Załącznik nr 1 do SIWZ, nr sprawy PN-135/18/MS/ZS/UE

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA (OPZ)

Do przetargu pod nazwą:
„Dostawa urządzeń peryferyjnych i komputerów dla Centrum Onkologii – Instytut Im. Marii Skłodowskiej-Curie" dla projektu: „Nowoczesny Szpital, Nowoczesny ZOZ"

1. Zakres projektu

Zgodnie z założeniami Projektu wynikającymi ze Studium Wykonalności o nazwie: „Nowoczesny Szpital, Nowoczesny ZOZ", realizowanego w ramach Regionalnego Programu Operacyjnego Województwa Mazowieckiego na lata 2014-2020 (RPO WM 2014-2020), Oś Priorytetowa: Wzrost e-potencjału Mazowsza, nr i nazwa Osi Priorytetowej: 2.1 E-usługi, numer i nazwa Poddziałania: 2.1.1 E-usługi dla Mazowsza, Centrum Onkologii – Instytut im. Marii Skłodowskiej-Curie w Warszawie znajdującego się przy ulicy Wawelskiej 15B, 02-034 Warszawa, oraz przy ulicy Wilhelma Konrada Roentgena 5, 02-781 Warszawa, zamawia niżej wyszczególnione produkty i usługi, zgodnie z opisem parametrów minimalnych poszczególnych elementów zamówienia, przedstawione poniżej.

Projekt zamówienia został podzielony na następujące Zadania, zgodne z Studium Wykonalności – „SW" oraz Tabelą Kosztów Projektu – „TKP":

1. Wdrożenie lokalnych e-usług (TKP 2)
    a. Licencje na e-usługi dla Partnerów, integracja z systemami informatycznymi Partnerów (TKP 2.2),
    b. Licencje na e-usługi dla Centrum Onkologii (TKP 2.3),
    c. Repozytorium elektronicznej dokumentacji medycznej (TKP 2.4), przeglądarka rekordu medycznego EHR (TKP 2.7),
    d. Adapter komunikacyjny (konektor) (TKP 2.5),
    e. Szyna Danych - Broker informacyjny (TKP 2.6),
    f. Usługi wdrożeniowe i utrzymaniowe (TKP 2.8),
    g. Usługi programistyczne i migracji bazy danych (TKP 2.9),
    h. System operacyjny (TKP 2.10),
    i. Bazy danych (TKP 2.11),
    j. System wideokonferencyjny (TKP 2.12),
    k. Oprogramowanie biurowe (TKP 2.13), oraz zestawy komputerowe (TKP 3.4),
    l. Cloud-computing (TKP 2.14), Koszty utrzymania, w tym zapewnienie dostępu do sieci Internet dla Cloud Computing (TKP 4.1)
2. Zakup sprzętu IT (TKP 3),
    a. Długopisy cyfrowe (TKP 3.1),
    b. Urządzenia wielofunkcyjne (TKP 3.2),
    c. Info-kioski (TKP 3.3),

d. Macierz hybrydowa (TKP 3.5),
e. Firewall Partnerzy Projektu (TKP 3.6),
f. Web Application Firewall - Centrum Danych (TKP 3.7),
g. Database Firewall - Centrum Danych (TKP 3.8),
h. Firewall - Centrum Danych - Centrum Danych (TKP 3.9),
i. Firewall - Centrum Onkologii (TKP 3.10),
j. Koszty utrzymania, w tym zapewnienie dostępu do sieci Internet

2. Przedmiot zamówienia

Niniejsze zamówienie dotyczy następujących części projektu według powyższej klasyfikacji:

1. Wdrożenie lokalnych e-usług (TKP 2)
   a. Oprogramowanie biurowe (TKP 2.13), oraz zestawy komputerowe (TKP 3.4),
2. Zakup sprzętu IT (TKP 3.1)
   a. Urządzenia wielofunkcyjne (TKP 3.2),
   b. Web Application Firewall - Centrum Danych (TKP 3.7),
   c. Database Firewall - Centrum Danych (TKP 3.8),
   d. Firewall - Centrum Danych - Centrum Danych (TKP 3.9),
   e. Firewall - Centrum Onkologii (TKP 3.10).

2. Rezultaty projektu

Niniejszy przetarg wynika z Projektu, który stanowi odpowiedź na zidentyfikowane braki i potrzeby oraz uwarunkowania rynkowe i środowiskowe i obejmuje wprowadzenie e-usług w drodze rozbudowy infrastruktury ICT w zakresie związanym z podstawową, statutową działalnością zarówno Centrum Onkologii jak i Partnerów Projektu, realizowaną w ramach publicznego systemu ochrony zdrowia. Tym samym Projekt przyczynia się do osiągnięcia celu szczegółowego *„Zwiększone wykorzystanie e-usług publicznych”* w ramach Regionalnego Programu Operacyjnego Województwa Mazowieckiego na lata 2014-2020. Jego zasadniczym celem jest *rozwój e-usług świadczonych w obszarze ochrony zdrowia* . Odbiorcami e-usług (beneficjentami Projektu) będą przede wszystkim osoby i instytucje korzystający z usług zarówno Centrum Onkologii jak i Partnerów Projektu. Tak określony cel zasadniczy osiągnięty zostanie poprzez realizację celów szczegółowych:

- *zmniejszenie kosztów funkcjonowania* Centrum Onkologii oraz Partnerów Projektu - realizowany Projekt umożliwi sprawniejszą pracę personelu medycznego, ale także zwiększy jego efektywność, co będzie miało istotny wpływ na świadczone przez niego usługi. Świadczenie usług medycznych na wysokim poziomie, wymaga poza kompetentnym personelem oraz wykorzystaniem nowoczesnego sprzętu również sprawnego dostępu do informacji dotyczących pacjenta,
- *wzrost jakości obsługi pacjenta* - poprawa oferowanych dotychczas usług w zakresie opieki zdrowotnej, a także skrócenie czasu na realizację poszczególnych czynności związanych z obsługą procesu leczniczego. Krótszy czas hospitalizacji będzie możliwy dzięki wczesnej diagnozie i podjęciu właściwego leczenia oraz umożliwi pacjentom szybszy powrót do aktywności zawodowej,
- *poprawa dostępności do danych medycznych* ,

- *wzrost skuteczności leczenia* poprzez bieżący, ciągły dostęp do dokumentacji medycznej pacjentów,
- *wzrost bezpieczeństwa informacji*,
- *skrócenie czasu obsługi pacjenta* – szacuje się, że obsługa pacjenta oraz kontakt z personelem medycznym skróci się o co najmniej 20 minut w przypadku pacjenta korzystającego z e-usług: w związku z wdrożoną usługą e-rejestracji proces obsługi pacjenta skróci się o 10 minut, o kontakt z lekarzem skrócony zostanie o kolejne 10 minut w związku z możliwością wypełnienia ankiety medycznej on-line przed umówioną wizytą (w chwili obecnej taka ankieta jest każdorazowo obowiązkowa do wypełnienia na miejscu tuż przed wizytą).

Rezultatem Projektu będzie w szczególności:
- zwiększenie dostępu do usług medycznych,
- poprawa jakości i bezpieczeństwa świadczonych usług,
- zwiększenie szans w dostępie do e-usług medycznych na obszarach wiejskich.

Realizacja Projektu związana jest z koniecznością sprostania nowym potrzebom w wyniku dynamicznie zmieniającego się otoczenia w następującym zakresie:
- rozwój nowoczesnych technologii w diagnostyce i terapii,
- budowa zintegrowanych platform ponadlokalnych i regionalnych do przechowywania i udostępniania danych medycznych,
- ogólnopolskie projekty:
- Elektroniczna Platforma Gromadzenia, Analizy i Udostępniania zasobów cyfrowych o Zdarzeniach Medycznych P1 (budowa elektronicznej platformy usług publicznych w zakresie ochrony zdrowia umożliwiającej organom administracji publicznej i obywatelom gromadzenie, analizę i udostępnianie zasobów cyfrowych o zdarzeniach medycznych, w zakresie zgodnym z ustawą z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia),
- Platforma P2 udostępniania on-line przedsiębiorcom usług i zasobów cyfrowych rejestrów medycznych.

3. Kontekst prawny

Infrastruktura i system objęty niniejszym postępowaniem obejmuje większą część działalności szpitala, w związku z czym zakres obowiązujących przepisów prawa do uwzględnienia jest bardzo szeroki. Istotnym czynnikiem determinującym zakres obowiązujących przepisów prawa jest również informatyzacja sektora publicznego oraz służby zdrowia przeprowadzana na szczeblu krajowym przez wprowadzenie obowiązkowej rejestracji Elektronicznej Dokumentacji Medycznej. Wobec powyższego Zamawiający wymaga, aby systemy dostarczone przez Wykonawcę spełniały wszelkie obowiązujące oraz wchodzące w życie do końca okresu świadczenia asysty powdrożeniowej przepisy prawa. W tej sytuacji, wskazane poniżej akty prawne, należy traktować jedynie jako akty podstawowe dotyczące przede wszystkim działalności i informatyzacji podmiotów leczniczych, których przepisy Wykonawca jest zobowiązany zastosować w dostarczonych systemach:

- Ustawa z dnia 27 sierpnia 2004 roku o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych (Dz. U. 2004 nr 210 poz. 2135 ze zm.),
- Ustawa z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia (Dz. U. 2015 poz. 636 ze zm.),
- Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2016 poz. 922 ze zm.),
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i

organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. 2004 Nr 100, poz. 1024),

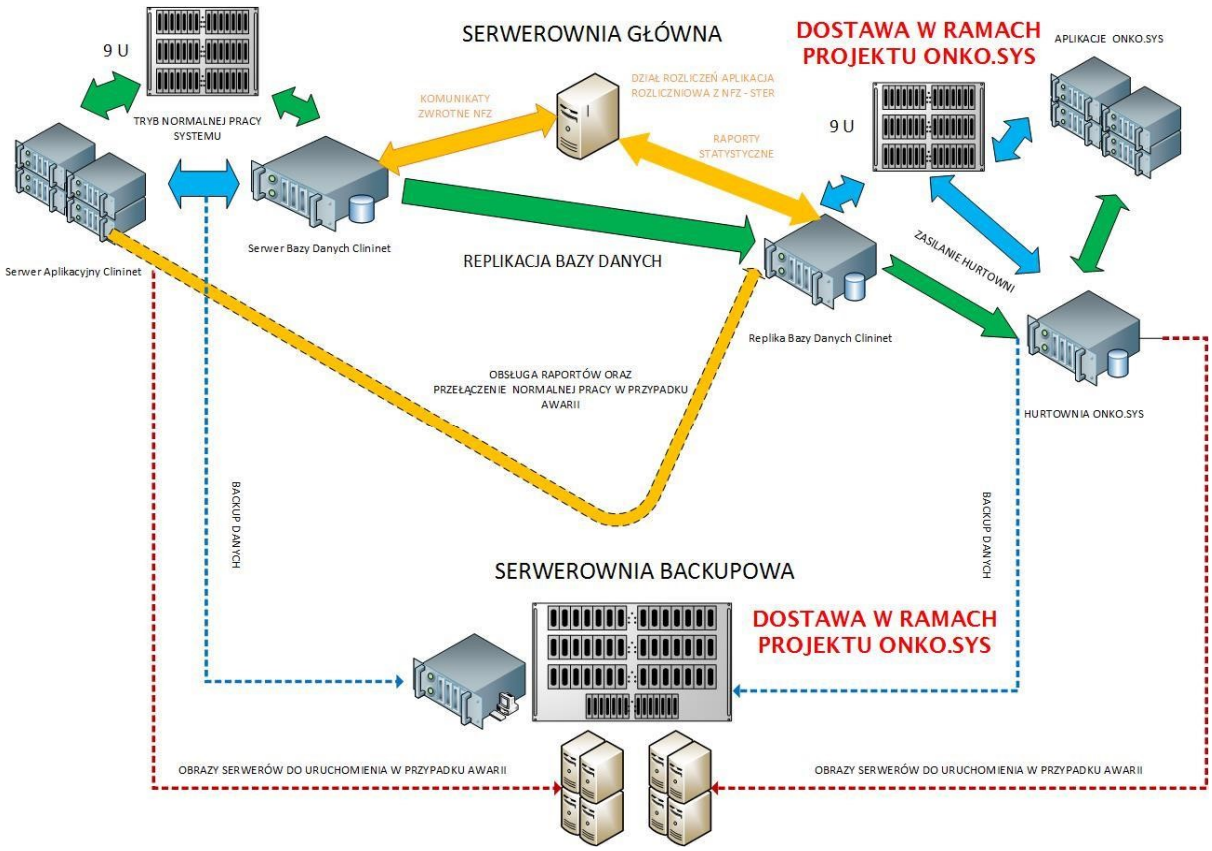
- Rozporządzenie Ministra Zdrowia z dnia 21 grudnia 2010 r. w sprawie rodzajów i zakresu dokumentacji medycznej oraz sposobu jej przetwarzania (Dz. U. 2014 poz. 177 ze zm.),
- Ustawa o dostępie do informacji publicznej (Dz. U. 2001 Nr 112 poz. 1198 z późn. zm.).
- Ustawa z dnia 18 września 2001 r. o podpisie elektronicznym (Dz. U. z 2013 poz. 262 ze zm.),
- Ustawa z dnia 27 lipca 2001r. o ochronie baz danych (Dz. U. 2001 nr 128 poz. 1402 ze zm.).
- Ustawa z dnia 7 lipca 1994 r. - Prawo budowlane (Dz. U. 1994 Nr 89 poz. 414 ze zm.)
- Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. 2012 poz. 526)
- Rozporządzenie Ministra Nauki i Informatyzacji z dnia 19 października 2005 r. w sprawie testów akceptacyjnych oraz badania oprogramowania interfejsowego i weryfikacji tego badania (Dz. U. 2005 nr 217 poz. 1836)
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 30 października 2006 r. w sprawie niezbędnych elementów struktury dokumentów elektronicznych (Dz. U. 2006 nr 206 poz. 1517)
- Rozporządzenie Ministra Infrastruktury z dnia 6 lutego 2003 r. w sprawie bezpieczeństwa i higieny pracy podczas wykonywania robót budowlanych (Dz. U. 2003 nr 47 poz. 401)
- Dyrektywa WE - numer 2006/95/WE w sprawie harmonizacji ustawodawstwa Państw Członkowskich odnoszących się do sprzętu elektrycznego przewidzianego do stosowania w określonych w granicach napięcia.
- PN-IEC 60364-... – Instalacje elektryczne w obiektach budowlanych.
- SEP-E-004 – Elektroenergetyczne i sygnalizacyjne linie kablowe. Projektowanie i budowa.
- Normami EIA/TIA 568 wraz z załącznikami TSB36
- Normami ISO/IEC 11801, EN55022 oraz EN55024 Montaż okablowania strukturalnego
- PN-EN 50130-5 Systemy alarmowe
- PN-EN 50131-1:2009 Systemy alarmowe. Systemy sygnalizacji włamania i napadu
- PN-EN 50131-6:2008 Systemy alarmowe - Systemy sygnalizacji włamania
- PN-EN 50133-1:2007 / A 1:2007 Systemy alarmowe - Systemy Kontroli Dostępu. Wymagania systemowe
- CLC/TS 50131-7:2003 Systemy sygnalizacji włamania
- Ustawa z dnia 22.08.1997r. o ochronie osób i mienia
- PN-B-02840:1991 - Ochrona przeciwpożarowa budynków - Nazwy i określenia
- PN-E-08106:1992 - Stopnie ochrony zapewniane przez obudowy (Kod IP)
- PN-IS08421-4 - Ochrona przeciwpożarowa - Terminologia – Wyposażenie gaśnicze
- PN-M-51004-1:1987 - Części składowe automatycznych urządzeń sygnalizacji pożarowej - Wprowadzenie
- BN 84/8984-10 Zakładowe sieci telekomunikacyjne wnętrzowe. Instalacje wnętrzowe. Ogólne wymagania.
- BN-88/8984-19 - Zakładowe sieci telekomunikacyjne przewodowe. Linie kablowe. Ogólne wymagania.
- PN-IEC 60364-5-52:2002 Instalacje elektryczne w obiektach budowlanych. Dobór i montaż wyposażenia elektrycznego. Oprzewodowanie.

- PN-IEC60364-6-61 Instalacje elektryczne w obiektach budowlanych. Sprawdzanie. Sprawdzanie odbiorcze.
- PN-EN 50173-1:2011 „Technika informatyczna. Systemy okablowania strukturalnego. Część 1: Wymagania ogólne”.
- PN-EN 50174-1:2010 „Technika informatyczna. Instalacja okablowania. Część 1: Specyfikacja i zapewnienie jakości.”
- PN-EN 50174-2:2010 „Technika informatyczna. Instalacja okablowania. Część 2: Planowanie i wykonawstwo instalacji wewnątrz budynków.”
- PN-EN 50174-3:2005 „Technika informatyczna. Instalacja okablowania. Część 3: Planowanie i wykonawstwo instalacji na zewnątrz budynków.”
- PN-EN 50346:2009 „Technika informatyczna. Instalacja okablowania - Badanie zainstalowanego okablowania”

4. Istniejąca infrastruktura

Zaplecze informatyczne Zamawiającego dzieli się na infrastrukturę sieciową, serwerowa, oprogramowanie, systemy medyczne i administracyjne, dwa centra przetwarzania danych zlokalizowane w dwóch lokalizacjach Zamawiającego oraz wiele systemów informatycznych, z którymi systemy wewnętrzne są zintegrowane.

Na poniższym rysunku przedstawiono aktualny stan w zakresie istniejącej infrastruktury:



Serwerownia

Obecna Serwerownia Centrum Onkologii jest obiektem powstałym w 2010 roku, posiada bezpośrednie zasilenie z rozdzielnicy prądowej, system niezależnych redundantnych klimatyzatorów, system alarmowy oraz system monitoringu. Posiada rozbudowaną infrastrukturę światłowodową łącząca budynki Centrum Onkologii (wraz z drugą lokalizacją przy ulicy Wawelskiej) oraz dwa niezależne łącza internetowe. Obecnie w serwerowni pracuje 24 serwerów blade tworzący klaster obsługujący systemy medyczne i administracyjne, na których zainstalowane jest 69 serwerów wirtualnych oraz 16 serwerów pełniących funkcje pomocnicze lub udostępniających usługi sieciowe. W bieżącym roku została uruchomiona druga serwerownia – w odrębnej lokalizacji, która pełni rolę centrum zapasowego. Przetrzymywane są w niej backupy i obrazy maszyn wirtualnych systemów produkcyjnych (medycznych i administracyjnych) oraz wykonywane są repliki on-line bazy danych systemów medycznych dla potrzeb Disaster Recovery i zasilania hurtowni danych. Dane z systemów produkcyjnych przechowywane są na 4 macierzach o łącznej pojemności ponad 200 TB.

Sieci

Obecnie na terenie Centrum Onkologii w Warszawie funkcjonują dwie sieci lokalne: w lokalizacjach przy ul. W.K. Roentgena i ul. Wawelskiej. Sieci są wykonane zgodnie z obowiązującymi normami i umożliwiają dołączenie specjalistycznego sprzętu, stacji roboczych, drukarek i urządzeń sieciowych. Sieci są obsługiwane przez 76 urządzeń aktywnych rozlokowanych w 24 punktach dystrybucyjnych połączonych ze sobą światłowodami. Obydwie lokalizacje są połączone ze sobą stałym łączem światłowodowym. Obecnie w sieci komputerowej Centrum Onkologii pracuje ponad 1700 urządzeń sieciowych (komputerów i drukarek sieciowych)

Partnerzy Projektu

W ramach realizacji projektu uczestniczyć będą Zakłady Opieki Zdrowotnej świadczące usługi na obszarach wiejskich w ramach publicznego systemu ochrony zdrowia. Infrastruktura poszczególnych Partnerów jest stosunkowo prosta z uwagi na fakt, iż nie są to duże podmioty. Każdy z Partnerów posiada od 2 do kilkunastu komputerów stacjonarnych oraz dostęp do sieci internet. Posiadany sprzęt zostanie wykorzystany na potrzeby świadczenia wdrażanych w ramach projektu e-usług. Dodatkowo każdy z Partnerów wyposażony zostanie w dodatkowe komputery, urządzenia wielofunkcyjne oraz infokioski. W każdym POZ Partnera zostanie umieszczony jeden infokiosk oraz zostanie wdrożony system e-usług złożony z e-konsultacji realizowanej z platformy e-Usług COI: e-rejestracja, dostępna poprzez Internet i infokiosk. Dokumenty elektroniczne będą trafiały do EDM dla COI. Partnerzy mogą korzystać z EDM w zakresie własnych systemów lub mogą zintegrować się z EDM COI.

