Administrowania kopią bezpieczeństwa (backupu):
 - o prezentacja dostarczonego oprogramowania i dysku NAS na potrzeby backupu; o omówienie architektury wdrożonego rozwiązania backupu; o omówienie konfiguracji backup;
 - o przedstawienie zasad i procedur administrowania i monitorowania pracy podsystemu backupu;
- Administrowania sieci informatycznej:
 - o prezentacja dostarczonych urządzeń sieciowych; o zapoznanie z systemem operacyjnym urządzeń; o omówienie konfiguracji środowiska;
 - o przedstawienie zasad i procedur administrowania i monitorowania pracy środowiska sieciowego;
- Administrowania urządzeniami wielofunkcyjnymi oraz pozostałymi dostarczonymi urządzeniami:
 - o prezentacja dostarczonych urządzeń; o omówienie zasad administrowania urządzeń oraz monitorowania ich pracy.

6.4.2. Szkolenia dla Użytkowników z obsługi funkcjonalności Systemu

W ramach realizacji zamówienia Wykonawca przeprowadzi cykl szkoleń dla wyznaczonego przez Zamawiającego personelu. Wykonawca zobowiązany jest do przeprowadzenia szkolenie w formie instruktażu stanowiskowego dla personelu w podziale na role w Systemie.

Zamawiający dostarczy Wykonawcy imienny podział uczestników szkoleń na poszczególne grupy, z założeniem, iż w każdej grupie będzie maksymalnie 5 osób. Zamawiający zapewni salę szkoleniową oraz niezbędny sprzęt komputerowy z dostępem do środowiska testowo-szkoleniowego wdrażanego systemu.

6.5. Wymagania dotyczące przygotowania dokumentacji

W ramach realizacji zamówienia Wykonawca opracuje i dostarczy Zamawiającemu następującą dokumentację:

- Projekt Wykonawczy;
- Plan szkoleń i materiały szkoleniowe;
- Dokumentację Powykonawczą.

Cała powyżej wymieniona dokumentacja opracowana zostanie w języku polskim i podlegać będzie akceptacji Zamawiającego. Zamawiający dopuszcza przekazanie dokumentacji w wersji elektronicznej w formacie Word lub PDF.

6.6. Wymagania dotyczące testów penetracyjnych funkcjonalności e-platformy (EDM/RDM, e-usługi).

Wykonawca po przeprowadzeniu procesu integracji przedstawia raport w formie uzgodnionej na etapie analizy przedwdrożeniowej oraz zgłasza gotowość systemu do testów funkcjonalnych. Raport z integracji musi dokumentować poprawność przeprowadzenia procesu integracji a w szczególności kompletność danych oraz oferowanych funkcjonalności.

Testy funkcjonalne wykonywane są na podstawie dokumentacji zatwierdzonej na etapie analizy przedwdrożeniowej i mają na celu sprawdzenie wdrożenia oferowanych przez Wykonawcę funkcjonalności. Za realizację testów odpowiada Wykonawca przy współudziale Zamawiającego. Zamawiający zastrzega sobie prawo samodzielnej realizacji testów przy lub bez obecności Wykonawcy. W przypadku realizacji testów bez obecności Wykonawcy, Zamawiający zobowiązuje się do opisu wykrytych błędów w sposób umożliwiający odtworzenie błędu Wykonawcy. Informacje takie będą przekazane w dokumencie będącym protokołem z sesji odbytych testów systemu przez Zamawiającego.

Jeżeli w procesie testowania uwidocznione zostały błędy uniemożliwiające odbiór systemu (lub poszczególnych e-usług) w ramach raportu z testów są one uwidaczniane w tym raporcie wraz z ustaleniem terminu przeprowadzaniem kolejnej tury testów.

Wykonawca w uzgodnionym terminie (jednak nie później niż w ciągu 3 dni roboczych) przedstawia system do drugiej tury testów. W ramach drugiej tury testów weryfikowane są funkcjonalności dla których stwierdzono występowanie błędów w ramach pierwszej tury. Każda tura testów kończy się raportem z testów przedstawionym Zamawiającemu.

W przypadku spełniania warunków odbioru testów funkcjonalnych wdrożenia EDM/RDM, e-usług Zamawiający i Wykonawca podpisują protokół odbioru testów funkcjonalnych.