W poniżej tabeli przedstawiono listę systemów informatycznych, funkcjonujących w Partnerów oraz przypisane urządzenia, które należy zainstalować:

1.	Samodzielny Publiczny Zakład Opieki Zdrowotnej w Cegłowie – Przychodnia Opieki Zdrowotne	Kamsoft	10 PC	9 Urządzeń wielofunkcyjnych	1 kpl sieciowy
2.	Samodzielny Publiczny Zakład Opieki Zdrowotnej w Kałuszynie – Przychodnia Opieki Zdrowotnej	Kamsoft	15 PC 2 Stacje Robocze	10 Urządzeń wielofunkcyjnych	1 kpl sieciowy

3.	Wiejski Ośrodek Zdrowia w Wyrozębach- Filia Przychodni Rejonowej w Sokołowie Podlaskim	Eskulap	3 PC	3 Urządzenia wielofunkcyjne	1 kpl sieciowy
4.	Wiejski Ośrodek Zdrowia w Czerwonce – Filia Przychodni Rejonowej w Sokołowie Podlaskim	Eskulap	3 PC	3 Urządzenia wielofunkcyjne	1 kpl sieciowy
5.	Wiejski Ośrodek Zdrowia w Skibniewie – Filia Przychodni Rejonowej w Sokołowie Podlaskim	Eskulap	3 PC	3 Urządzenia wielofunkcyjne	1 kpl sieciowy
6.	Gminny Ośrodek Zdrowia w Repkach – Filia Przychodni Rejonowej w Sokołowie Podlaskim	Eskulap	4 PC	4 Urządzenia wielofunkcyjne	1 kpl sieciowy

5. Streszczenie zakresu zamówienia

Projekt polega na wdrożeniu systemów prowadzenia Elektronicznej Dokumentacji Medycznej zgodnie z ustawą z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia, e-usług oraz stworzeniu zewnętrznego repozytorium przechowywania i wymiany elektronicznej dokumentacji medycznej wraz ze stworzeniem adaptera komunikacyjnego oraz szyny danych ESB umożliwiających podłączenia systemów generujących dokumenty medyczne do repozytorium dokumentów źródłowych. Aby było to możliwe, wszystkie funkcjonalności starego systemu HIS Zamawiającego, którym jest obecnie system CompuGroup Medical Polska CLININET w wersji na system bazodanowy Sybase, muszą zostać zainstalowane na nowej, szybkiej bazie danych, która jest przedmiotem niniejszego zamówienia, oraz zabezpieczone przez urządzenia firewall, będące również przedmiotem niniejszego zamówienia. Po uruchomieniu wszystkich funkcjonalności nowego systemu funkcjonującego na nowej bazie danych, zostanie uruchomiony bezpieczny interfejs komunikacyjny API do komunikacji dwustronnej pomiędzy bazą danych, systemem HIS a systemami EDM i e-Usług. Wykonawca jest zobowiązany zaproponować „Interfejs komunikacyjny API systemu szpitalnego Centrum Onkologii do systemów EDM i e-Usług", który powstanie na podstawie specyfikacji formatów danych i standardów stosowanych w lokalnych systemach HIS i Repozytorium Elektronicznej Dokumentacji Medycznej, stanowiący Załącznik nr 2 do OPZ. Interfejs komunikacyjny, zaproponowany przez Wykonawcę musi zostać załączony jako część analizy przedwdrożeniowej.

Infrastruktura serwerowa dla Projektu ma zostać oparta na outsourcingu mocy obliczeniowych, czyli tzw. „chmury obliczeniowej". Dla potrzeb Projektu wynajęta zostanie moc obliczeniowa w centrum danych oraz zestawione zostaną bezpieczne szyfrowane połączenia za pomocą VPN na urządzeniach Firewall dostarczonych dla każdego z Partnerów w ramach Projektu. Dodatkowo Repozytorium Elektronicznej Dokumentacji Medycznej będzie składowane na macierzy dyskowej umieszczonej w Centrum Danych na zasadach kolokacji. Dla każdego z Parterów zostanie zainstalowana odrębna instancja bazy danych, w ramach której zainstalowane zostaną systemu udostępniające e-usługi. Dodatkowo odrębna baza danych obsługiwała będzie repozytorium elektronicznej dokumentacji medycznej. Zabezpieczenie dostępu do systemów i baz danych realizowane będzie za pomocą dedykowanych urządzeń typu Firewall, Web Application Firewall, Database Firewall.

W ramach Projektu zostanie także przeprowadzona migracja systemu zarządzania bazą danych systemu medycznego Centrum Onkologii do bardziej wydajnego środowiska. Pozwoli to na pełne wdrożenie Elektronicznej Dokumentacji Medycznej w Centrum Onkologii. Obecnie Centrum Onkologii posiada wszystkie niezbędne licencje programowe i infrastrukturę serwerową umożliwiającą prowadzenie Elektronicznej Dokumentacji Medycznej (w tym obsługę podpisu elektronicznego, uruchomiony moduł dokumentacji elektronicznej, lokalne repozytorium EDM), jednakże wielkość liczy rekordów w bazie danych i skala nie pozwala na efektywne wdrożenie rozwiązania. Obecnie w bazie danych systemu medycznego znajduje się:

- 92 566 694 rekordy zawierające pojedyncze badania,
- 85 640 256 rekordów zawierających wyniki (w tym wyniki opisowe),
- 10 135 660 notatek lekarskich ambulatoryjnych,
- 8 288 185 elektronicznych skierowań,
- 5 186 213 notatek lekarskich wykonanych podczas hospitalizacji,
- 636 696 rekordów pojedynczych pacjentów.

Dodatkowo system obsługi medycznej (HIS) jest obecnie zintegrowany ze wszystkimi systemami dziedzinowymi (takimi jak Laboratorium, Mikrobiologia, Markery Nowotworowe, Apteka, systemy obrazowe PACS i systemy obsług Radiologii RIS) – komunikacja odbywa się za pomocą protokołu HL7. Obecnie w systemie w trakcie doby pracuje średnio 1226 osób, z czego w najbardziej obciążonych godzinach ponad 650 jednocześnie.

Dla potrzeb uruchomienia pełnej obsługi elektronicznej dokumentacji medycznej konieczna jest migracja systemu zarządzania bazą danych na bardziej wydajną platformę. Obecny system zarządzania bazą danych przestał być wydajny, pomimo migracji bazy danych na nowe macierze SDD i na nowe serwery o większej mocy obliczeniowej. Ograniczenia licencyjne liczby procesorów obsługujących bazę danych powodują zbyt wolne działanie systemu szpitalnego, a koszty zakupu licencji wersji Enterprise w konfiguracji z repliką on-line są zbyt duże w porównaniu do migracji systemu do nowego systemu zarządzania bazą danych.

Ponadto zostaną zakupione elektroniczne długopisy, dzięki którym pacjenci będą podpisywali dokumenty, które wymagają własnoręcznego podpisu. Obecnie w Centrum Onkologii wymaganych jest ponad 70 różnego rodzaju dokumentów (zgód pacjenta, ankiet itp.), które wymagają takiego podpisu. Poprzez wdrożenie elektronicznego długopisu i integracji go z systemem HIS dokumenty takie będą automatycznie przenoszone do formy elektronicznej, dostępne będą z poziomu rekordu medycznego pacjenta i archiwizowane będą w repozytorium elektronicznej dokumentacji medycznej. Dodatkowo dla w/w potrzeb zostaną zakupione skanery dokumentów, które po zintegrowaniu z systemem HIS będą skanowały dokumenty dostarczone przez Pacjentów i umieszczały je w rekordzie medycznym pacjenta. Dla potrzeb prowadzenia Elektronicznej Dokumentacji Medycznej zostaną zakupione także zestawy komputerowe, które uzupełnią infrastrukturę informatyczną Centrum Onkologii i Partnerów.

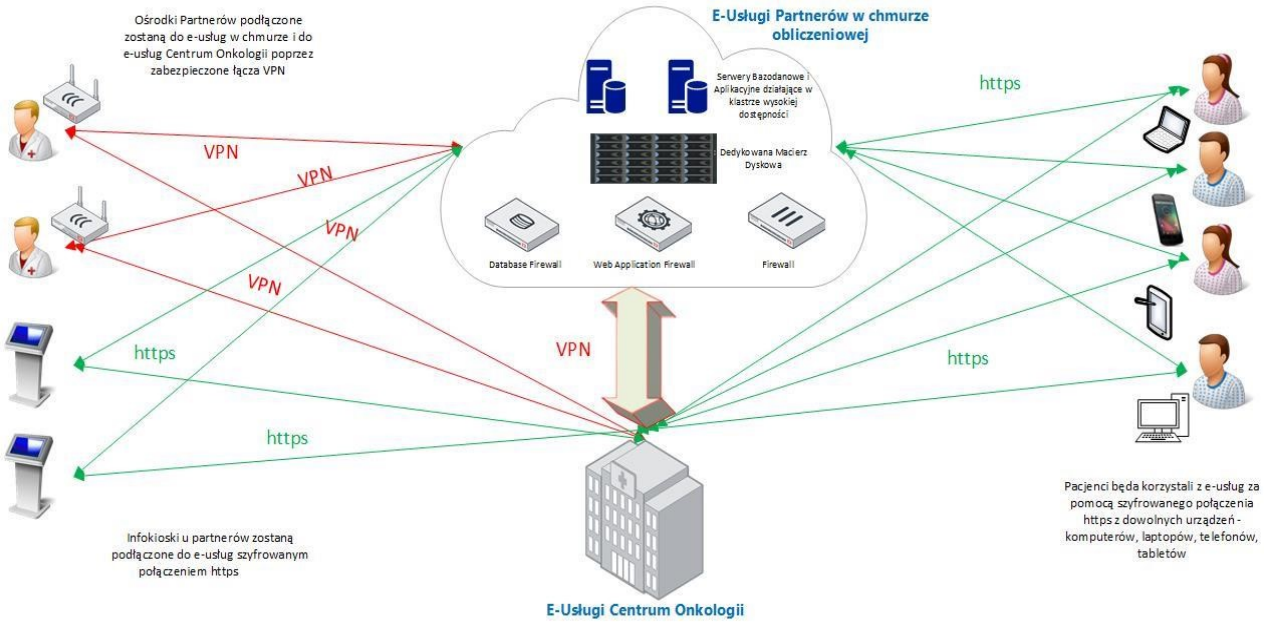
Dla potrzeb obsługi procesu rejestracji pacjentów dostarczone infokioski zostaną zintegrowane z systemem HIS Centrum Onkologii i dzięki wbudowanym skanerom będą umożliwiały potwierdzenie przybycia do Poradni poprzez zeskanowanie kodu z Karty Pacjenta.

Metody uwierzytelniania
Przewiduje się następujące metody uwierzytelniania:

- ePUAP - dla pacjentów korzystających z e-Usług wdrażanych w ramach projektu,
- ePUAP z możliwością dodatkowej autoryzacji tokenem SMS - dla pacjentów korzystających z e-Usług A2C,
- login+hasło lub certyfikat+PIN - dla lekarzy działających na systemie medycznym w placówce medycznej,
- ePUAP + token SMS lub specjalnie założone konto przez administratora systemu dla użytkownika na podstawie wniosku podmiotu współpracującego, uwierzytelnianie hasłem i nazwą użytkownika - dla współpracujących podmiotów wykorzystujących e-Usługi typu A2B.

Systemy u Partnerów należy zintegrować z e-usługami przewidzianymi dla Partnerów, wcześniej wykonać inwentaryzacje zasobów programowych systemu. Jeżeli jest taka możliwość przewiduje się wyłącznie integrację EDM Partnerów z EDM COI. W przypadku starych wersji oprogramowania w Kałuszynie i Cegłowie dopuszcza się równoważnie upgrade systemu do wersji obsługującej e-usługi.

Schemat logiczny Projektu:



Źródło: Studium Wykonalności

6. Szczegółowy opis parametrów minimalnych dla poszczególnych części przedmiotu zamówienia (zgodnie z pkt. 2 OPZ)

Ad 1. Wdrożenie lokalnych e-usług (TKP 2)

a. Oprogramowanie biurowe (TKP 2.13) oraz zestawy komputerowe (TKP 3.4) - 150 zestawów

Dostawa komputerów stacjonarnych (all in one) PC wraz z zainstalowanym systemem operacyjnym i oprogramowaniem biurowym – 120 zestawów.

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne komputerów
1.	Ekran	Przekątna: min. 23 cale Rozdzielczość: min. FHD 1080p (1920x1080), podświetlenie LED, 250nits, format 16:9,
2.	Obudowa	– zintegrowana z monitorem (AIO) – musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej (złącze blokady Kensingtona) – założona blokada kensington musi uniemożliwiać otworzenie tylnej obudowy – Możliwość zainstalowania komputera na ścianie przy wykorzystaniu

		ściennego systemu montażowego VESA z możliwością demontażu stopy. – Obudowa trwale oznaczona nazwą producenta, nazwą komputera, part numberem, numerem seryjnym – Obudowa musi umożliwiać beznarzędziowy demontaż podstawy komputera oraz możliwość wymiany pamięci RAM, dysku M.2 oraz napędy optycznego – Podstawa urządzenia musi oferować użytkownikowi możliwość regulacji w zakresie min. -5° do 24°
3.	Chipset	Dostosowany do zaoferowanego procesora
4.	Płyta główna	Zaprojektowana i wyprodukowana przez producenta komputera Wyposażona w min. 2 złącza M.2 z czego jedno obsługujące dysk SSD PCIe NVMe
5.	Wydajność obliczeniowa	Zaoferowane urządzenie w konfiguracji zgodnej z opisem musi uzyskać w teście BAPCo®SYSmark®2014 „Overall Performance" wynik nie mniej niż 1100 punktów. (wydruk testu załączyć do oferty) Testy, o których jest mowa powyżej, winny być przeprowadzane na urządzeniu z zainstalowanym systemem operacyjnym zgodnym z oferowanym przez Wykonawcę. Jedyna różnica może dotyczyć wersji językowej" Zamawiający zastrzega sobie, iż w celu sprawdzenia poprawności przeprowadzonych testów Wykonawca na życzenie Zamawiającego musi dostarczyć Zamawiającemu oprogramowanie testujące wraz z licencją, zestaw komputerowy w konfiguracji identycznej z wymaganą oraz dokładne opisy użytych testów wraz z wynikami w formatach FDR (Full Disclosure Report) i PDF w terminie nie dłuższym niż 3 dni od otrzymania zawiadomienia od Zamawiającego.
6.	Pamięć operacyjna	min. 8 GB SODIMM DDR4 Ilość banków pamięci: min. 2 szt. Obsługa do min. 32 GB
7.	Dysk twardy	Min 1000 GB, zawierający partycję RECOVERY umożliwiającą odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii.
8.	Napęd optyczny	Nagrywarka DVD +/-RW
9.	Karta graficzna	Zintegrowana karta graficzna wykorzystująca pamięć RAM systemu dynamicznie przydzielaną na potrzeby grafiki w trybie UMA (Unified Memory Access) – z możliwością dynamicznego przydzielenia pamięci.
10.	Audio/Video	Wbudowana, zgodna z HD Audio, wbudowane głośniki stereo 2 x 3W, wbudowany mikrofon, wbudowana kamera HD720p z mechaniczną przesłoną umożliwiającą fizyczne zasłonięcie kamery

11.	Karta sieciowa	LAN 10/100/1000 Mbit/s z funkcją PXE oraz Wake on LAN WiFi 1x1 AC + BT 4.0
12.	Porty/złącza	Wbudowane (minimum): HDMI-out oraz HDMI-in, 5 x USB z czego min 2 x USB3.0 z boku obudowy, 1 x RJ 45 (LAN), 1 x wyjście na słuchawki/wejście na mikrofon (combo) , czytnik kart pamięci min 6 w 1. Wymagana ilość portów nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp.
13.	Klawiatura/mysz	Klawiatura przewodowa w układzie US. Mysz przewodowa z rolką (scroll)
14.	Zasilacz	Maksymalna moc zasilacza nie większa niż 90W 85%
15.	System operacyjny	Microsoft Windows 10 Pro 64 bit lub równoważny umożliwiający: System operacyjny klasy PC musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji: 1. Dostępne dwa rodzaje graficznego interfejsu użytkownika: a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, b. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych 2. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się" pisma użytkownika – obsługa języka polskiego 3. Interfejs użytkownika dostępny w wielu językach do wyboru – w tym polskim i angielskim 4. Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitami i przełączanie się pomiędzy pulpitami za pomocą skrótów klawiaturowych lub GUI. 5. Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe 6. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych, 7. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików. 8. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim 9. Wbudowany system pomocy w języku polskim. 10. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących). 11. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego.

		12. Możliwość dostarczania poprawek do systemu operacyjnego w modelu peer-to-peer. 13. Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące. 14. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników. 15. Możliwość dołączenia systemu do usługi katalogowej on-premise lub w chmurze. 16. Umożliwienie zablokowania urządzenia w ramach danego konta tylko do uruchamiania wybranej aplikacji - tryb "kiosk". 17. Możliwość automatycznej synchronizacji plików i folderów roboczych znajdujących się na firmowym serwerze plików w centrum danych z prywatnym urządzeniem, bez konieczności łączenia się z siecią VPN z poziomu folderu użytkownika zlokalizowanego w centrum danych firmy. 18. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem. 19. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe. 20. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej. 21. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci. 22. Możliwość przywracania systemu operacyjnego do stanu początkowego z pozostawieniem plików użytkownika. 23. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu)." 24. Wbudowany mechanizm wirtualizacji typu hypervisor." 25. Wbudowana możliwość zdalnego dostępu do systemu i pracy zdalnej z wykorzystaniem pełnego interfejsu graficznego. 26. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego. 27. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych, zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6. 28. Identyfikacja sieci komputerowych, do których jest podłączony system

		operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.). 29. Możliwość zdefiniowania zarządzanych aplikacji w taki sposób aby automatycznie szyfrowały pliki na poziomie systemu plików. Blokowanie bezpośredniego kopiowania treści między aplikacjami zarządzanymi a niezarządzanymi. 30. Wbudowany system uwierzytelnienia dwuskładnikowego oparty o certyfikat lub klucz prywatny oraz PIN lub uwierzytelnienie biometryczne. 31. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami. 32. Wbudowany system szyfrowania dysku twardego ze wsparciem modułu TPM 33. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania dysku w usługach katalogowych. 34. Możliwość tworzenia wirtualnych kart inteligentnych. 35. Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu (Secure Boot) 36. Wbudowany w system, wykorzystywany automatycznie przez wbudowane przeglądarki filtr reputacyjny URL. 37. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny. 38. Mechanizmy logowania w oparciu o: a. Login i hasło, b. Karty inteligentne i certyfikaty (smartcard), c. Wirtualne karty inteligentne i certyfikaty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), d. Certyfikat/Klucz i PIN e. Certyfikat/Klucz i uwierzytelnienie biometryczne 39. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5 40. Wbudowany agent do zbierania danych na temat zagrożeń na stacji roboczej. 41. Wsparcie .NET Framework 2.x, 3.x i 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach 42. Wsparcie dla VBScript – możliwość uruchamiania interpretera poleceń 43. Wsparcie dla PowerShell 5.x – możliwość uruchamiania interpretera poleceń
16.	BIOS	BIOS zgodny ze specyfikacją UEFI - Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych podłączonych do niego urządzeń zewnętrznych informacji o:

		- modelu komputera, producencie komputera - numerze seryjnym, - AssetTag, - MAC Adres karty sieciowej, - wersja Biosu wraz z datą produkcji, - zainstalowanym procesorze, jego taktowaniu i ilości rdzeni - ilości pamięci RAM wraz z taktowaniem, - stanie pracy wentylatora - napędach lub dyskach podłączonych do portów SATA oraz M.2 (model dysku twardego i napędu optycznego) Możliwość z poziomu Bios: - wyłączenia selektywnego (pojedynczego) portów USB, - wyłączenia selektywnego (pojedynczego) portów SATA, - wyłączenia wbudowanej kamery, karty WiFi, karty audio, mikrofonu, czytnika kart, - ustawienia hasła: administratora, Power-On, HDD, - wglądu w system zbierania logów z możliwością czyszczenia logów, - wyboru trybu uruchomienia komputera po utracie zasilania (włącz, wyłącz, poprzedni stan) - ustawienia trybu wyłączenia komputera w stan niskiego poboru energii - zdefiniowania trzech sekwencji botujących (podstawowa, WOL, po awarii) - załadowania optymalnych ustawień Bios - zablokowania komputera po nieautoryzowanej zmianie konfiguracji sprzętowej, z poziomu BIOS, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych.
17.	Zintegrowany System Diagnostyczny	Wizualny system diagnostyczny producenta działający nawet w przypadku uszkodzenia dysku twardego z systemem operacyjnym komputera umożliwiający na wykonanie diagnostyki następujących podzespołów: • wykonanie testu pamięci RAM • test dysku twardego • test matrycy LCD • test magistrali PCI-e • test portów USB • test CPU Wizualna sygnalizacja w przypadku błędów któregokolwiek z powyższych podzespołów komputera. Ponadto system powinien umożliwiać identyfikacje testowanej jednostki i jej komponentów w następującym zakresie:

		• Notebook: Producent, PN, model • BIOS: Wersja oraz data wydania Bios • Procesor : Nazwa, taktowanie, obsługiwane instrukcje, ilości pamięci L1, L2, L3 • Pamięć RAM : Ilość zainstalowanej pamięci RAM, obłożenie pamięci na poszczególnych bankach, producent oraz numer seryjny poszczególnych kości pamięci • Dysk twardy: model, numer seryjny, wersja firmware, pojemność, prędkość obrotowa, temperatura pracy • LCD: producent, model, rozmiar, rozdzielczość, System Diagnostyczny działający nawet w przypadku uszkodzenia dysku twardego z systemem operacyjnym komputera.
18.	Certyfikaty i standardy	- Certyfikat ISO9001:2000 dla producenta sprzętu (należy załączyć do oferty) – ENERGY STAR 6.1 - Deklaracja zgodności CE (załączyć do oferty) - Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki
19.	Waga/rozmiary urządzenia	Waga urządzenia wraz ze stopą max. 6,4 kg Suma wymiarów (z podstawą) nie może przekraczać: 1180 mm
20.	Bezpieczeństwo i zdalne zarządzanie	- Złącze typu Kensington Lock - możliwość ustawienia portów USB z poziomu BIOS w jednym z dwóch trybów: 1. użytkownik może kopiować dane z urządzenia pamięci masowej podłączonego do pamięci USB na komputer ale nie może kopiować danych z komputera na urządzenia pamięci masowej podłączone do portu USB; 2. użytkownik nie może kopiować danych z urządzenia pamięci masowej podłączonego do portu USB na komputer oraz nie może kopiować danych z komputera na urządzenia pamięci masowej
21.	Gwarancja	Zgodnie z Załącznikiem nr 6 do SIWZ
22.	Wsparcie techniczne producenta	Dedykowany numer oraz adres email dla wsparcia technicznego i informacji produktowej - możliwość weryfikacji konfiguracji fabrycznej zakupionego sprzętu - możliwość weryfikacji posiadanej/wykupionej gwarancji - możliwość weryfikacji statusu naprawy urządzenia po podaniu unikalnego numeru seryjnego

Dostawa komputerów stacjonarnych (stacja robocza) PC wraz z zainstalowanym systemem operacyjnym i oprogramowaniem biurowym – 2 zestawy dla Partnera w Ka łuszynie.

Nazwa komponentu	Wymagane minimalne parametry techniczne
Typ	Stacja robocza PC lub RACK
Zastosowanie	Komputer będzie wykorzystywany dla potrzeb aplikacji obliczeniowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna
Procesor	Procesor wielordzeniowy osiągający wynik w teście SPECin_rate2006 Base wynik nie mniejszy niż 240 pkt.
Pamięć operacyjna RAM	32GB DDR3 1600MHz non-ECC
Parametry pamięci masowej	Min. dwa dyski 1TB/7200rpm SATA RAID0
Wydajność grafiki	Grafika zintegrowana z procesorem powinna umożliwiać pracę ze wsparciem DirectX 11.1, OpenGL 4.0, OpenCL 1.2
Zgodność z systemami operacyjnymi i standardami	Potwierdzenie kompatybilności komputera na daną platformę systemową (wydruk ze strony)
Wirtualizacja	Sprzętowe wsparcie technologii wirtualizacji realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji dla poszczególnych komponentów systemu).
Warunki gwarancji	Zgodnie z Załącznikiem nr 6 do SIWZ
Wsparcie techniczne producenta	Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej komputera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. Dostęp do najnowszych sterowników i uaktualnień na stronie producenta zestawu realizowany poprzez podanie na dedykowanej stronie internetowej producenta numeru seryjnego lub modelu komputera.
System operacyjny	Zainstalowany system okienkowy system operacyjny w wersji pozwalającej na zarządzanie domeną, umożliwiający instalacje w trybie natywnych aplikacji dedykowanych dla systemu Windows Server umożliwiający uruchomienie minimum dwóch instalacji VM.
Złącza i porty	Wbudowane porty: 1. min. 1 x HDMI out 2. min. 1 x DP out 3. karta WiFi 4. Karta sieciowa 10/100/1000 Ethernet RJ 45, zintegrowana z płytą główną, 5. Klawiatura USB w układzie polski programisty 6. Mysz laserowa USB 7. Dołączony nośnik ze sterownikami
Oprogramowanie biurowe	Pakiet biurowy musi spełniać mieć możliwość podglądu bez edycji materiałów dostępnych w plikach min: rtf, doc, docx, xls, xlsx, ppt.

Dostawa komputerów przenośnych PC wraz z zainstalowanym systemem operacyjnym i oprogramowaniem biurowym – 28 zestawów

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne komputerów
1.	Typ	Komputer przenośny typu notebook z ekranem min 12 max 13" Ekran Wielodotykowy, FHD min. (1920x1200) IPS z podświetleniem w technologii WLED, 320 nits, 16:10 Konstrukcja obudowy musi umożliwiać podłączenie dedykowanej przez producenta klawiatury.
2.	Zastosowanie	Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna
3.	Procesor	Procesor klasy x86, min. 2 rdzeniowy, TDP max. 15W, taktowany zegarem co najmniej 1,60 GHz, z pamięcią last level cache CPU co najmniej 6 MB lub równoważny 4 rdzeniowy procesor klasy x86. Zaoferowany procesor musi osiągać wydajność min. 7500 pkt. osiągniętej w teście Passmark CPU Mark, według wyników procesorów publikowanych na stronie http://cpubenchmark.net.
4.	Pamięć operacyjna RAM	Min. 8 GB DDR4-2133
5.	Parametry pamięci masowej	Min. 256 GB SSD zawierający fabryczną partycję recovery.
6.	Karta graficzna	Zintegrowana w procesorze z możliwością dynamicznego przydzielenia pamięci systemowej, ze sprzętowym wsparciem dla DirectX 12, OpenGL 4.4, ze wsparciem dla 4K, uzyskująca rozdzielczość wyświetlanego obrazu do 4096x2160@60Hz
7.	Wyposażenie multimedialne	Karta dźwiękowa stereo, wbudowane głośniki stereo. Wbudowana w obudowę urządzenia dwie kamery przednia min. 2 Mpix, tylna min. 5 Mpix z auto focusem, dwa mikrofony
8.	Wymagania dotyczące baterii i zasilania	Max 2-cell, min. 39 WH. Zasilacz o mocy max. 45W
9.	Waga i wymiary	Waga i wymiary wraz z klawiatura Waga max 1,26 kg Wysokość przód/tył: max 16 mm
10.	Warunki gwarancji	Zgodnie z Załącznikiem nr 6 do SIWZ
11.	System operacyjny	Microsoft Windows 10 Pro 64 bit lub równoważny umożliwiający: System operacyjny klasy PC musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji: 1. Dostępne dwa rodzaje graficznego interfejsu użytkownika: a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, b. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych 2. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się" pisma użytkownika – obsługa języka polskiego

		3. Interfejs użytkownika dostępny w wielu językach do wyboru – w tym polskim i angielskim 4. Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitami i przełączanie się pomiędzy pulpitami za pomocą skrótów klawiaturowych lub GUI. 5. Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe 6. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych, 7. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików. 8. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim 9. Wbudowany system pomocy w języku polskim. 10. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących). 11. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego. 12. Możliwość dostarczania poprawek do systemu operacyjnego w modelu peer-to-peer. 13. Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące. 14. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników. 15. Możliwość dołączenia systemu do usługi katalogowej on-premise lub w chmurze. 16. Umożliwienie zablokowania urządzenia w ramach danego konta tylko do uruchamiania wybranej aplikacji - tryb "kiosk". 17. Możliwość automatycznej synchronizacji plików i folderów roboczych znajdujących się na firmowym serwerze plików w centrum danych z prywatnym urządzeniem, bez konieczności łączenia się z siecią VPN z poziomu folderu użytkownika zlokalizowanego w centrum danych firmy. 18. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem.

		19. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe. 20. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej. 21. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci. 22. Możliwość przywracania systemu operacyjnego do stanu początkowego z pozostawieniem plików użytkownika. 23. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu)." 24. Wbudowany mechanizm wirtualizacji typu hypervisor." 25. Wbudowana możliwość zdalnego dostępu do systemu i pracy zdalnej z wykorzystaniem pełnego interfejsu graficznego. 26. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego. 27. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych, zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6. 28. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.). 29. Możliwość zdefiniowania zarządzanych aplikacji w taki sposób aby automatycznie szyfrowały pliki na poziomie systemu plików. Blokowanie bezpośredniego kopiowania treści między aplikacjami zarządzanymi a niezarządzanymi. 30. Wbudowany system uwierzytelnienia dwuskładnikowego oparty o certyfikat lub klucz prywatny oraz PIN lub uwierzytelnienie biometryczne. 31. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami. 32. Wbudowany system szyfrowania dysku twardego ze wsparciem modułu TPM 33. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania dysku w usługach katalogowych. 34. Możliwość tworzenia wirtualnych kart inteligentnych. 35. Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu (Secure Boot) 36. Wbudowany w system, wykorzystywany automatycznie przez

		wbudowane przeglądarki filtr reputacyjny URL. 37. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny. 38. Mechanizmy logowania w oparciu o: a. Login i hasło, b. Karty inteligentne i certyfikaty (smartcard), c. Wirtualne karty inteligentne i certyfikaty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), d. Certyfikat/Klucz i PIN e. Certyfikat/Klucz i uwierzytelnienie biometryczne 39. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5 40. Wbudowany agent do zbierania danych na temat zagrożeń na stacji roboczej. 41. Wsparcie .NET Framework 2.x, 3.x i 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach 42. Wsparcie dla VBScript – możliwość uruchamiania interpretera poleceń 43. Wsparcie dla PowerShell 5.x – możliwość uruchamiania interpretera poleceń
12.	Wymagania dodatkowe	BIOS zgodny ze specyfikacją UEFI - Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych podłączonych do niego urządzeń zewnętrznych informacji o: - modelu komputera, producencie komputera - numerze seryjnym, - AssetTag, - MAC Adres karty sieciowej, - wersja Biosu wraz z datą produkcji, - zainstalowanym procesorze, jego taktowaniu i ilości rdzeni - ilości pamięci RAM wraz z taktowaniem, - stanie pracy wentylatora - napędach lub dyskach podłączonych do portów SATA oraz M.2 (model dysku twardego i napędu optycznego) Możliwość z poziomu Bios: - wyłączenia selektywnego (pojedynczego) portów USB, - wyłączenia selektywnego (pojedynczego) portów SATA, - wyłączenia wbudowanej kamery, karty WiFi, karty audio, mikrofonu, czytnika kart, - ustawienia hasła: administratora, Power-On, HDD, - wglądu w system zbierania logów z możliwością czyszczenia logów, - wyboru trybu uruchomienia komputera po utracie zasilania (włącz,

		wyłącz, poprzedni stan) - ustawienia trybu wyłączenia komputera w stan niskiego poboru energii - zdefiniowania trzech sekwencji botujących (podstawowa, WOL, po awarii) - załadowania optymalnych ustawień Bios - zablokowania komputera po nieautoryzowanej zmianie konfiguracji sprzętowej, 1. z poziomu BIOS, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych.

Oprogramowanie biurowe – pakiet 150 licencji

Zamawiający informuje, że posiada aktywną umowę Select Plus Program nadrzędny : S0097938 nr Klienta: 9B0A5E47

Pakiet zintegrowanych aplikacji biurowych
1. Zamawiający nie dopuszcza zaoferowania pakietów biurowych, programów i planów licencyjnych opartych o rozwiązania chmury oraz rozwiązań wymagających stałych opłat w okresie używania zakupionego produktu. 2. Zamawiający nie dopuszcza dostawy licencji typu OEM, PKC i licencji współdzielonych dla użytku domowego 3. Dla oprogramowania musi być publicznie znany cykl życia przedstawiony przez producenta systemu i dotyczący rozwoju wsparcia technicznego – w szczególności w zakresie bezpieczeństwa. Wymagane jest prawo do instalacji aktualizacji i poprawek do danej wersji oprogramowania, udostępnianych bezpłatnie przez producenta na jego stronie internetowej w okresie co najmniej 5 lat. 4. Licencje na oprogramowanie biurowe muszą pozwalać na przenoszenie oprogramowania pomiędzy stacjami roboczymi (np. w przypadku wymiany stacji roboczej). 5. Zamawiający wymaga, aby wszystkie elementy oprogramowania biurowego oraz jego licencja pochodziły od tego samego producenta.
1. interfejs użytkownika w pełnej polskiej wersji językowej, 2. możliwość zdalnej instalacji pakietu oprogramowania poprzez zasady grup (GPO), 3. możliwość automatycznej instalacji komponentów pakietu (przy użyciu instalatora systemowego), 4. wykorzystanie tej samej licencji na komputerze stacjonarnym oraz na komputerze przenośnym użytkownika, 5. prawo do instalacji udostępnianych przez producenta oprogramowania bezpłatnych aktualizacji w okresie co najmniej 5 lat, 6. możliwość zintegrowania uwierzytelniania użytkowników z usługą katalogową (Active Directory) tak, aby użytkownik zalogowany z poziomu systemu operacyjnego stacji roboczej był automatycznie rozpoznawany we wszystkich modułach oferowanego rozwiązania bez potrzeby ponownego uwierzytelniania, 7. tworzenie i edycja dokumentów elektronicznych w ustalonym formacie, który spełnia następujące

warunki:
a) posiada kompletny i publicznie dostępny opis formatu,
b) ma zdefiniowany układ informacji w postaci XML zgodnie z załącznikiem 2 do rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2016 r., poz. 113),
c) umożliwia wykorzystanie schematów XML,
d) wspiera w swojej specyfikacji podpis elektroniczny w formacie XAdES,

8. możliwość nadawania uprawnień do modyfikacji dokumentów tworzonych za pomocą aplikacji wchodzących w skład pakietów oprogramowania,
9. możliwość automatycznego odświeżania danych pochodzących z Internetu w wytworzonych dokumentach elektronicznych, np. w arkuszu kalkulacyjnym,
10. możliwość dodawania do dokumentów i arkuszy kalkulacyjnych podpisów elektronicznych pozwalających na stwierdzenie, czy dany dokument lub arkusz pochodzi z bezpiecznego źródła i nie został w żaden sposób zmieniony,
11. możliwość automatycznego odzyskiwania dokumentów elektronicznych w wypadku nieoczekiwanego zamknięcia aplikacji, np. w wyniku wyłączenia zasilania komputera,
12. prawidłowe odczytywanie i zapisywanie danych w dokumentach w formatach: .DOC, .DOCX, .XLS, .XLSX, .XLSM, .PPT, .PPTX, .MDB, .ACCDB, w tym obsługa formatowania, makr, formuł i formularzy w plikach wytworzonych w MS Office 2003, MS Office 2007, MS Office 2010, MS Office 2013 i MS Office 2016, bez utraty danych oraz bez konieczności reformatowania dokumentów,
13. automatyczne wyróżnianie i aktywowanie hiperłączy w dokumentach podczas edycji i odczytu,
14. oprogramowanie zawiera narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleceń, język skryptowy),
15. oprogramowanie umożliwia dostosowanie dokumentów i szablonów do potrzeb urzędu oraz udostępnianie narzędzia umożliwiające dystrybucję odpowiednich szablonów do właściwych odbiorców,
16. dostępna jest pełna dokumentacja w języku polskim do aplikacji,
17. wszystkie aplikacje w pakiecie oprogramowania biurowego muszą być integralną częścią tego samego pakietu, współpracować ze sobą (osadzanie i wymiana danych), posiadać jednolity interfejs oraz ten sam jednolity sposób obsługi,
18. pakiet zintegrowanych aplikacji biurowych składa się z następujących aplikacji:
    a) edytora tekstów,
    b) arkusza kalkulacyjnego,
    c) narzędzia do przygotowywania i prowadzenia prezentacji,
    d) narzędzia do tworzenia drukowanych materiałów informacyjnych,
    e) narzędzia do zarządzania informacją prywatą (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami),
    f) narzędzia do tworzenia notatek, przy pomocy klawiatury lub notatek odręcznych na ekranie urządzenia typu tablet PC z mechanizmem OCR,
19. edytor tekstów umożliwia:
    a) edycję i formatowanie tekstu w języku polskim, przy czym zapewniona jest obsługa języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalność autokorekty i słownika wyrazów bliskoznacznych,
    b) wstawianie i formatowanie tabel i obiektów graficznych, powiększanie obiektów na cały ekran,

wstawianie obrazów i klipów wideo online, prowadnice wyrównania ułatwiające zestawianie wykresów, zdjęć i diagramów z tekstem,
c) wstawianie tabel i wykresów z arkusza kalkulacyjnego, w tym tabel przestawnych,
d) wykonywanie korespondencji seryjnej bazującej na danych adresowych, np. pochodzących z arkusza kalkulacyjnego, bazy danych, narzędzia do zarządzania informacją prywatną,
e) automatyczne numerowanie rozdziałów, punktów, akapitów, tabel, rysunków, automatyczne tworzenie spisu treści,
f) określenie układu stron (pionowa/pozioma), formatowanie nagłówków i stopek stron, wydruk dokumentów,
g) nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności,
h) praca zespołowa, śledzenie i porównywanie zmian wprowadzonych w dokumencie przez użytkowników, prosta adiustacja zapewniająca przejrzysty widok dokumentu z zachowaniem oznaczeń miejsc wprowadzenia śledzonych zmian, komentarze z możliwością oznaczania ich jako gotowe i dodawania odpowiedzi,
i) pracę na dokumentach utworzonych przy pomocy Microsoft Word 2003, Microsoft Word 2007, Microsoft Word 2010, Microsoft Word 2013 i Microsoft Word 2016, z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu,
j) otwieranie plików PDF i edytowanie ich zawartości (w tym akapitów, list, tabel),
k) zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji,
l) wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go jako środowiska udostępniającego formularze bazujące na schematach XML z centralnego repozytorium wzorów dokumentów elektronicznych (o którym mowa w art. 19b ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2014 r., poz. 1114), które po wypełnieniu umożliwiają zapisanie pliku XML,
m) wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go jako środowiska udostępniającego formularze i pozwalające zapisać plik wynikowy zgodnie z rozporządzeniem Prezesa Rady Ministrów z dnia 27 grudnia 2011 r. w sprawie wymagań technicznych dla dokumentów elektronicznych zawierających akty normatywne i inne akty prawne, dzienników urzędowych wydawanych w postaci elektronicznej oraz środków komunikacji elektronicznej i informatycznych nośników danych (Dz. U. z 2011 r., Nr 289, poz. 1699),

20. arkusz kalkulacyjny umożliwia:
a) tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu, zapis wielu arkuszy kalkulacyjnych w jednym pliku, formatowanie czasu, daty i wartości finansowych z polskim formatem,
b) tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych, automatyczne polecanie wykresu odpowiedniego do wprowadzonych danych,
c) wyszukiwanie i zamianę danych, wykonywanie analiz danych przy użyciu formatowania warunkowego, nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie,
d) tworzenie raportów tabelarycznych,
e) tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice), możliwość osadzania fragmentów arkusza na stronie sieci Web,
f) obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych; narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów

optymalizacyjnych,
g) tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych, automatyczne polecanie sposobów podsumowania danych, korzystanie z możliwości tworzenia układu tabeli przestawnej wykorzystującej jedną lub wiele tabel z wykorzystaniem tej samej listy pól, tworzenie relacji między tabelami, tworzenie osi czasu tabeli przestawnej w celu interaktywnego filtrowania dat,
h) nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności,
i) zachowanie pełnej zgodności z formatami plików utworzonych za pomocą oprogramowania Microsoft Excel 2003, Microsoft Excel 2007, Microsoft Excel 2010, Microsoft Excel 2013 i Microsoft Excel 2016, z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń,
j) zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji,

21. narzędzie do przygotowywania i prowadzenia prezentacji umożliwia:
a) przygotowywanie prezentacji multimedialnych, które będą prezentowane przy użyciu projektora multimedialnego, na monitorze lub tablecie,
b) drukowanie w formacie umożliwiającym robienie notatek,
c) zapisanie jako prezentacja tylko do odczytu,
d) umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo, korzystanie z formatu panoramicznego i rozdzielczości HD, nagrywanie narracji i dołączanie jej do prezentacji, ułatwienia wyrównywania obiektów i stosowania jednakowych odstępów,
e) umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego, odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym,
f) możliwość tworzenia animacji obiektów i całych slajdów,
g) prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera, h) pełna zgodność z formatami plików utworzonych za pomocą oprogramowania MS PowerPoint 2003, MS PowerPoint 2007, MS PowerPoint 2010, MS PowerPoint 2013 i MS PowerPoint 2016,

22. narzędzie do tworzenia drukowanych materiałów informacyjnych umożliwia:
a) tworzenie i edycję drukowanych materiałów informacyjnych, podział treści na kolumny, umieszczanie elementów graficznych,
b) tworzenie materiałów przy użyciu dostępnych z narzędziem szablonów: broszur, biuletynów, katalogów,
c) płynne przesuwanie elementów po całej stronie publikacji, tworzenie tła z obrazów, stosowanie efektów do obrazów i tekstu (np. cienia, odbicia, poświaty, obrotów 3-W),
d) wydruk publikacji, wykorzystanie mechanizmu korespondencji seryjnej,
e) eksport publikacji do formatu PDF oraz TIFF,
f) możliwość przygotowywania materiałów do wydruku w standardzie CMYK,

23. narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) umożliwia:
a) pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego MS Exchange 2010/2013/2016,
b) przechowywanie wiadomości na serwerze lub w lokalnym pliku tworzonym z zastosowaniem efektywnej kompresji danych,
c) filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców,
d) tworzenie katalogów, pozwalających katalogować pocztę elektroniczną, automatyczne grupowanie poczty o tym samym tytule,
e) wspieranie funkcji asystenta podczas nieobecności,

f) tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy, oflagowanie poczty elektronicznej z określeniem terminu przypomnienia, oddzielnie dla nadawcy i adresatów,
g) zarządzanie kalendarzem, udostępnianie kalendarza innym użytkownikom z możliwością określania uprawnień użytkowników, przeglądanie kalendarza innych użytkowników,
h) zapraszanie uczestników na spotkania, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach,
i) zarządzanie listą zadań, zlecanie zadań innym użytkownikom,
j) zarządzanie listą kontaktów, udostępnianie listy kontaktów innym użytkownikom, przeglądanie listy kontaktów innych użytkowników, możliwość przesyłania kontaktów innym użytkowników,

24. narzędzie do tworzenia notatek umożliwia:
a) rejestrowanie informacji przy pomocy klawiatury lub notatek odręcznych na ekranie urządzenia typu tablet PC z mechanizmem OCR,
b) przechowywanie i udostępnianie informacji,

Ad 2. Zakup sprzętu IT (TKP 3)

Wykonawca jest zobowiązany do dostarczenia i zamontowania następujących elementów wyposażenia Zamawiającego i Partnerów, zgodnie z wymaganiami minimalnymi opisanymi poniżej:

a. Urządzenia wielofunkcyjne (TKP 3.2)

Urządzenia drukujące i skanery:

1. Urządzenia wielofunkcyjne – 70 szt.

Lp.		Wymagane minimalne parametry techniczne
1.	Funkcje urządzenia	Drukarka, kopiarka, skanowanie, fax
2.	Technologia druku	Laserowa monochromatyczna
3.	Maks. rozmiar papieru	A4
4.	Maks. szybkość druku mono	Min. 38 str./min.
5.	Dwustronny druk automatyczny	Tak
6.	Maks. wydajność	Min. 100 000 str. miesięcznie
7.	Czas wydruku pierwszej strony	Max. 6,5 sekundy
8.	Procesor	Min. Dual Core 800 MHz
9.	Pamięć	Min. 512 MB
10.	Pojemność podajnika standardowego	250 arkuszy
11.	Pojemność podajnika ręcznego	50 arkuszy
12.	Interfejsy	Min. USB 2.0 (Typ B) Gigabit Ethernet (10/100/1000) IEEE 802.11 b/g/n

		Port USB z przodu zgodny z USB 2.0 (Typ A)
13.	Rozdzielczość druku	Min. 1200x1200 dpi
14.	Druk i skanowanie do USB	Tak
15.	Praca w sieci	Tak
16.	Skaner	Skaner płaski z ADF
17.	Rozdzielczość skanera	Min. 1200 x 600 ppi (mono)
18.	Szybkość skanowania jednostronnego mono	Min. 42 str./min.
19.	Skanowanie do	Min. Skanowanie do email, FTP, USB, do sieci
20.	Skanowanie dwustronne	Tak
21.	Skanowanie do plików	Min. JPEG, JPG, PDF, TIFF
22.	Sterowanie	Kolorowy ekran dotykowy min. 4”
23.	Waga	Max. 20 kg
24.	Gwarancja	Min. 3 lata producenta
25.	Wydajność tonera	Urządzenie dostarczone z oryginalnym tonerem o wydajności min. 2 500 stron
26.	Dodatkowe	Możliwość zakupu oryginalnego tonera pozwalającego na wydruk min. 8 500 stron

2. Urządzenia wielofunkcyjne Typ 2 – 6 szt.

Format papieru min. A4
Rozdzielczość optyczna min. 600x600dpi
Głębia koloru 24-bitowa
Poziomy szarości 256
Prędkość skanowania min. 200ipm
ADF TAK
Szyba skanera TAK
Pojemność ADF min. 150 arkuszy przy 75g/m2
Obciążalność min. 10.000str/dzień
Sieć Ethernet / wifi
Interfejs USB
Ekran dotykowy Tak
Polski Interfejs Użytkownika TAK
Formaty plików PDF, JPG, PNG, BMP, TIFF, TXT, RTF
Kompatybilność Windows 7/8/8.1/10
Skanowanie obustronne TAK
Obsługa sterownika TWAIN, ISIS
Gwarancja - minimum 36 miesięcy

3. Urządzenia wielofunkcyjne Typ 3 – 8 szt.

Format papieru	min. A4
Rozdzielczość optyczna	min. 600x600dpi
Głębia koloru	24-bitowa
Poziomy szarości	256
Prędkość skanowania	min. 60ipm
ADF	TAK
Szyba skanera	TAK
Pojemność ADF	min. 50 arkuszy przy 75g/m2
Sieć	Ethernet / wifi
Obciążalność	min. 4.000str/dzień
Interfejs	USB
Ekran dotykowy	TAK
Polski Interfejs Użytkownika	TAK
Formaty plików	PDF, JPG, PNG, BMP, TIFF, TXT, RTF
Kompatybilność	Windows 7/8/8.1/10
Skanowanie obustronne	TAK
Obsługa sterownika	TWAIN, ISIS
Gwarancja	- minimum 36 miesięcy

b. Web Application Firewall - Centrum Danych (TKP 3.7)

Web Application Firewall (WAF) – 1 szt.

System ochrony aplikacji webowych oraz Firewall XML, którego zadaniem będzie wykrywanie i blokowanie ataków celujących w aplikacje webowe a następnie alarmowanie w wyniku wystąpienia określonych zdarzeń. Powinien zostać dostarczony w postaci komercyjnej platformy sprzętowej lub programowej. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

Architektura systemu

1. Dla zapewnienia wysokiej sprawności i skuteczności działania wymaganym jest aby system pracował w oparciu o dedykowane oprogramowanie, wzmocnione z punktu widzenia bezpieczeństwa.
2. Dla zapewnienia bezpieczeństwa inwestycji i szybkiego wsparcia technicznego ze strony dostawcy wymaga się, aby wszystkie funkcje podstawowe oraz zastosowane w nich technologie, w tym system operacyjny i sprzęt pochodziły od jednego producenta. Nie dopuszcza się aby elementy funkcji podstawowych zastosowane w systemie były opracowane przez firmy trzecie.

3. Powinna istnieć możliwość implementacji systemu w trybach: inline reverse proxy lub transparent, jak również implementacji w trybie nasłuchu.
4. Produkt nie powinien posiadać ograniczeń co do ilości chronionych aplikacji web.
5. Powinna istnieć możliwość zdefiniowania co najmniej 10 domen administracyjnych, w których poszczególni administratorzy zarządzają określonymi funkcjami podstawowymi systemu.
6. System powinien mieć możliwość pracy w konfiguracji HA (High Availability) w trybie Active-Passive.

Parametry fizyczne systemu

1. System realizujący funkcje podstawowe musi dysponować minimum:
   - 4 portami Gigabit Ethernet RJ-45.
   - 2 gniazdami SFP 1 Gbps.
   - 2 gniazdami SFP+ 10 Gbps.
2. Powierzchnia dyskowa – 2 dyski o pojemności minimum 1TB
3. Redundantne zasilanie z sieci 230V/50Hz.
4. Obudowa urządzenia o wysokości do 2U z możliwością montażu w standardowej szafie teletechnicznej 19 cali.

Parametry wydajnościowe

1. Przepustowość dla chronionego ruchu HTTP - min 1,25 Gbps.

Podstawowe funkcje systemu

System musi realizować co najmniej poniższe funkcje:

1. Tryb auto-uczenia – przyspieszający i ułatwiający implementację.
2. Podział obciążenia na kilkanaście serwerów (loadbalancing) z mechanizmami weryfikacji stanu pracy serwerów.
3. Terminowanie połączeń SSL dla wybranych chronionych serwisów.
4. Możliwość analizy poszczególnych rodzajów ruchu w oparciu o polityki bezpieczeństwa (polityka to obiekt określający zbiór ustawień zabezpieczających aplikacje).
5. Kontrola komunikacji XML z możliwością routingu w oparciu o kontent, walidacją schematów XML.
6. Ochrona aplikacji www przed takimi zagrożeniami jak:
   - SQL and OS Command Injection.
   - Cross Site Scripting (XSS).
   - Cross Site Request Forgery.
   - Outbound Data Leakage.
   - HTTP Request Smuggling.
   - Buffer Overflow.
   - Encoding Attacks.
   - Cookie Tampering / Poisoning.
   - Session Hijacking.
   - Broken Access Control.
   - Forceful Browsing /Directory Traversal.
   - Ochrona przed innymi zagrożeniami specyfikowanymi przez listę OWASP.
   - DoS w warstwie aplikacji.

- Ochrona przed atakami typu Brute force.

7. Mechanizmy ochrony przed wyciekiem informacji poufnych.
8. Definiowanie polityk w oparciu o geo-lokalizację.
9. Analiza komunikacji w oparciu o bazy reputacyjne adresów IP, dostarczane przez producenta rozwiązania.
10. Integracja z zewnętrznymi systemami uwierzytelniania dwu-składnikowego.

Wymagane funkcje dodatkowe

1. Kontrola antywirusowa dla komunikacji http realizowana na firewall'u aplikacyjnym lub zewnętrznym systemie w oparciu o protokół icap. W ramach postępowania muszą zostać dostarczone wszystkie elementy (urządzenia, licencje) niezbędne do uruchomienia tej funkcji. Moduł kontroli antywirusowej musi mieć możliwość współpracy z dedykowaną, komercyjną platformą (sprzętową lub wirtualną) lub usługą w chmurze typu Sandbox w celu rozpoznawania nieznanych dotąd zagrożeń.
2. Skaner aplikacji WWW realizowany bezpośrednio na firewall'u aplikacyjnym lub zewnętrznym systemie (w przypadku zewnętrznego systemu skanującego – musi istnieć możliwość importu wyników skanowania do systemu WAF oraz na tej podstawie konfiguracji polityk ochrony). W ramach postępowania muszą zostać dostarczone wszystkie elementy (urządzenia, licencje) niezbędne do uruchomienia tej funkcji.
3. Ochrona przed podmianą strony WWW realizowana bezpośrednio na firewall'u aplikacyjnym lub zewnętrznym systemie. W ramach postępowania muszą zostać dostarczone wszystkie elementy (urządzenia, licencje) niezbędne do uruchomienia tej funkcji.

Zarządzanie

1. Dostarczony system musi umożliwiać lokalne zarządzanie z wykorzystaniem protokołów HTTPS oraz SSH.

Logowanie i Raportowanie

1. System musi zapewniać lokalne logowanie oraz raportowanie - w oparciu o zestaw predefiniowanych wzorców raportów.
2. Możliwość logowania do zewnętrznego serwera Syslog.
3. Obsługa powiadomień o zdarzeniach systemowych oraz incydentach bezpieczeństwa mailem.
4. Powiadomienia o zdarzeniach systemowych oraz incydentach bezpieczeństwa za pośrednictwem trapów SNMP.

Certyfikaty

1. Z punktu widzenia jakości i skuteczności rozwiązania koniecznym jest przedstawienie wyników testów niezależnych organizacji, np. NSS Labs, ICSA Labs lub równoważnego.

Sygnatury, subskrypcje

1. Bazy sygnatur wykorzystywane przez funkcje ochronne powinny być systematycznie aktualizowane zgodnie ze zdefiniowanych harmonogramem.
2. W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych i serwisów. Powinny one obejmować:
   - Skanowanie aplikacji www na okres 60 miesięcy.

- Kontrolę antywirusową, sygnatury ochrony dla aplikacji www oraz bazy reputacyjne adresów IP na okres 60 miesięcy.

Gwarancja oraz wsparcie

System musi być objęty serwisem gwarancyjnym producenta przez okres 60 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 8x5.

Rozszerzone wsparcie serwisowe i inne wymagania

1. System musi być objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w następnym dniu roboczym od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres 60 miesięcy.
2. Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 8x5. Oferent winien przedłożyć oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej).
3. W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.
4. Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

c. Database Firewall - Centrum Danych (TKP 3.8)

System monitorowania poziomu bezpieczeństwa oraz dostępności systemów baz danych.

1. System musi umożliwiać, co najmniej:
   a. Monitorowanie wydajności procesów bazodanowych

   b. Monitorowanie logów bezpieczeństwa pochodzących z monitorowanych systemów baz danych
   c. Monitorowanie dostępności baz danych
   d. Monitorowanie zgodności z założonymi praktykami konfiguracyjnymi baz danych
   e. Liczba monitorowanych systemów baz danych min. 15
   f. Liczba monitorowanych systemów baz danych opartych o system Windows: min. 5
2. Rozwiązanie musi być w stanie przetworzyć min. 5 000 zdarzeń na sekundę, z możliwością rozbudowy.
3. System musi być dostarczony w formie zintegrowanego urządzenia typu appliance lub w formie maszyn wirtualnych wraz z odpowiednią platformą wirtualizacją i sprzętową. Infrastruktura ta musi być zgodna z wymaganiami producenta w zakresie kompatybilności oraz mocy obliczeniowej (RAM,CPU,HDD/SSD) do obsługi monitorowania systemów baz danych wg. wymagań z pkt 1. Niezależnie od formy infrastruktury sprzętowej musi ona spełniać następujące parametry: redundantne zasilanie, minimum 10TB przestrzeni dyskowej z możliwością rozbudowy,
4. System musi umożliwiać zbieranie danych z systemów operacyjnych oraz bazodanowych za pomocą następujących kanałów komunikacji i protokołów:
   a. SYSLOG
   b. WMI
   c. JDBC
   d. ICMP
   e. VMware SDK
   f. JMX
   g. SSH
   h. Telnet
5. Rozwiązanie musi umożliwiać monitorowanie parametrów w obszarze:
   a. Wirtualizatora – min. VMware, Hyper-V, na którym może być zainstalowane środowisko bazodanowe
   b. Systemu operacyjnego gdzie jest zainstalowany silnik bazy danych
   c. Silnika bazy danych
6. Rozwiązanie musi umożliwiać natywne monitorowanie minimum następujących systemów bazodanowych w minimalnym zakresie jak przedstawiono poniżej:
   a. MS SQL Server
      i. Wsparcie minimalnie w następujących wersjach:
         1. SQL Server 2005
         2. SQL Server 2008
         3. SQL Server 2008 R2
         4. SQL Server 2012
         5. SQL Server 2014
      ii. Monitorowanie wydajności minimum w zakresie:
         1. Poziom zużycia procesora (CPU) i pamięci (RAM)
         2. Poziom wykonywanych operacji na dyskach (Read I/O KBytes/sec, Write I/O KBytes/sec)

3. Monitorowanie per instancja bazy danych w zakresie następujących parametrów:
    a. Buffer cache hit ratio,
    b. Log cache hit ratio,
    c. Transactions /sec,
    d. Page reads/sec,
    e. Page writes/sec,
    f. Page splits/sec,
    g. Full scans/sec,
    h. Deadlocks/sec,
    i. Log flush waits/sec,
    j. Latch waits/sec,
    k. Data file(s) size,
    l. Log file(s) used,
    m. Log growths,
    n. Log shrinks,
    o. User connections,
    p. Target server memory,
    q. Total Server Memory,
    r. Active database users,
    s. Logged-in database users,
    t. Available buffer pool pages,
    u. Free buffer pool pages,
    v. Average wait time
4. Monitorowanie per instancja i per baza następujących parametrów:
    a. Database name
    b. Data file size
    c. Log file used
    d. Log growths
    e. Log shrinks
    f. Log flush waits/sec
    g. Transaction /sec
    h. Log cache hit ratio
5. Informacje o zatrzymaniach bazy danych (locks) w zakresie:
    a. Database id,
    b. Database object id,
    c. Lock type,
    d. Locked resource,
    e. Lock mode,
    f. Lock status
6. Informacje o zblokowaniach bazy danych (blocking info) w zakresie:
    a. Blocked Sp Id,
    b. Blocked Login User,
    c. Blocked Database,

d. Blocked Command,
e. Blocked Process Name,
f. Blocking Sp Id,
g. Blocking Login User,
h. Blocking Database, Blocking Command,
i. Blocking Process Name,
j. Blocked duration

iii. Monitorowanie dostępności minimalnie w zakresie:
1. Ogólne informacje o bazie danych:
a. database name,
b. database version,
c. database size,
d. database owner,
e. database created date,
f. database status,
g. database compatibility level
2. Informacje o konfiguracji bazy danch:
a. Configure name,
b. Configure value,
c. Configure max and min value,
d. Configure running value
3. Informacje o kopi zapasowej bazy danych:
a. Database name,
b. Last backup date,
c. Days since last backup

iv. Monitorowanie poziomu bezpieczeństwa oraz zgodności w zakresie:
1. Zdarzenia aplikacyjne silnika bazy danych
2. Śledzenie logów audytowych bazy danych w zakresie:
a. Logowanie użytkowników do bazy danych – poprawne i niepoprawne,
b. Śledzenie operacji na bazie danych w szczególności akcje typu CREATE/ALTER/DROP/TRUNCATE oraz operacje na obiektach typu: tables,table spaces, databases, clusters, users, roles, views, table indices, triggers

b. Oracle Database Server
i. Wsparcie minimalnie w następujących wersjach:
1. Oracle Database 10g
2. Oracle Database 11g
3. Oracle Database 12c
ii. Ogólne informacje o bazie danych:
1. version,
2. Character Setting,

3. Archive Enabled,
4. Listener Status,
5. Instance Status,
6. Last backup date,

iii. Monitorowanie wydajności minimum w zakresie:

1. Poziom zużycia procesora (CPU) i pamięci (RAM)
2. Uptime procesu
3. Poziom wykonywanych operacji na dyskach (Read I/O KBytes/sec, Write I/O KBytes/sec)
4. Monitorowanie parametrów wydajności bazy danych:
   a. Buffer cache hit ratio,
   b. Row cache hit ratio,
   c. Library cache hit ratio,
   d. Shared pool free ratio,
   e. Wait time ratio,
   f. Memory Sorts ratio,
   g. Host CPU Util ratio,
   h. CPU Time ratio,
   i. Disk Read/Write rates (operations and MBps),
   j. Network I/O Rate,
   k. Enqueue Deadlock rate,
   l. Database Request rate,
   m. User Transaction rate,
   n. User count, Logged on user count,
   o. Session Count, System table space usage,
   p. User table space usage, Temp table space usage,
   q. Last backup date, Days since last backup
5. Monitorowanie parametrów wydajności table:
   a. Table space name,
   b. table space type,
   c. table space usage,
   d. table space free space,
   e. table space next extent
6. Monitorowanie logów pochodzących z:
   a. Audit log, Listener Log, Alert log
7. Monitorowanie bezpieczeństwa na podstawie:
   a. Logowanie użytkowników do bazy danych – poprawne i niepoprawne,
   b. Śledzenie operacji na bazie danych w szczególności akcje typu CREATE/ALTER/DROP/TRUNCATE oraz operacje na obiektach typu: tables,table spaces, databases, clusters, users, roles, views, table indices, triggers

c. MySQL Server

i.

ii. Ogólne informacje o bazie danych:
    1. version,
    2. Character Setting,
iii. Monitorowanie wydajności minimum w zakresie:
    1. Poziom zużycia procesora (CPU) i pamięci (RAM)
    2. Uptime procesu
    3. Poziom wykonywanych operacji na dyskach (Read I/O KBytes/sec, Write I/O KBytes/sec)
    4. Monitorowanie bazy danych w oparciu o parametry:
        a. User COnnections,
        b. Table Updates,
        c. table Selects,
        d. Table Inserts,
        e. Table Deletes,
        f. Temp Table Creates,
        g. Slow Queries,
        h. Query cache Hits,
        i. Queries registered in cache,
        j. Database Questions,
        k. Users,
        l. Live Threads
    5. Monitorowanie przestrzeni table w oparciu o parametry:
        a. Table space name,
        b. table space type,
        c. Character set and Collation,
        d. table space usage,
        e. table space free space,
        f. Database engine, Table version,
        g. Table Row Format,
        h. Table Row Count,
        i. Average Row Length,
        j. Index File length,
        k. Table Create time,
        l. Table Update Time
    6. Śledzenie logów audytowych bazy danych w zakresie:
        a. Logowanie użytkowników do bazy danych – poprawne i niepoprawne,
        b. Śledzenie operacji na bazie danych w szczególności akcje typu CREATE/DELETE/MODIFY na bazie danych, CREATE/DELETE/MODIFY/INSERT na tabeli

d. IBM DB2 Server
    i. Ogólne informacje o bazie danych:

1. version,
2. Character Setting,

ii. Monitorowanie wydajności minimum w zakresie:
1. Poziom zużycia procesora (CPU) i pamięci (RAM)
2. Uptime procesu
3. Poziom wykonywanych operacji na dyskach (Read I/O KBytes/sec, Write I/O KBytes/sec)
4. Monitorowanie bazy danych w oparciu o parametry:
   a. User Connections,
   b. Table Updates,
   c. table Selects,
   d. Table Inserts,
   e. Table Deletes,
   f. Temp Table Creates,
   g. Slow Queries,
   h. Query cache Hits,
   i. Queries registered in cache,
   j. Database Questions,
   k. Users, Live Threads
5. Monitorowanie przestrzeni tabel w oparciu o parametry:
   a. Table space name,
   b. table space type,
   c. Character set and Collation,
   d. table space usage,
   e. table space free space,
   f. Database engine,
   g. Table version,
   h. Table Row Format,
   i. Table Row Count,
   j. Average Row Length,
   k. Index File length,
   l. Table Create time,
   m. Table Update Time
6. Śledzenie logów audytowych bazy danych w zakresie:
   a. Logowanie użytkowników do bazy danych – poprawne i niepoprawne,
   b. Śledzenie operacji na bazie danych w szczególności akcje typu CREATE/DELETE/MODIFY na bazie danych, CREATE/DELETE/MODIFY/INSERT na tabeli

e. System musi umożliwiać dodanie innych – niewspieranych domyślnie typów baz danych lub dodatkowych parametrów do monitorowania, które można uzyskać za pomocą wspieranych protokołów przez takich jak:
   i. SYSLOG
   ii. WMI

iii. JDBC
iv. ICMP
v. VMware SDK
vi. JMX
vii. SSH
viii. Telnet

Gwarancja oraz wsparcie

System musi być objęty serwisem gwarancyjnym producenta przez okres 60 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 8x5.

Rozszerzone wsparcie serwisowe i inne wymagania

1. System musi być objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w następnym dniu roboczym od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres 60 miesięcy.
2. Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 8x5. Oferent winien przedłożyć oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej).
3. W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.
4. Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

d. Firewall - Centrum Danych - Centrum Danych (TKP 3.9)

Wymagania Ogólne
Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trybów: Routera z funkcją NAT, transparentnym.

W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, IPS, Antywirus. Powinna istnieć możliwość dedykowania co najmniej 8 administratorów do poszczególnych instancji systemu.

System musi wspierać IPv6 oraz IPv4 w zakresie:

- Firewall.
- Protokołów routingu dynamicznego.

Redundancja, monitoring i wykrywanie awarii

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Passive. Powinna istnieć funkcja synchronizacji sesji firewall.
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.
4. System musi umożliwiać agregację linków w oparciu o protokół LACP

Interfejsy, Dysk, Zasilanie:

1. System realizujący funkcję Firewall musi dysponować minimum:
   - 10 portami Gigabit Ethernet RJ-45.
   - 8 gniazdami SFP 1 Gbps.
   - 4 gniazdami SFP+ 10 Gbps.
2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.
4. System realizujący funkcję Firewall musi być wyposażony w dysk SSD o pojemności minimum 120 GB.
5. System musi być wyposażony w zasilanie AC.

Parametry wydajnościowe:

1. W zakresie Firewall'a obsługa nie mniej niż 2 mln jednoczesnych połączeń oraz 100.000 nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 36 Gbps dla pakietów 1518 B.
3. Wydajność szyfrowania VPN IPSec, przy zastosowaniu algorytmu o mocy nie mniejszej niż AES256: nie mniej niż 5 Gbps.
4. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) - minimum 11 Gbps.
5. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 4 Gbps.

Funkcje Systemu Bezpieczeństwa:

W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, HTTP, FTP, HTTPS.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Analiza ruchu szyfrowanego protokołem SSL.

Polityki, Firewall

1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
   - Translację jeden do jeden oraz jeden do wielu.
3. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.

Połączenia VPN

1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:
   - Wsparcie dla IKE v1 oraz v2.
   - Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów.
   - Obsługa protokołu Diffie-Hellman grup 19 i 20.
   - Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh.
   - Tworzenie połączeń typu Client-to-Site oraz Site-to-Site.
   - Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
   - Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
   - Obsługa mechanizmów: IPSec NAT Traversal.

- Mechanizm „Split tunneling” dla połączeń Client-to-Site.

2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:
   - Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki.
   - Pracę w trybie Tunnel przy zastosowaniu dedykowanego klienta.

Routing i obsługa łączy WAN

1. W zakresie routingu rozwiązanie powinno zapewniać obsługę:
   - Routingu statycznego.
   - Policy Based Routingu.
2. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP.
3. System musi umożliwiać obsługę kilku (co najmniej dwóch) łączy WAN z mechanizmami statycznego lub dynamicznego podziału obciążenia oraz monitorowaniem stanu połączeń WAN.

Zarządzanie pasmem

1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.

Kontrola Antywirusowa

1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.
3. Moduł kontroli antywirusowej musi mieć możliwość współpracy z dedykowaną, komercyjną platformą (sprzętową lub wirtualną) lub usługą w chmurze typu Sandbox w celu rozpoznawania nieznanych dotąd zagrożeń.

Ochrona przed atakami

1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. Baza sygnatur ataków powinna zawierać minimum 1500 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
4. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS.
5. Mechanizmy ochrony (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, BotNETy) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL.
6. Wykrywanie i blokowanie komunikacji do sieci botnet.

Kontrola aplikacji

1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji powinna zawierać minimum 300 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.

3. Powinny być kontrolowane aplikacje chmurowe co najmniej: Google Docs, Facebook, Dropbox.
4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.

Kontrola WWW

1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 20 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, proxy avoidance.
3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.
4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.

Uwierzytelnianie użytkowników w ramach sesji

1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:
   - Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
   - Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
   - Haseł dynamicznych (RADIUS) w oparciu o zewnętrzne bazy danych.
2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.
3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory.

Zarządzanie

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
3. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3.
4. System musi mieć wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.

Logowanie

1. System musi mieć możliwość logowania do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
2. W ramach logowania system musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.

3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
4. Musi istnieć możliwość logowania do serwera SYSLOG.

Certyfikaty

Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:

- ICSA lub EAL4 dla funkcji Firewall.
- ICSA lub EAL4 dla funkcji VPN.

Serwisy i licencje

W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować: kontrole aplikacji, IPS, Antywirus, Antyspam, Web Filtering na okres 60 miesięcy.

Gwarancja oraz wsparcie

1. Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 60 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 8x5.

Rozszerzone wsparcie serwisowe i inne wymagania

5. System musi być objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w następnym dniu roboczym od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres 60 miesięcy.
6. Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 8x5. Oferent winien przedłożyć oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej).
7. W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.

8. Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

e. Firewall - Centrum Onkologii (TKP 3.10)

Firewall – Centrum Onkologii –1 szt.

Wymagania Ogólne
Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trybów: Routera z funkcją NAT, transparentnym.

W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, IPS, Antywirus. Powinna istnieć możliwość dedykowania co najmniej 8 administratorów do poszczególnych instancji systemu.

System musi wspierać IPv6 oraz IPv4 w zakresie:

- Firewall.
- Protokołów routingu dynamicznego.

Redundancja, monitoring i wykrywanie awarii

5. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Passive. Powinna istnieć funkcja synchronizacji sesji firewall.
6. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
7. Monitoring stanu realizowanych połączeń VPN.
8. System musi umożliwiać agregację linków w oparciu o protokół LACP

Interfejsy, Dysk, Zasilanie:

6. System realizujący funkcję Firewall musi dysponować minimum:
   - 10 portami Gigabit Ethernet RJ-45.
   - 8 gniazdami SFP 1 Gbps.
   - 4 gniazdami SFP+ 10 Gbps.
7. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.

8. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.
9. System realizujący funkcję Firewall musi być wyposażony w dysk SSD o pojemności minimum 120 GB.
10. System musi być wyposażony w zasilanie AC.

Parametry wydajnościowe:

6. W zakresie Firewall'a obsługa nie mniej niż 2 mln jednoczesnych połączeń oraz 100.000 nowych połączeń na sekundę.
7. Przepustowość Stateful Firewall: nie mniej niż 36 Gbps dla pakietów 1518 B.
8. Wydajność szyfrowania VPN IPSec, przy zastosowaniu algorytmu o mocy nie mniejszej niż AES256: nie mniej niż 5 Gbps.
9. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) - minimum 11 Gbps.
10. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 4 Gbps.

Funkcje Systemu Bezpieczeństwa:

W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

10. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
11. Kontrola Aplikacji.
12. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
13. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, HTTP, FTP, HTTPS.
14. Ochrona przed atakami - Intrusion Prevention System.
15. Kontrola stron WWW.
16. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
17. Zarządzanie pasmem (QoS, Traffic shaping).
18. Analiza ruchu szyfrowanego protokołem SSL.

Polityki, Firewall

4. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
5. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
   - Translację jeden do jeden oraz jeden do wielu.
6. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.

Połączenia VPN

3. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:
   - Wsparcie dla IKE v1 oraz v2.
   - Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów.
   - Obsługa protokołu Diffie-Hellman grup 19 i 20.
   - Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh.

- Tworzenie połączeń typu Client-to-Site oraz Site-to-Site.
- Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
- Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
- Obsługa mechanizmów: IPSec NAT Traversal.
- Mechanizm „Split tunneling" dla połączeń Client-to-Site.

4. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:
   - Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki.
   - Pracę w trybie Tunnel przy zastosowaniu dedykowanego klienta.

Routing i obsługa łączy WAN

4. W zakresie routingu rozwiązanie powinno zapewniać obsługę:
   - Routingu statycznego.
   - Policy Based Routingu.
5. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP.
6. System musi umożliwiać obsługę kilku (co najmniej dwóch) łączy WAN z mechanizmami statycznego lub dynamicznego podziału obciążenia oraz monitorowaniem stanu połączeń WAN.

Zarządzanie pasmem

3. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
4. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.

Kontrola Antywirusowa

4. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
5. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.
6. Moduł kontroli antywirusowej musi mieć możliwość współpracy z dedykowaną, komercyjną platformą (sprzętową lub wirtualną) lub usługą w chmurze typu Sandbox w celu rozpoznawania nieznanych dotąd zagrożeń.

Ochrona przed atakami

7. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
8. Baza sygnatur ataków powinna zawierać minimum 1500 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
9. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
10. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS.
11. Mechanizmy ochrony (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, BotNETy) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL.
12. Wykrywanie i blokowanie komunikacji do sieci botnet.

Kontrola aplikacji

6. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu nie bazując jedynie na wartościach portów TCP/UDP.
7. Baza Kontroli Aplikacji powinna zawierać minimum 300 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
8. Powinny być kontrolowane aplikacje chmurowe co najmniej: Google Docs, Facebook, Dropbox.
9. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
10. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.

Kontrola WWW

6. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 20 milionów adresów URL pogrupowanych w kategorie tematyczne.
7. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, proxy avoidance.
8. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.
9. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
10. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.

Uwierzytelnianie użytkowników w ramach sesji

4. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:
   - Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
   - Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
   - Haseł dynamicznych (RADIUS) w oparciu o zewnętrzne bazy danych.
5. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.
6. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory.

Zarządzanie

5. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.
6. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
7. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3.
8. System musi mieć wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.

Logowanie

5. System musi mieć możliwość logowania do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system

logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.

6. W ramach logowania system musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
7. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
8. Musi istnieć możliwość logowania do serwera SYSLOG.

Certyfikaty

Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:

- ICSA lub EAL4 dla funkcji Firewall.
- ICSA lub EAL4 dla funkcji VPN.

Serwisy i licencje

W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować: kontrole aplikacji, IPS, Antywirus, Antyspam, Web Filtering na okres 60 miesięcy.

Gwarancja oraz wsparcie

2. Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 60 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 8x5.

Rozszerzone wsparcie serwisowe i inne wymagania

9. System musi być objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w następnym dniu roboczym od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres 60 miesięcy.
10. Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 8x5. Oferent winien przedłożyć oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej).
11. W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz

dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.

Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

Załącznik Nr 2 do SIWZ
Formularz ofertowy

Postępowanie nr PN-135/18/MS/ZS/UE

Dotyczy: postępowania o udzielenie zamówienia publicznego prowadzonego w trybie przetargu nieograniczonego na „Dostawę urządzeń peryferyjnych i komputerów dla Centrum Onkologii – Instytut Marii Skłodowskiej Curie" ramach RPMA.02.01.01-14-2641/15-00"

FORMULARZ OFERTOWY

I. OFERTĘ SKŁADA:

Nazwa Wykonawcy	
wpisany do:	• Rejestru przedsiębiorców Krajowego Rejestru Sądowego prowadzonego przez Sąd Rejonowy ..... pod nr KRS ..... • lub do Centralnej Ewidencji i Informacji o Działalności Gospodarczej .....
NIP	
REGON	
Adres:	
Telefon:	
Fax:	
e-mail:	

Osoba upoważniona do kontaktu z Zamawiającym (imię i nazwisko, telefon, fax, e-mail)	
To małe/średnie przedsiębiorstwo	TAK/NIE* *(odpowiednie skreślić)*
Hasło dostępu do dokumentu JEDZ	
Nazwa programu szyfrującego	
Instrukcja odszyfrowania pliku z dokumentem JEDZ	

II. OFERTA WYKONAWCY

My, niżej podpisani, niniejszym oświadczamy, co następuje:

1. Oferujemy realizację całego przedmiotu zamówienia zgodnie z wymaganiami zawartymi w Specyfikacji Istotnych Warunków Zamówienia za **łączną** cenę:

Wartość netto: ..... PLN

(słownie wartość netto: .....PLN)

Wartość brutto: ..... PLN

(słownie wartość brutto: .....PLN)

w tym:

Lp.	Przedmiot oferty	Liczba szt.	Opis sprzętu i oprogramowania (Typ, rodzaj, nazwa, producent, numer oraz inne informację w celu weryfikacji)	Cena jednostkowa netto w zł	Cena łączna netto w zł	Stawka podatku VAT lub „odwrotne obciążenie”	Cena łączna brutto w zł	uwagi
1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*
1.	Zestawy komputerowe, w tym:	150						
1a	Typ 1 stacjonarne z systemem operacyjnym i pakietem biurowym	120						
1b	Typ 2 stacjonarne z systemem operacyjnym i pakietem biurowym	2						
1c	Typ 3 przenośne z systemem operacyjnym i pakietem biurowym	28						
2.	Urządzenia wielofunkcyjne, w tym:	84						
2a	Urządzenia wielofunkcyjne typ 1	70						
2b	Urządzenia wielofunkcyjne typ 2	6						
2c	Urządzenia wielofunkcyjne typ 3	8						

3.	Web Application Firewall - Centrum Danych	1						
4.	Database Firewall - Centrum Danych	1						
5.	Firewall - Centrum Danych - Centrum Danych	1						
6.	Firewall - Centrum Onkologii	1						
∑ pozycji: 1-6								

1.1. Okres gwarancji w zakresie poz. 1-23 : ..... (min. 36 mcy)
1.2. Okres gwarancji w zakresie poz.: 3-6 :.....(min. 60 mcy)

2. Oferujemy 60 dniowy termin płatności od daty dostarczonej faktury.

3. Podane w Ofercie ceny obejmują pełny przedmiot i zakres zamówienia zgodnie z zasadami i warunkami określonymi w SIWZ a także uwzględniają wszystkie składniki związane z realizacją przedmiotu zamówienia wpływające na wysokość ceny.

4. Oświadczamy, że przedmiot zamówienia wykonamy w terminie – do 60 dni od daty zawarcia umowy

5. Uważamy się za związanych niniejszą ofertą przez okres 60 dni od upływu terminu składania ofert. Na potwierdzenie tego wnieśliśmy wadium w wysokości .....PLN (słownie:.....PLN)

   w postaci .....

6. Jesteśmy świadomi, że gdyby z naszej winy nie doszło do zawarcia umowy, wniesione przez nas wadium ulega przepadkowi.

7. Wadium należy zwrócić na rachunek bankowy *(w przypadku gdy wadium zostało wniesione w formie pieniężnej)*

   .....
   (nazwa banku, numer rachunku bankowego)

   .....
   (nazwa i adres posiadacza rachunku bankowego)

8. W przypadku wyboru naszej oferty zobowiązujemy się do podpisania umowy bez zastrzeżeń na warunkach zawartych w Specyfikacji Istotnych Warunków w terminie i miejscu wyznaczonym przez Zamawiającego.

9. Informujemy, że zamierzamy* / nie zamierzamy* powierzyć części zamówienia podwykonawcom (jeżeli TAK, należy wskazać w ofercie części zamówienia, których wykonanie zostanie powierzone podwykonawcom):

   1) .....
   2) .....

10. Informacje zawarte na stronach ..... stanowią tajemnicę przedsiębiorstwa w rozumieniu art. 11 ust. 4 Ustawy O Zwalczaniu Nieuczciwej Konkurencji (tekst jednolity Dz. U. z 2003 r. Nr 153, poz. 1503 z późn. zm.) i nie mogą być udostępniane przez Zamawiającego. *
11. Nadzór nad realizacją umowy ze strony Wykonawcy będzie pełnił/a:

.....

tel. ..... faks:..... e-mail: .....

12. Ofertę niniejszą składamy na ..... kolejno ponumerowanych stronach.

13. Oświadczam, że wypełniłem obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu.

Zgodnie z wymaganiami zawartymi w SIWZ załącznikami do niniejszego formularza stanowiącymi integralną część oferty są:

1) ..... str. .....
2) ..... str. .....
3) ..... str. .....

....

Miejscowość, data

Czytelny podpis osób uprawnionych do składania oświadczeń woli w imieniu Wykonawcy lub pieczątka wraz z podpisem

**niepotrzebne skreślić*

Załącznik Nr 3 do SIWZ, nr sprawy PN-135/18/MS/ZS/UE

pieczęć Wykonawcy

OŚWIADCZENIE

składane w terminie 3 dni od zamieszczenia na stronie internetowej zamawiającego informacji o której mowa w art. 86 ust. 5 ustawy PZP (protokół z otwarcia ofert)

Zgodne z art. 24 ust. 11 ustawy z dn. 29 stycznia 2004 r. – Prawo zamówień publicznych

Przystępując do udziału w postępowaniu o udzielenie zamówienia publicznego na:

„Dostawa urządzeń peryferyjnych i komputerów dla Centrum Onkologii – Instytut Marii Skłodowskiej Curie" realizowanym w ramach RPMA.02.01.01-14-2641/15-00"

oświadczam/y, że wobec reprezentowanego przeze mnie podmiotu nie zachodzą przesłanki wykluczenia z art. 24 ust. 1 pkt. 23 upzp

⇒ nie przynależę do tej samej grupy kapitałowej, w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (Dz. U. z 2015 r. poz. 184, 1618 i 1634), z Wykonawcami którzy złożyli odrębne oferty, oferty częściowe lub wnioski o dopuszczenie do udziału w przedmiotowym postępowaniu, *
lub

⇒ należę do tej samej grupy kapitałowej, w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (Dz. U. z 2015 r. poz. 184, 1618 i 1634), z Wykonawcami którzy złożyli odrębne oferty, oferty częściowe lub wnioski o dopuszczenie do udziału w przedmiotowym postępowaniu,

⇒ i składam (nie składam)* wyjaśnienia i dowody, ze powiązania z innym wykonawcą nie prowadzą do zakłócenia konkurencji w postępowaniu o udzielenie przedmiotowego zamówienia.*

.....

....., dnia .....2018 r.

.....
podpis i pieczęć imienna osoby(osób) uprawnionej(ych) do reprezentowania Wykonawcy

*- *niepotrzebne skreślić*

Załącznik nr 4 do SIWZ, nr PN-135/18/MS/ZS/UE
Wykaz dostaw

.....

Pieczęć firmowa Wykonawcy

W Y K A Z DOSTAW
(wykaz wykonanych zamówień)

Przystępując do udziału w postępowaniu o udzielenie zamówienia publicznego w trybie przetargu nieograniczonego, którego przedmiotem jest:

„Dostawa urządzeń peryferyjnych i komputerów dla Centrum Onkologii – Instytut Marii Skłodowskiej Curie" realizowanym w ramach RPMA.02.01.01-14-2641/15-00"

przedstawiam wykaz wykonanych dostaw, w okresie ostatnich trzech lat przed upływem terminu składania ofert:

L.p.	Przedmiot dostawy	Wartość brutto dostawy (PLN)	Termin realizacji dostawy		Podmiot, na rzecz którego dostawa została wykonana
			Data rozpoczęcia	Data zakończenia	

Do wykazu należy dołączyć dowód potwierdzający, że wymienione dostawy zostały wykonane należycie

Dowodami są:

1) referencje bądź inny dokumenty wystawione przez podmiot, na rzecz którego dostawy były wykonywane,
2) oświadczenie Wykonawcy - jeżeli z uzasadnionych przyczyn o obiektywnym charakterze Wykonawca nie jest w stanie uzyskać referencji/dokumentów, o którym mowa w pkt. 1.

W przypadku gdy Wykonawca wystawia dokument o którym mowa w pkt. 2, należy wskazać uzasadnione przyczyny o obiektywnym charakterze, że Wykonawca nie jest w stanie uzyskać referencji/dokumentów o którym mowa w pkt. 1

data.....

.....

czytelny podpis lub podpis z pieczątką imienną osoby/osób upoważnionej/upoważnionych do reprezentowania Wykonawcy

Załącznik nr 5 do SIWZ
Lista lokalizacji

Postępowanie nr PN-

Dotyczy: postępowania o udzielenie zamówienia publicznego prowadzonego w trybie przetargu nieograniczonego na „Dostawa urządzeń peryferyjnych i komputerów dla Centrum Onkologii – Instytut Marii Skłodowskiej Curie" realizowanym w ramach RPMA.02.01.01-14-2641/15-00"

CENTRUM ONKOLOGII-INSTYTUT IM. MARII SKŁODOWSKIEJ-CURIE
Ul. WK. Roentgena 5, 02-781 Warszawa

SAMODZIELNY ZAKŁAD OPIEKI ZDROWOTNEJ W KAŁUSZYNIE
ul. Wojska polskiego 24, 05-310 Kałuszyn

SAMODZIELNY PUBLICZNY ZAKŁAD OPIEKI ZDROWOTNEJ W CEGŁOWIE
ul. Pl. Anny Jagiellonki 13, 05-319 Cegłów

SAMODZIELNY PUBLICZNY ZAKŁAD OPIEKI ZDROWOTNEJ W SOKOŁOWIE PODLASKIM
ul. Ks. Bosco 5, 08-300 Sokołów Podlaski

Ośrodki Zdrowia w strukturze SPZOZ w Sokołowie Podlaskim:

- GMINNY OŚRODEK ZDROWIA W REPKACH
  ul. Parkowa 2 , 08-307 Repki

  WIEJSKI OŚRODEK ZDROWIA W SKIBNIEWIE
  08-300 Sokołów Podlaski

- WIEJSKI OŚRODEK ZDROWIA W WYROZĘBACH
  Wyrozęby Podawce 23A , 08-307 Repki

- WIEJSKI OŚRODEK ZDROWIA W CZERWONCE
  08-300 Sokołów Podlaski

Załącznik nr 6 do SIWZ, nr sprawy PN-135/18/MS/ZS
wzór umowy

WZÓR UMOWY

UMOWA NR ...../

zawarta w dniu .....pomiędzy

Centrum Onkologii - Instytutem im. Marii Skłodowskiej – Curie z siedzibą w Warszawie, ul. Wawelska 15B, 02-034 Warszawa, wpisanym do Rejestru Przedsiębiorców Krajowego Rejestru Sądowego prowadzonego przez Sąd Rejonowy dla m.st. Warszawy w Warszawie, XIII Wydział Gospodarczy Krajowego Rejestru Sądowego pod nr KRS 0000144803, Regon 000288366, NIP 525-000-80-57, zwanym dalej „Zamawiającym" w imieniu którego działa:

……

a

.....

wpisanym do Krajowego Rejestru Sądowego, prowadzonego przez ....., pod nr KRS ....., Regon ....., NIP ..... o kapitale zakładowym …… lub do Centralnej Ewidencji i Informacji o Działalności Gospodarczej RP, zwanym dalej Wykonawcą, wybranym w trybie przetargu nieograniczonego na dostawę urządzeń peryferyjnych i komputerów dla Centrum Onkologii – Instytut im. Marii Skłodowskiej-Curie dla projektu: „Nowoczesny Szpital, Nowoczesny ZOZ" realizowanego w ramach RPMA.02.01.01-14-2641/15-00" , nr sprawy PN – 135/18/MS/ZS/UE, na podstawie art. 39 ustawy z dnia 29.01.2004 r. Prawo zamówień publicznych (Dz. U. z 2017 r., poz. 1579), w imieniu którego działają:

1. .....
2. .....

zwanymi dalej łącznie „Stronami"

§ 1

Przedmiot Umowy

1. Przedmiotem umowy jest sprzedaż i dostawa przez Wykonawcę na rzecz Zamawiającego następującego sprzętu i oprogramowania (zwanego dalej Sprzętem IT):
   a. zestawy komputerowe wraz z oprogramowaniem biurowym;
   b. urządzenia wielofunkcyjne;
   c. Web Application Firewall – Centrum Danych;
   d. Database Firewall – Centrum Danych;
   e. Firewall – Centrum Danych – Centrum Danych;
   f. Firewall – Centrum Onkologii

   w ilości i zgodnie z charakterystyką określoną w Opisie Przedmiotu Zamówienia stanowiącą załącznik nr 1 do umowy „*Opis Przedmiotu Zamówienia*" oraz ofertą Wykonawcy stanowiącą załącznik nr 2 do umowy „*Oferta Wykonawcy*".
2. Wykonawca zobowiązany jest do dostarczenia Przedmiotu Umowy do siedziby Zamawiającego oraz we wskazane przez Zamawiającego lokalizacje, na własny koszt, w terminach wskazanym w § 3 umowy. Wykaz lokalizacji zawiera załącznik nr 3 do umowy.
3. W zakres Przedmiotu Umowy wchodzi również instalacja i konfiguracja Przedmiotu Umowy określonego w ust. 1 pkt. c-f w terminie wskazanym w § 3 umowy.
4. W ramach umowy Wykonawca zapewni Zamawiającemu bezterminowe prawo do korzystania z oprogramowania, stanowiącego Przedmiot Umowy, na warunkach niezbędnych do korzystania z Przedmiotu Umowy. W przypadku, jeżeli producent oprogramowania wchodzącego w skład Przedmiotu Umowy, wystawi dla oprogramowania dokument licencyjny lub oprogramowanie, które wymagać będzie odrębnego licencjonowania, Wykonawca zobowiązany jest dostarczyć Zamawiającemu niezbędny w zakresie potwierdzenia praw do korzystania z oprogramowania dokument licencyjny w terminie dostarczenia Przedmiotu Umowy, wskazanym w § 3 ust.1 .Udzielone licencje będą nieograniczone czasowo i terytorialnie.

§ 2

Obowiązki Wykonawcy

1. Wykonawca oświadcza, że posiada konieczne doświadczenie i kwalifikacje niezbędne do prawidłowego wykonania umowy i zobowiązuje się przy wykonaniu umowy do zachowania należytej staranności uwzględniającej zawodowy charakter prowadzonej działalności.
2. Wykonawca oświadcza, że Przedmiot Umowy jest fabrycznie nowy, oryginalny, wolny od wad fizycznych i prawnych, zgodnych z wymaganiami techniczno-ilościowymi określonymi w Opisie Przedmiotu Zamówienia. Wykonawca dostarczy wraz z Przedmiotem Umowy wszelkie dokumenty, licencje, certyfikaty, karty gwarancyjne czy dokumenty umożliwiające dostęp do najnowszych sterowników niezbędne do korzystania z Przedmiotu Umowy zgodnie z Opisem Przedmiotu Zamówienia. Wykonawca gwarantuje, że Przedmiot Umowy jest zgodny z polskimi normami bezpieczeństwa.
3. Wykonawca oświadcza, że:

1) dysponuje odpowiednim potencjałem techniczno-organizacyjnym, posiada wiedzę i doświadczenie pozwalające na należyte wykonanie umowy;
2) przysługują mu wszelkie niezbędne prawa do wykonywania umowy;
3) korzystanie przez niego oraz przez Zamawiającego ze Sprzętu IT będącego Przedmiotem Umowy nie narusza przepisów prawa, prawem chronionych dóbr osobistych lub praw majątkowych osób trzecich ani też praw na dobrach niematerialnych, w szczególności praw autorskich, praw pokrewnych, praw z rejestracji wzorów przemysłowych oraz praw ochronnych na znaki towarowe. Wykonanie umowy nie będzie prowadzić do wypełniania przesłanek czynu nieuczciwej konkurencji, w szczególności nie stanowi naruszenia tajemnicy przedsiębiorstwa osoby trzeciej.

§3

Terminy i odbiory

1. Dostarczenie Przedmiotu Umowy do siedziby Zamawiającego oraz do poszczególnych lokalizacji (wykaz lokalizacji zawiera załącznik nr 3 do umowy) nastąpi nie później niż w terminie do 45 dni od daty zawarcia umowy. Zamawiający dopuszcza dostawę Przedmiotu Umowy w partiach, pod warunkiem dotrzymania terminu dostawy określonego powyżej. Instalacja Sprzętu IT wymienionego w § 1 ust 1 pkt. c-f nastąpi nie później niż 70 dni od daty zawarcia umowy.
2. Odbiór Przedmiotu Umowy zarówno w siedzibie Zamawiającego jak i w lokalizacjach odbędzie się zgodnie z ust. 3-9 i zostanie każdorazowo potwierdzony, podpisanym bez zastrzeżeń, przez umocowanych przedstawicieli Stron, *Protokołem odbioru Sprzętu IT*, którego wzór stanowi załącznik nr 4 do umowy.
3. Wykonawca powiadomi, w formie pisemnej, Zamawiającego o terminie dostarczenia Przedmiotu Umowy z wyprzedzeniem co najmniej 3-ch dni roboczych, wskazując również w powiadomieniu przewidywany dzień i godzinę dostawy. Zamawiający w terminie do 2-ch dni roboczych potwierdzi wskazany termin lub wskaże inny, jednak nie późniejszy niż 7 dni roboczych od daty otrzymania od Wykonawcy ww. powiadomienia. Odbiór Przedmiotu Umowy zostanie dokonany z udziałem upoważnionych przedstawicieli Wykonawcy i Zamawiającego.
4. Do współpracy i koordynacji realizacji Przedmiotu Umowy, w tym do podpisania Protokołu Odbioru Sprzętu IT, Protokołu Instalacji Sprzętu IT, upoważnione są osoby ze strony Wykonawcy:

   1) …, tel. …, e-mail: …
   lub
   2) …, tel. …, e-mail: …

   Do współpracy i koordynacji realizacji przedmiotu Umowy, w tym do podpisania Protokołu Odbioru Sprzętu IT, Protokołu Instalacji Sprzętu IT, upoważnione są osoby ze strony Zamawiającego:

   1) …, tel. …, e-mail: …
   lub
   2) …, tel. …, e-mail: …

   Korespondencja związana z wykonywaniem umowy będzie dostarczana osobiście lub pocztą tradycyjną lub pocztą elektroniczną na adres:

   1) do Zamawiającego: ……..
   2) do Wykonawcy: ……..

5. Zmiana osób lub danych, o których mowa w ust. 4 nie stanowi zmiany umowy. Zmiana taka staje się skuteczna z chwilą pisemnego poinformowania drugiej Strony o dokonanej zmianie.
6. W trakcie odbioru Wykonawca w obecności Zamawiającego:
   1) rozpakuje dostarczony Sprzęt IT i sprawdzi czy nie nosi on znamion uszkodzeń mechanicznych oraz czy jest fabrycznie nowy,
   2) podłączy Sprzęt IT do sieci zasilającej oraz uruchomi Sprzęt IT,
   3) oraz w przypadku zgody Zamawiającego usunie i zutylizuje wszelkie opakowania, pozostałe po dostarczeniu Sprzętu IT.
7. Odbiór Przedmiotu Umowy potwierdzony zostanie podpisaniem Protokołem Odbioru Sprzętu IT pod warunkiem, iż Zamawiający nie wniesie żadnych zastrzeżeń.
8. Zamawiający, bez jakichkolwiek roszczeń finansowych ze strony Wykonawcy, może odmówić odbioru Przedmiotu Umowy w całości albo w części w przypadku stwierdzenia wad Przedmiotu Umowy, w szczególności:
   1) niezgodności z załącznikiem nr 1 do umowy,
   2) śladami zewnętrznego uszkodzenia Przedmiotu Umowy ;
   3) nieprawidłowym funkcjonowaniem po podłączeniu do sieci zasilającej
   4) brakiem wymaganych dokumentów, o których mowa w §2 ust. 2.
9. W przypadku skorzystania przez Zamawiającego z prawa odmowy odbioru, o którym mowa w ust. 8, Wykonawca jest zobowiązany do dostarczenia Przedmiotu Umowy zgodnego z umową w terminie granicznym do 45 dni daty zawarcia umowy.
10. W przypadku niedostarczenia Przedmiotu Umowy zgodnego z umową w terminie, o którym mowa w ust. 9, Zamawiającemu przysługuje prawo do odstąpienia od umowy albo jej części w terminie 30 dni od dnia powzięcia informacji o wystąpieniu tej przesłanki, jednak nie później niż w terminie 60 dni od terminu określonego w § 3 ust. 1 umowy.

§ 4

Gwarancja i rękojmia

1. W ramach wynagrodzenia, o którym mowa w § 5 ust. 1 umowy, Wykonawca udziela Zamawiającemu gwarancji na dostarczony Przedmiot Umowy na okres …..... miesięcy od dnia podpisania bez zastrzeżeń Protokołu Odbioru Sprzętu IT (załącznik nr 4 do umowy) w zakresie Przedmiotu Umowy określonego w § 1 ust. 1 pkt. a-b oraz na okres ……. miesięcy od dnia podpisania bez zastrzeżeń Protokołu Instalacji (załącznik nr 5 do umowy) w zakresie Przedmiotu Umowy określonego w § 1 ust. 1 pkt. c-f . W ramach gwarancji Zamawiający będzie miał prawo do aktualizacji wersji oprogramowania będącego integralną częścią Sprzętu IT (updates, upgrade, patches) oraz do nowych wersji oprogramowania i udoskonaleń do wersji bieżących oprogramowania (nowych edycji oprogramowania, wydań uzupełniających, poprawek programistycznych). Zamawiający, w ramach wynagrodzenia, o którym mowa w § 5 ust. 1 Umowy, uzyskuje prawo do zainstalowania, uruchamiania, przechowywania i nieograniczonego w czasie korzystania z aktualizacji.

2. W przypadku ujawnienia w okresie gwarancji wad w dostarczonym Przedmiocie Umowy, Wykonawca zobowiązuje się, na własny koszt i ryzyko, do ich naprawy lub wymiany na nowe, wolne od wad w terminach wskazanych w *Warunkach Gwarancji* (stanowiących załącznik nr 6 do umowy) od dnia zgłoszenia przez Zamawiającego tego faktu, z zastrzeżeniem, że naprawy odbywać się będą w dni robocze, jeśli Wykonawca będzie je realizował w siedzibie Zamawiającego lub w lokalizacjach wyszczególnionych w załączniku nr 3 do umowy. W przypadku naprawy trwającej dłużej niż terminy określone w Warunkach Gwarancji Wykonawca zobowiązany jest do dostarczenia na swój koszt zastępczego Sprzętu IT
3. Zgłoszenia będą przyjmowane przez Wykonawcę:
   Na adres poczty elektronicznej: ……
   Telefonicznie pod numerem: ……..
   Przez internetowy system zgłoszeń ……
4. O każdej zmianie adresu lub numerów telefonów i faksów wskazanych powyżej, Wykonawca zobowiązany jest niezwłocznie powiadomić na piśmie Zamawiającego. Zmiana danych nie wymaga zmiany umowy w formie pisemnego aneksu.
5. W ramach wynagrodzenia, o którym mowa w § 5 ust. 1, w okresie trwania gwarancji, Wykonawca zapewni udzielanie pomocy technicznej w zakresie obsługi Przedmiotu Umowy. Czynności związane ze świadczeniem przez Wykonawcę gwarancji będą dokonywane w języku polskim, tj. zgłoszenia, konsultacje itp.
6. Zakres gwarancji obejmuje następujące czynności:
   1) diagnozę uszkodzeń;
   2) wymianę uszkodzonych części;
   3) naprawę i transport części z serwisu do siedziby Zamawiającego lub lokalizacji wskazanych w załączniku nr 3 do umowy;
   4) dostarczenie zastępczego Sprzętu IT na czas naprawy o parametrach nie gorszych niż naprawiany Sprzęt IT.
7. W okresie gwarancji wszystkie koszty związane z dojazdem oraz przewozem Przedmiotu Umowy do lub z serwisu pokrywa Wykonawca.
8. Gwarancji podlegają wady materiałowe i konstrukcyjne, a także nie spełnianie deklarowanych przez producenta funkcji użytkowych w dostarczonym Przedmiocie Umowy.
9. Fakt awarii, naprawy i ewentualnej wymiany Przedmiotu Umowy na nowy będzie odnotowywany każdorazowo w Protokole Gwarancyjnym stanowiącym załącznik nr 7 do umowy *„Protokół Gwarancyjny”.*
11. W przypadku wystąpienia drugiej takiej samej wady w danym Przedmiocie Umowy, Wykonawca na żądanie Zamawiającego zobowiązuje się do wymiany Przedmiotu Umowy, w którym ujawniły się wady, na nowe, wolne od wad, w terminie 10 dni roboczych od dnia zgłoszenia przez Zamawiającego takiego żądania.
12. W przypadku stwierdzenia wady uniemożliwiającej prawidłowe użytkowanie Przedmiotu Umowy w okresie gwarancji Wykonawca gwarantuje wymianę wadliwego Przedmiotu Umowy na wolny od wad, o takich samych funkcjach użytkowych w terminie 10 dni roboczych od dnia zgłoszenia przez Zamawiającego takiego żądania.

13. Jeśli w wykonaniu swoich obowiązków Wykonawca dostarczył Zamawiającego zamiast wadliwego Przedmiotu Umowy, Przedmiot Umowy nowy, wolny od wad lub dokonał istotnej naprawy Przedmiotu Umowy objętego gwarancją, termin gwarancji biegnie od nowa od dnia dostarczenia wymienionego Przedmiotu Umowy lub zwrócenia Przedmiotu Umowy naprawionego.
14. W przypadku awarii dysku twardego lub innego nośnika danych, Przedmiot Umowy będzie wymieniony przez Wykonawcę na nowy wolny od wad.
16. Zamawiający może wykonywać uprawnienia z tytułu rękojmi za wady fizyczne Przedmiotu Umowy niezależnie od uprawnień wynikających z gwarancji. Wykonanie uprawnień z gwarancji nie wpływa na odpowiedzialność Wykonawcy z tytułu rękojmi.
17. Postanowienia określone w niniejszym paragrafie stanowią dokument gwarancyjny dla gwarancji Wykonawcy w rozumieniu art. 577^2 Kodeksu Cywilnego.

§ 5
Wynagrodzenie

1. Z tytułu należytego i terminowego wykonania Przedmiotu Umowy, Wykonawca otrzyma łączne wynagrodzenie, w kwocie brutto (w tym podatek VAT) …….. **zł** (słownie złotych: …….. zł.).
2. Wynagrodzenie, o którym mowa w ust. 1 obejmuje wszelkie koszty związane z realizacją Przedmiotu Umowy opisanym w Opisie Przedmiotu Zamówienia stanowiącym załącznik nr 1 do umowy, w tym m.in. koszty udzielenia licencji, koszty i opłaty związane z wydaniem dokumentacji niezbędnej do normalnego użytkowania Przedmiotu Umowy oraz świadczenie usług serwisu gwarancyjnego na zasadach określonych w Umowie. Wynagrodzenie wyczerpuje wszelkie należności Zamawiającego wobec Wykonawcy związane z realizacją Umowy. Wykonawcy nie przysługuje zwrot od Zamawiającego jakichkolwiek dodatkowych kosztów, opłat i podatków poniesionych przez Wykonawcę w związku z realizacją Umowy.
3. Wynagrodzenie, o którym mowa w ust. 1 płatne będzie w dwóch częściach, tj.:
    a. 70% wynagrodzenia, w kwocie …… **zł** (słownie: ……..zł) brutto, zostanie wypłacone Wykonawcy po dokonaniu odbioru Przedmiotu Umowy w zakresie dostawy Sprzętu IT określonego w § 1 ust. 1 pkt. a-f – bez zastrzeżeń na podstawie podpisanego przez Strony Protokołu Odbioru Sprzętu IT;
    b. 30% wynagrodzenia, w kwocie …….. **zł** (słownie: …….. zł) brutto, zostanie wypłacone Wykonawcy po dokonaniu instalacji Sprzętu IT określonego w § 1 ust. 1 pkt. c-f – bez zastrzeżeń na podstawie podpisanego przez Strony Protokołu Instalacji;
4. Zapłata nastąpi przelewem na rachunek bankowy Wykonawcy nr …… podany na fakturze, w terminie 30 dni licząc od daty dostarczenia prawidłowo wystawionej faktury, z zastrzeżeniem ust. 7.
5. Za dzień otrzymania faktury przyjmuje się datę jej dostarczenia wraz z właściwym Protokołem Odbioru/Protokołem Instalacji do: Kancelarii Zamawiającego w Warszawie przy ul. W.K. Roentgena 5 lub do Działu Księgowości Zamawiającego w Warszawie przy ul. Wawelskiej 15B.
6. Za datę otrzymania zapłaty strony przyjmują datę obciążenia rachunku bankowego Zamawiającego.
7. Wynagrodzenie płatne jest ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach osi priorytetowej II „Wzrost e-potencjału na Mazowszu”, działanie 2.1 „e-usługi”, poddziałania 2.1.1 „e-usługi dla Mazowsza” Regionalnego Programu Operacyjnego Województwa Mazowieckiego na lata 2014 – 2020 w ramach

umowy nr UDA-RPMA.02.01.01-14-2641/15-00 zawartej z Województwem Mazowieckim. W przypadku niezawinionego przez Zamawiającego opóźnienia przekazania środków przez Instytucję Pośredniczącą, Wykonawca nie będzie domagał się zapłaty odsetek pod warunkiem, że Zamawiający pisemnie poinformuje Wykonawcę o przyczynie opóźnienia i przewidywanym terminie zapłaty

§ 6

Kary umowne i roszczenia odszkodowawcze

1. W przypadku, gdy Wykonawca nie dochowa terminów dostawy i instalacji Przedmiotu Umowy określonych w § 3 ust. 1 Zamawiający zastrzega sobie prawo obciążenia Wykonawcy karami umownymi w wysokości 0,5% wartości całkowitego wynagrodzenia brutto, o którym mowa w § 5 ust. 1, za każdy rozpoczęty dzień opóźnienia.
2. W przypadku, gdy Wykonawca nie dochowa terminów określonych § 4 ust. 2, 10, 11 lub 12 Zamawiający zastrzega sobie prawo obciążenia Wykonawcy karami umownymi w wysokości 0,1% wartości całkowitego wynagrodzenia brutto, o którym mowa w § 5 ust. 1, za każdy rozpoczęty dzień opóźnienia.
3. W przypadku, gdy odstąpienie od Umowy w całości nastąpi z przyczyn leżących po stronie Wykonawcy, Zamawiający zastrzega sobie prawo obciążenia Wykonawcy karami umownymi w wysokości 20% wartości całkowitego wynagrodzenia brutto, o którym mowa w § 5 ust.1 Umowy.
4. W przypadku, gdy odstąpienie od Umowy w części, nastąpi z przyczyn leżących po stronie Wykonawcy, Zamawiający zastrzega sobie prawo obciążenia Wykonawcy karami umownymi w wysokości 20% wartości Umowy, której dotyczy odstąpienie.
5. Kary umowne będą potrącane w pierwszej kolejności z wynagrodzenia należnego Wykonawcy, na co Wykonawca wyraża zgodę i do czego upoważnia Zamawiającego bez potrzeby uzyskania pisemnego potwierdzenia.
6. Kary umowne za opóźnienie podlegają stosownemu łączeniu.
7. Kary umowne określone w niniejszym paragrafie mogą być dochodzone niezależnie od siebie.
8. Zamawiający zastrzega sobie możliwość dochodzenia na zasadach ogólnych odszkodowania przewyższającego ustalone kary umowne.

§ 7

Wady prawne

1. Wykonawca gwarantuje, że Sprzęt IT nie narusza ani innych praw osób trzecich.
2. W przypadku wystąpienia osób trzecich wobec Zamawiającego z roszczeniami opartymi na twierdzeniu, iż używany przez Zamawiającego Sprzęt IT narusza jakiekolwiek prawa, o których mowa w ust. 1, Zamawiającemu przysługują wszystkie niżej wymienione uprawnienia, które ma prawo zrealizować według swojego wyboru (łącznie lub osobno):
   1) prawo odstąpienia od umowy w terminie 30 dni od powzięcia wiadomości o powyższych okolicznościach z wyłączeniem zapłaty na rzecz Wykonawcy jakichkolwiek kosztów, odszkodowań itp.,
   2) prawo żądania zapłaty przez Wykonawcę kary umownej w wysokości 20 % łącznego wynagrodzenia brutto określonego w § 5 ust. 1 umowy oraz prawo żądania odszkodowania uzupełniającego na zasadach ogólnych Kodeksu cywilnego.

3. W przypadku wytoczenia przeciwko Zamawiającemu powództwa opartego na twierdzeniu opisanym w ust. 2, Wykonawca zobowiązuje się zapewnić Zamawiającemu na swój koszt ochronę prawną oraz ponieść konsekwencje zapadłego wyroku sądowego.

§ 8

Zabezpieczenie należytego wykonania Umowy

1. Wykonawca udzieli Zamawiającemu zabezpieczenia należytego wykonania Umowy w formie ……. w wysokości …….. zł (słownie złotych: ...), tj. 10% wartości całkowitego wynagrodzenia z podatkiem VAT, o którym jest mowa w § 5 ust. 1 Umowy.
2. W przypadku wniesienia zabezpieczenia w pieniądzu, Wykonawca zobowiązany jest do złożenia pisemnego wniosku o zwrot zabezpieczenia ze wskazaniem numeru rachunku bankowego, na który należy dokonać zwrotu.
3. Wykonawca może zmienić formę zabezpieczenia należytego wykonania Umowy na jedną lub kilka form, o których mowa w art. 148 ust. 1 ustawy Prawo zamówień publicznych. Za zgodą Zamawiającego Wykonawca może zmienić formę zabezpieczenia w zakresie określonym w art.148 ust. 2 Ustawy.
4. Zabezpieczenie należytego wykonania Umowy, o którym mowa w ust. 1, z zastrzeżeniem ust. 5 i 6 zostanie zwolnione:
   1) w wysokości 70% kwoty zabezpieczenia – w terminie 30 dni od daty podpisania przez Strony Protokołu Odbioru wnioskującego o rozliczenie finansowe;
   2) w wysokości 30% kwoty zabezpieczenia – w ciągu 15 dni od upływu okresu rękojmi za wady.
5. Zabezpieczenie należytego wykonania Umowy służy do pokrycia roszczeń Zamawiającego z tytułu niewykonania lub nienależytego wykonania Umowy, w tym potrąceń kar umownych bez potrzeby uzyskania akceptacji Wykonawcy.
6. Wykonawca oświadcza, że wyraża zgodę na bezpośrednie potrącenie przez Zamawiającego z zabezpieczenia należytego wykonania Umowy, wszelkich należności powstałych w wyniku niewykonania lub nienależytego wykonania Umowy, a w szczególności kar umownych.
7. Potwierdzenia wpłaty wniesionego zabezpieczenia należytego wykonania umowy stanowi załącznik nr 8 do Umowy.

§ 9

Odstąpienie od Umowy

1. Zamawiający może odstąpić od umowy w przypadkach wskazanych w umowie lub określonych w przepisach obowiązującego prawa, w szczególności Kodeksu cywilnego.
2. W razie zaistnienia istotnej zmiany okoliczności powodującej, że wykonanie umowy nie leży w interesie publicznym, czego nie można było przewidzieć w chwili zawarcia umowy lub powzięcia informacji o nieotrzymaniu środków budżetowych koniecznych do realizacji umowy od dysponenta odpowiedniego stopnia, Zamawiający może odstąpić od umowy albo jej części w terminie 30 dni od powzięcia wiadomości o tych okolicznościach jednak nie później niż w terminie 60 dni od terminu określonego w § 3 ust. 1 umowy. W przypadku odstąpienia od umowy, Wykonawcy przysługiwało będzie jedynie wynagrodzenie za zrealizowaną część umowy.

3. Opóźnienie w dostawie powyżej 30 dni od ostatecznego terminu, o którym mowa w § 3 ust. 1 umowy, na dostarczenie Przedmiotu Umowy uprawnia Zamawiającego do odstąpienia od umowy albo jej części w terminie 30 dni od daty powzięcia okoliczności uzasadniających prawo odstąpienia jednak nie później niż w terminie 60 dni od terminu określonego w § 3 ust. 1 umowy.
4. Każda ze Stron ma prawo odstąpienia od umowy albo jej części w wypadku zaistnienia przeszkód wynikających z siły wyższej uniemożliwiających realizację umowy. Przez siłę wyższą należy rozumieć zdarzenie nadzwyczajne, zewnętrzne, niemożliwe do przewidzenia i przeciwdziałania, którego wystąpienie jest niezależne od Stron, a które uniemożliwia wykonanie zobowiązań wynikających z umowy.
5. Zamawiający może odstąpić od umowy albo jej części w przypadkach naruszenia postanowień umowy przez Wykonawcę oraz gdy Wykonawca nie wykonuje lub nienależycie wykonuje umowę, w szczególności nie przestrzega ustalonych terminów lub narusza inne postanowienia umowy oraz po bezskutecznym upływie terminu wskazanego przez Zamawiającego w wezwaniu do zaniechania przez Wykonawcę naruszeń postanowień umowy i usunięcia ewentualnych skutków naruszeń, Wykonawca nie zastosuje się do wezwania.
6. Odstąpienie od Umowy wymaga formy pisemnej pod rygorem nieważności.

§ 10

Zmiany Umowy

1. Zamawiający przewiduje możliwość zmian istotnych postanowień zawartej umowy w stosunku do treści oferty, na podstawie, której dokonano wyboru Wykonawcy, w następujących przypadkach:

1) zmiany powszechnie obowiązujących przepisów prawa w zakresie mającym wpływ na realizację umowy;
2) w zakresie Przedmiotu Umowy, co do terminu realizacji, jeżeli zaszły okoliczności, których nie można było przewidzieć w chwili zawarcia umowy;
3) zmiany postanowień umowy w sytuacji, gdy dotyczy ona zmiany producenta, modelu Przedmiotu Umowy, w szczególności w przypadku zakończenia jego produkcji lub wycofania go z produkcji lub braku jego dostępności na rynku europejskim, z tym, że cena wskazana w ofercie nie może ulec podwyższeniu, a parametry techniczne Przedmiotu Umowy nie mogą być gorsze niż wskazane w Opisie Przedmiotu Zamówienia;
4) zmiany terminu realizacji umowy, jeżeli wystąpią okoliczności, których nie można było przewidzieć w momencie zawierania umowy, a które uniemożliwiłyby wykonanie Umowy zgodnie z jej treścią i celem.

2. O ile umowa nie stanowi inaczej wszelkie zmiany i uzupełnienia umowy wymagają zachowania formy pisemnej pod rygorem nieważności.
3. Każda ze Stron może jednostronnie dokonać zmian w zakresie danych teleadresowych, osób upoważnionych do kontaktu, zawiadamiając niezwłocznie o tym na piśmie drugą Stronę. Zmiany w tym zakresie nie stanowią zmiany Umowy w rozumieniu art. 144 Prawa zamówień publicznych.

§ 11

Cesja i poufność

1. Wykonawca nie może przenieść praw i obowiązków wynikających z niniejszej umowy na osoby trzecie, bez uprzedniej pisemnej zgody Zamawiającego, w szczególności na podstawie umowy przelewu wierzytelności, umowy poręczenia, umowy zastawu ani żadnej innej podobnej umowy, wskutek której dochodzi do przeniesienia praw i obowiązków Wykonawcy na osobę trzecią, w tym do zarządzania i administrowania wierzytelnością Wykonawcy.
2. Czynność dokonana z naruszeniem ust. 1 jest nieważna.
3. Strony zobowiązują się do nie ujawniania, nie publikowania, nie przekazywania, nie udostępniania w żaden inny sposób osobom trzecim jakichkolwiek danych o transakcjach stron, jak również:

a) informacji dotyczących, podejmowania przez każdą ze stron czynności w toku realizacji niniejszej umowy,
b) informacji zastrzeżonych jako tajemnice stron w rozumieniu Ustawy z dnia z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji,
c) innych informacji prawnie chronionych, które uzyskają w związku z realizacją niniejszej umowy, bez względu na sposób i formę ich utrwalenia lub przekazania- o ile informacje nie są powszechnie znane, bądź obowiązek ich ujawnienia nie wynika z obowiązujących przepisów prawa.

4. Obowiązkiem zachowania poufności nie jest objęty fakt zawarcia umowy ani jej treść w zakresie określonym obowiązującymi przepisami prawa.
5. Każda ze stron może ujawnić informacje poufne z ograniczeniami wynikającymi z przepisów prawa - członkom swoich władz, kancelariom prawnym, firmom audytorskim, pracownikom organów nadzoru, w takim zakresie w jakim będzie to niezbędne do wypełnienia przez nią zobowiązań wynikających z innej ustawy.
6. Każda ze Stron zobowiązuje się do ochrony informacji poufnych, udostępnionych przez drugą stronę w celu prowadzenia działań wynikających z niniejszej umowy i nie wykorzystywania ich przeciwko interesom drugiej strony.
7. Warunki przetwarzania danych osobowych z baz Zamawiającego określone zostaną w odrębnej umowie powierzenia przetwarzania danych osobowych.
8. W celu prawidłowego wykonania przez Wykonawcę obowiązków wynikających z niniejszej Umowy i wyłącznie w zakresie niezbędnym dla wykonania przez Wykonawcę takich obowiązków, Wykonawca zobowiązuje się do przetwarzania danych osobowych zgodnie z przepisami prawa powszechnie obowiązującego. Wykonywanie przez Wykonawcę operacji przetwarzania danych w zakresie lub w celu przekraczającym zakres i cel opisane powyżej wymaga każdorazowej pisemnej zgody Zamawiającego.
9. Wykonawca zobowiązuje się zapoznać osoby przy udziale których wykonuje obowiązki umowne z postanowieniami umowy dotyczącymi ochrony poufnych informacji, oraz zobowiązać je do ich stosowania, a także do zachowania w tajemnicy.

10. Zobowiązania określone w niniejszym paragrafie wiążą Strony w czasie obowiązywania niniejszej Umowy oraz po jej rozwiązaniu lub wygaśnięciu .
11. W przypadku ujawnienia informacji poufnej wbrew powyższym postanowieniom, Wykonawca ponosi odpowiedzialność odszkodowawczą za szkodę wyrządzoną Zamawiającemu wskutek ujawnienia informacji poufnej.

§ 12

Przetwarzanie danych osobowych i obowiązek informacyjny*

1. Administratorem danych osobowych osób działających w imieniu Wykonawcy, jego pracowników lub zleceniobiorców, w tym podwykonawców) jest Wykonawca a osób działających w imieniu Zamawiającego, jego pracowników lub zleceniobiorców – Zamawiający.
2. Dane kontaktowe do Inspektora Ochrony Danych Osobowych u Zamawiającego –adres e-mail: oid.@coi.pl, u Wykonawcy – adres: e-mail: …….. .
3. Każdy Administrator danych osobowych jest zobowiązany przetwarzać dane osobowe zgodnie z obowiązującymi przepisami prawa, w szczególności Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119, s.1) (RODO) oraz ustawy z dnia 10 maja 2018 r. – o ochronie danych osobowych (Dz. U. z 2018 r. poz. 1000)
4. Każdy Administrator danych osobowych jest zobowiązany posiadać prawo do powierzenia przetwarzania danych osobowych na potrzeby niniejszej umowy - przez cały okres jej realizacji oraz przez czas niezbędny do realizacji uprawnień każdej ze stron wynikających z tej umowy.

   Lub

   Każdy z Administratorów danych osobowych oświadcza, że posiada zgody osób, na powierzenie przetwarzania ich danych osobowych zamawiającemu/Wykonawcy na potrzeby niniejszej umowy - przez cały okres jej obowiązywania oraz przez czas niezbędny do realizacji uprawnień każdej ze stron wynikających z tej umowy.
5. Wykonawca i Zamawiający przetwarzać będą powierzone im do przetwarzania dane osobowe wyłącznie w związku i na potrzeby realizacji niniejszej umowy .
6. Postawa prawna przetwarzania danych osobowych- uzasadniony interes Zamawiającego lub uzasadniony interes Wykonawcy.
7. Powierzone przez Administratora dane osobowe nie są i nie będą udostępniane innym odbiorcom poza przypadkami, gdy taki obowiązek wynika z przepisów powszechnie obowiązującego prawa lub została na to wyrażona zgoda osoby, której dane dotyczą .
8. Każdy Administrator zobowiązany jest do zabezpieczenia za pomocą odpowiednich środków technicznych i organizacyjnych powierzonych Danych Osobowych przed ich utratą, udostępnieniem osobom nieupoważnionym, uszkodzeniem lub zniszczeniem, oraz nieuprawnionym zbieraniem, udostępnianiem, usuwaniem, zmianą, utrwaleniem, przechowywaniem lub opracowywaniem.
9. Każdy z Administrator jest zobowiązany do poinformowania osób, których dane przekazał na potrzeby wykonania niniejszej umowy o prawie dostępu do danych osobowych oraz prawie ich sprostowania, usunięcia, ograniczenia przetwarzania, prawie wniesienia sprzeciwu, o ile jest to zgodne z przepisami powszechnie obowiązującego prawa oraz o prawie do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych gdy uzna, iż przetwarzanie jego danych osobowych narusza przepisy powszechnie obowiązującego prawa.

10. Powierzone do przetwarzania przez Administratora dane osobowe będą przetwarzane w sposób zautomatyzowany w tym również w formie profilowania.

Obowiązek informacyjny*

1. Administratorem danych osobowych Wykonawcy, dalej zwanych „danymi osobowymi" jest Centrum Onkologii-Instytut im. Marii Skłodowskiej- Curie z siedzibą w Warszawie, dalej „Administrator" .
2. Dane osobowe przetwarzane będą przez Administratora jedynie w celu realizacji Umowy.
3. Dane osobowe nie są i nie będą udostępniane innym odbiorcom poza przypadkami, gdy taki obowiązek wynika z przepisów powszechnie obowiązującego prawa lub została na to wyrażona zgoda Wykonawcy.
4. Dane osobowe będą przechowywane przez okres obowiązywania Umowy oraz okres 5 lat od dnia wygaśnięcia lub rozwiązania Umowy, chyba że powszechnie obowiązujące przepisy prawa wymagają przechowywania danych osobowych przez czas dłuższy.
5. Wykonawca posiada prawo dostępu do danych osobowych oraz prawo żądania ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo wniesienia sprzeciwu, o ile jest to zgodne z przepisami powszechnie obowiązującego prawa.
6. Wykonawca ma prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych gdy uznają, iż przetwarzanie ich danych osobowych narusza przepisy powszechnie obowiązującego prawa.
7. Dane osobowe nie będą przetwarzane w sposób zautomatyzowany w tym również w formie.

§ 13

Postanowienia końcowe

1. W sprawach nie uregulowanych Umową stosuje się przepisy ustawy Prawo zamówień publicznych oraz Kodeksu Cywilnego.
2. Wszelkie spory mogące wyniknąć z niniejszej umowy Strony będą się starały rozwiązać polubownie. Jeżeli rozwiązanie polubowne nie będzie możliwe wszelkie spory wynikłe z niniejszej umowy podlegać będą rozstrzygnięciu sądu właściwego miejscowo dla siedziby Zamawiającego.
3. Wszelkie zmiany do niniejszej umowy mogą być wprowadzane jedynie w formie pisemnego Aneksu pod rygorem nieważności.
4. Niniejsza Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach po jednym dla każdej ze Stron.
5. Załączniki wymienione w Umowie stanowią jej integralną część:

1) Załącznik nr 1 - Opis Przedmiotu Zamówienia;
2) Załącznik nr 2 – Oferta Wykonawcy
3) Załącznik nr 3 - Wykaz Lokalizacji;
4) Załącznik nr 4 - WZÓR Protokołu Odbioru Sprzętu IT
5) Załącznik nr 5 – WZÓR Protokołu Instalacji
6) Załącznik nr 6 – Warunki Gwarancji
7) Załącznik nr 7 – WZÓR Protokołu Gwarancyjnego
8) Załącznik nr 8 – potwierdzenie wpłaty wniesionego zabezpieczenia należytego wykonania umowy
9) Załącznik nr 9 – umowa powierzenia przetwarzania danych osobowych

Wykonawca Zamawiający

Załącznik nr 1 do Umowy nr ……z dnia ……..

Specyfikacja Techniczna Sprzętu – Opis Przedmiotu Zamówienia

Załącznik nr 2 do Umowy nr ……z dnia ……

Oferta Wykonawcy

Załącznik nr 3 do Umowy nr ……z dnia ……

Wykaz lokalizacji

CENTRUM ONKOLOGII-INSTYTUT IM. MARII SKŁODOWSKIEJ-CURIE
Ul. WK. Roentgena 5, 02-781 Warszawa

SAMODZIELNY ZAKŁAD OPIEKI ZDROWOTNEJ W KAŁUSZYNIE
ul. Wojska polskiego 24, 05-310 Kałuszyn

SAMODZIELNY PUBLICZNY ZAKŁAD OPIEKI ZDROWOTNEJ W CEGŁOWIE
ul. Pl. Anny Jagiellonki 13, 05-319 Cegłów

SAMODZIELNY PUBLICZNY ZAKŁAD OPIEKI ZDROWOTNEJ W SOKOŁOWIE PODLASKIM

ul. Ks. Bosco 5, 08-300 Sokołów Podlaski

Ośrodki Zdrowia w strukturze SPZOZ w Sokołowie Podlaskim:

- GMINNY OŚRODEK ZDROWIA W REPKACH
  ul. Parkowa 2 , 08-307 Repki
- WIEJSKI OŚRODEK ZDROWIA W SKIBNIEWIE
  08-300 Sokołów Podlaski
- WIEJSKI OŚRODEK ZDROWIA W WYROZĘBACH
  Wyrozęby Podawce 23A , 08-307 Repki
- WIEJSKI OŚRODEK ZDROWIA W CZERWONCE
  08-300 Sokołów Podlaski

Załącznik nr 4 do Umowy nr …….z dnia ……

WZÓR protokołu odbioru Sprzętu IT

zgodnie z Umową nr ... ……...../…… zawartą w dniu …….

pomiędzy:

…….. („Zamawiający")

a

.....(„Wykonawca"),

Zamawiający potwierdza, że Wykonawca dostarczył Sprzęt IT do siedziby Zamawiającego/Lokalizacji * w poniższej specyfikacji:

Lp.	Nazwa sprzętu	Liczba szt.	Numer seryjny	Uwagi

Upoważnieni przedstawiciele Zamawiającego i Wykonawcy złożonymi pod niniejszym protokołem podpisami zgodnie oświadczają, że:

1. Dostarczony do siedziby Zamawiającego/ Lokalizacji* Sprzęt IT jest fabrycznie nowy i nie nosi śladów uszkodzeń zewnętrznych oraz uprzedniego używania.
2. Ilość i rodzaj dostarczonego do siedziby Zamawiającego/ Lokalizacji* Sprzętu IT jest zgodna z Umową (w tym z Załącznikiem nr 1 do Umowy).
3. Wraz ze Sprzętem IT do siedziby Zamawiającego/ Lokalizacji* dostarczono wymaganą dokumentację.

Wykonawca

Zamawiający

Załącznik nr 5 do Umowy nr …….z dnia ……

WZÓR Protokołu Instalacji

zgodnie z Umową nr ... ……../…… zawartą w dniu …….

pomiędzy:

…… („Zamawiający")

a

.....(„Wykonawca"),

Zamawiający potwierdza, że Wykonawca zainstalował Sprzęt IT w siedzibie Zamawiającego/Lokalizacji * o poniższej specyfikacji:

Lp.	Nazwa sprzętu	Liczba szt.	Numer seryjny	Uwagi

Upoważnieni przedstawiciele Zamawiającego i Wykonawcy złożonymi pod niniejszym protokołem podpisami zgodnie oświadczają, że instalacja Sprzętu IT w siedzibie Zamawiającego/ Lokalizacji* została przeprowadzona prawidłowo.

Wykonawca

Zamawiający

Załącznik nr 6 do Umowy nr …….z dnia …….

Warunki Gwarancji

Warunki Gwarancji i Serwisu dla urządzeń:

Web Application Firewall - Centrum Danych
Database Firewall - Centrum Danych
Firewall - Centrum Danych - Centrum Danych
Firewall - Centrum Onkologii

1. Urządzenia muszą być objęte rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w następnym dniu roboczym (tj. poniedziałek – piątek w godzinach 8:00 – 16:00) od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres 60 miesięcy. Udostępniony sprzęt zastępczy musi być dostarczony i zainstalowany w miejscu użytkowania.
2. W ramach serwisu producent musi zapewniać dostęp do aktualizacji oprogramowania dostarczonych urządzeń
3. Czas reakcji serwisu – 4 godziny
4. Czas naprawy sprzętu – 30 dni
5. Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie:

a) 24x7 przez dedykowany serwisowy moduł internetowy (zgłoszenia dokonane po godzinie 16:00 będą kwalifikowane jako zgłoszenie dokonane w następnym dniu roboczym)
b) 8x5 przez infolinię w języku polskim 8x5 (poniedziałek – piątek w godzinach 8:00 – 16:00)

6. Oferent winien przedłożyć oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej).

Warunki Gwarancji i Serwisu dla urządzeń:

Zestawy komputerowe oraz urządzenia wielofunkcyjne:
Typ 1 stacjonarne z systemem operacyjnym i pakietem biurowym
Typ 3 przenośne z systemem operacyjnym i pakietem biurowym
Urządzenia wielofunkcyjne typ 1
Urządzenia wielofunkcyjne typ 1
Urządzenia wielofunkcyjne typ 2

1. Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie:

- 24x7 przez dedykowany serwisowy moduł internetowy (zgłoszenia dokonane po godzinie 16:00 będą kwalifikowane jako zgłoszenie dokonane w następnym dniu roboczym)
- 8x5 przez infolinię w języku polskim 8x5 (poniedziałek – piątek w godzinach 8:00 – 16:00)

2. W ramach serwisu producent musi zapewniać dostęp do aktualizacji oprogramowania dostarczonych urządzeń

3. Czas reakcji serwisu – następny dzień roboczy

4. Czas naprawy sprzętu – 14 dni

5. Urządzenia muszą być objęte rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w ciągu następnych 3 dni roboczych (tj. poniedziałek – piątek w godzinach 8:00 – 16:00) od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta sprzętu lub autoryzowanego dystrybutora przez cały okres gwarancji Udostępniony sprzęt zastępczy musi być dostarczony i zainstalowany w miejscu użytkowania.

6. Oferent winien przedłożyć oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej).

Typ 2 stacjonarne z systemem operacyjnym i pakietem biurowym:

1. Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie:

- 24x7 przez dedykowany serwisowy moduł internetowy (zgłoszenia dokonane po godzinie 16:00 będą kwalifikowane jako zgłoszenie dokonane w następnym dniu roboczym)
- 8x5 przez infolinię w języku polskim 8x5 (poniedziałek – piątek w godzinach 8:00 – 16:00)

2. Czas reakcji serwisu – 4 godziny

3. Czas naprawy sprzętu – następny dzień roboczy. Naprawa realizowana w miejscu użytkowania.

4. W przypadku uszkodzenia dysków – dyski pozostają u Zamawiającego

5. Oferent winien przedłożyć oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej).

Załącznik nr 7 do Umowy nr …….z dnia …….

WZÓR Protokół Gwarancyjny nr ....

PROTOKÓŁ GWARANCYJNY NR ……..
Sporządzony w dniu .....
w związku ze zgłoszeniem reklamacji na podstawie Umowy nr ……/…/2018 z dnia .....
Imię i nazwisko przedstawiciela Zamawiającego .....
Dokładny adres: ……
……...
……..
Nr telefonu .....
Data nabycia Przedmiotu Umowy .....
Nazwa Przedmiotu Umowy .....
nr seryjny .....
Producent .....
Transport : Wykonawcy .....
Dokładny opis wad .....
Żądanie Zamawiającego co do sposobu załatwienia reklamacji .....
Data i podpis osoby składającej reklamację po stronie Zamawiającego: .....
Data i podpis osoby przyjmującej reklamację po stronie Wykonawcy: .....
Opinia pracownika / rzeczoznawcy Wykonawcy.....
Decyzja pracownika Wykonawcy .....

Wykonawca
(upoważniony przedstawiciel)

Zamawiający
(upoważniony przedstawiciel)

Załącznik nr 8 do Umowy nr …….z dnia …….

Zabezpieczenie należytego wykonania umowy

Załącznik nr 9 do Umowy nr …….z dnia …….

UMOWA POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

zawarta w dniu …… - ……..-…….. roku w Warszawie pomiędzy:

Centrum Onkologii - Instytutem im. Marii Skłodowskiej – Curie z siedzibą w Warszawie, adres: 02-034 Warszawa, ul. Wawelska 15 B, wpisanym do Rejestru Przedsiębiorców Krajowego Rejestru Sądowego prowadzonego przez Sąd Rejonowy dla m.st. Warszawy, XII Wydział Gospodarczy Krajowego Rejestru Sądowego pod nr KRS 0000144803, NIP 525-000-80-57, Regon 000288366, zwanym dalej „Administratorem”,

w imieniu którego działa, należycie umocowany:

……..

a

.....,

wpisaną/wpisanym do:

- Rejestru …….. Krajowego Rejestru Sądowego prowadzonego przez Sąd Rejonowy w……., ……. Wydział Gospodarczy Krajowego Rejestru Sądowego pod nr KRS ....., NIP ....., Regon ……. wysokość kapitału zakładowego …….. PLN*

……., prowadzącą/prowadzącym działalność gospodarczą pod firmą:……., adres prowadzenia działalności ……., wpisaną/wpisanym do Centralnej Ewidencji i Informacji o Działalności Gospodarczej, NIP ....., Regon .....*,

zwaną/zwanym dalej „Przetwarzającym”, w imieniu którego działa należycie umocowany:
.....
Zważywszy, że:

1. Strony zawarły umowę ……..(zwana dalej „Umowa Podstawowa”), w związku z wykonywaniem której Administrator powierzy Przetwarzającemu przetwarzanie danych osobowych w zakresie określonym Umową;

2. Celem Umowy jest ustalenie warunków, na jakich Przetwarzający wykonuje operacje przetwarzania danych osobowych w imieniu Administratora;
3. Strony, zawierając Umowę, dążą do takiego uregulowania zasad przetwarzania danych osobowych, aby odpowiadały one w pełni postanowieniom rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119, s.1) – dalej Rozporządzenie oraz innym przepisom powszechnie obowiązującym, w szczególności ustawie z dnia 10 maja 2018 r. o ochronie danych osobowych.

NINIEJSZYM STRONY POSTANOWIŁY, CO NASTĘPUJE:

§1.

W niniejszej Umowie poniższe wyrażenia otrzymują następujące znaczenia:

1. Przetwarzający – podmiot, któremu Administrator powierza przetwarzanie danych osobowych na mocy niniejszej umowy;
2. Administrator – Centrum Onkologii – Instytut im. Marii Skłodowskiej – Curie w Warszawie;
3. Dane Osobowe – dane osobowe w rozumieniu Rozporządzenia dotyczące pacjentów i pracowników, przekazywane przez Zamawiającego Wykonawcy do przetwarzania;
4. Przetwarzanie danych – jakiekolwiek operacje wykonywane na danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takie jak zbieranie, utrwalanie, organizowanie, przechowywanie, porządkowanie, adoptowanie lub modyfikowanie, pobieranie przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, ograniczanie, usuwanie lub niszczenie;
5. Rozporządzenie (RODO) - rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119, s.1);
6. Ustawa - ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2018 r. poz. 1000);
7. Podprzetwarzajacy – podmiot któremu Przetwarzający powierza dalsze przetwarzanie danych powierzonych do przetwarzania przez Administratora.
8. Umowa Podstawowa - Umowa Nr …… , zawarta w dniu ……2018 r. pomiędzy Administratorem a Przetwarzającym.

§ 2.

1. Przedmiotem umowy jest powierzenie Przetwarzającemu przez Administratora przetwarzania Danych Osobowych. Niniejsza umowa stanowi umowę powierzenia przetwarzania danych osobowych, o której mowa w art. 28 ust 3 Rozporządzenia.
2. Celem powierzenia jest:

1) dostawa, instalacja, uruchomienie ……..,
2) serwis ……;
3) serwis systemu……;

4) szkolenie pracowników Zamawiającego;

5) kontakt z wyznaczonymi pracownikami Zamawiającego jedynie w zakresie niezbędnym do realizacji Umowy Podstawowej;

6) ……..*

w zakresie niezbędnym do właściwej realizacji Umowy Podstawowej.

3. Przetwarzanie będzie wykonywane w okresie obowiązywania Umowy Podstawowej.

4. Przetwarzający zobowiązuje się do ich przetwarzania zgodnie z prawem i niniejszą umową.

§ 3.

1. Przetwarzanie danych osobowych będzie dotyczyć następujących kategorii osób:
   1) Pracownicy Administratora
   2) ……..
2. Zakres powierzonych danych:
   1) dane osobowe ……..:
      a) nazwisko i imię (imiona),
      b) datę urodzenia,
      c) oznaczenie płci,
      d) adres miejsca zamieszkania,
      e) numer PESEL, jeżeli został nadany, ……..,
   2) dane osobowe pacjentów – dane szczególnych kategorii:
      a) dane dotyczące zdrowia w rozumieniu art. 4 pkt 15 RODO, w tym informacje gromadzone w dokumentacji medycznej, informacje o stanie zdrowia, diagnozy, stosowane leczenie, opisy i wyniki badań (co obejmuje także zapisane w postaci cyfrowej filmy, badania obrazowe),
   3) dane pracowników Administratora:
      a) dane osobowe lekarzy lub innych osób uprawnionych do wystawiania zlecenia na badania (imię i nazwisko lekarza kierującego, tytuł zawodowy, uzyskane specjalizacje, numer prawa wykonywania zawodu),
      b) dane osób pobierających materiał do badań (imię i nazwisko, tytuł zawodowy, numer prawa wykonywania zawodu),
      c) dane pracowników upoważnionych do działania po stronie Administratora (imię i nazwisko, adres e-mail).
3. Zakres danych osobowych wymienionych w ust. 2 jest maksymalnym katalogiem danych, które mogą być przetwarzane w związku z realizacją Umowy. W rzeczywistości dane mogą być przekazywane przez Administratora w mniejszym zakresie bez uszczerbku dla postanowień niniejszej umowy. Zakres danych może ulec zmianie w przypadku zmiany aktualnie obowiązujących przepisów prawa.

§ 4

Przetwarzający:

1) nie decyduje o celach i środkach przetwarzania danych osobowych;
2) nie jest uprawniony do tworzenia jakichkolwiek zbiorów lub kopii danych osobowych, chyba że obowiązek taki wynika z Umowy Podstawowej lub obowiązujących przepisów prawa;
3) przetwarza dane wyłącznie na polecenie Administratora i w zakresie przez niego wskazanym.

§ 5

1. Przetwarzający zobowiązuje się do zabezpieczenia za pomocą odpowiednich środków technicznych i organizacyjnych określonych w art. 32 Rozporządzenia powierzonych Danych Osobowych przed ich utratą, udostępnieniem osobom nieupoważnionym, uszkodzeniem lub zniszczeniem, oraz nieuprawnionym zbieraniem, usuwaniem, zmianą, utrwaleniem, przechowywaniem lub opracowywaniem.
2. Dane Osobowe będą przetwarzane w budynkach należących do Administratora/poza budynkami Administratora.*
3. W ramach realizacji Umowy, w przypadku konieczności Przetwarzający jest uprawniony do zdalnego dostępu do systemów Administratora wyłącznie z zastosowaniem bezpiecznego, wydzielonego łącza VPN/…….(innego systemu bezpieczeństwa adekwatnego do przedmiotu umowy)*.
4. Przetwarzający oświadcza, że realizacja zdalnego dostępu do systemów Administratora odbywać się będzie wyłącznie z lokalizacji stanowiącej obszar przetwarzania danych Przetwarzającego, stanowiących pomieszczenia będące w posiadaniu Przetwarzającego. Zabroniona jest realizacja zdalnego dostępu z miejsc nie pozostających pod nadzorem fizycznym Przetwarzającego w szczególności z miejsc publicznie dostępnych.
5. Przetwarzający niezwłocznie będzie informował Administratora o dokonanych zmianach w zakresie zabezpieczeń technicznych i organizacyjnych wymaganych przepisami prawa, a także, na żądanie Administratora będzie mu niezwłocznie przekazywał informacje niezbędne do wypełnienia przez Administratora wymagań nałożonych przez Rozporządzenie.
6. Przetwarzający gwarantuje, że dostęp do przetwarzania powierzonych danych osobowych będą miały wyłącznie osoby przeszkolone w zakresie ochrony danych osobowych oraz posiadające pisemne upoważnienie do ich przetwarzania w zakresie objętym Umową Podstawową, wystawione przez Przetwarzającego.
7. Przetwarzający jest zobowiązany prowadzić ewidencję osób upoważnionych do przetwarzania Danych Osobowych.
8. Przetwarzający zobowiązuje się do dochowania szczególnej staranności, aby osoby, o których mowa w ust 6 zachowały powierzone do przetwarzania dane osobowe w tajemnicy, również po zakończeniu realizacji Umowy.
9. Przetwarzający oświadcza, że nie przekazuje Danych Osobowych do państwa trzeciego lub organizacji międzynarodowej (czyli poza Europejski Obszar Gospodarczy („EOG"). Przetwarzający oświadcza również, że nie korzysta z podwykonawców, którzy przekazują Dane osobowe poza EOG.
10. Jeżeli Przetwarzający ma zamiar lub obowiązek przekazywać Dane Osobowe poza EOG, informuje o tym Administratora, w celu umożliwienia Administratorowi podjęcia decyzji i działań niezbędnych do zapewnienia zgodności przetwarzania z prawem lub zakończenia powierzenia przetwarzania.

11. Wynagrodzenie określone w Umowie podstawowej obejmuje także wynagrodzenie za wykonywanie niniejszej Umowy. Przetwarzający oświadcza, że wynagrodzenie wskazane w zdaniu poprzednim wyczerpuje jego roszczenia wobec Administratora wynikające z niniejszej Umowy.

§ 6

1. Przetwarzający może powierzyć konkretne operacje przetwarzania Danych Osobowe w drodze pisemnej umowy podpowierzenia innym podmiotom przetwarzającym pod warunkiem uprzedniej akceptacji Podprzetwarzającego przez Administratora.
2. Dokonując podpowierzenia Przetwarzający ma obowiązek zobowiązać Podprzetwarzającego do realizacji wszystkich obowiązków Przetwarzającego wynikających z niniejszej Umowy, z wyjątkiem tych, które nie mają zastosowania ze względu na naturę konkretnego podpowierzenia.
3. Przetwarzający dostarczy Administratorowi Umowę podpowierzenia przetwarzania danych osobowych zawartą z Podprzetwarzającym.

§ 7

1. Przetwarzający powiadomi Administratora o każdym podejrzeniu naruszenia ochrony Danych osobowych nie później niż w 24 godziny od pierwszego zgłoszenia, umożliwi Administratorowi uczestnictwo w czynnościach wyjaśniających i poinformuje go o ustaleniach z chwilą ich dokonania, w szczególności o stwierdzeniu naruszenia.
2. Powiadomienie o stwierdzeniu naruszenia, powinno być przesłane wraz z wszelką niezbędną dokumentacją dotyczącą naruszenia, aby umożliwić Administratorowi spełnienie obowiązku powiadomienia organ nadzoru.
3. Przetwarzający zobowiązuje się do udzielania Administratorowi pomocy w zakresie:
    1) realizacji obowiązku odpowiadania na żądanie osoby której dane dotyczą, w zakresie wykonywania przez nią praw określonych w RODO.
    2) zapewnienia realizacji obowiązków wynikających z art. 32-36 RODO.

§8

1. W czasie trwania Umowy Administrator jest uprawniony do przeprowadzania kontroli przestrzegania przez Przetwarzającego zasad przetwarzania Danych Osobowych, w zakresie kontroli dokumentów, urządzeń i pomieszczeń związanych z przetwarzaniem Danych Osobowych.
2. Przedstawiciele Administratora uprawnieni będą do żądania od osób wyznaczonych przez Przetwarzającego udzielania potrzebnych informacji dotyczących przetwarzania przez Przetwarzającego Danych Osobowych.
3. Kontrola przestrzegania zasad przetwarzania Danych Osobowych może nastąpić wyłącznie po uprzednim powiadomieniu Przetwarzającego przez Administratora o zamiarze przeprowadzenia kontroli, co najmniej dwa dni przed planowanym terminem rozpoczęcia kontroli ze wskazaniem na piśmie osób wyznaczonych przez Administratora do przeprowadzenia kontroli.
4. Przetwarzający zobowiązuje się ujawnić niezbędne dokumenty i informacje, przedstawić sposób realizacji Umowy oraz przekazać inne dane niezbędne do sprawdzenia sposobu i zakresu ochrony Danych Osobowych.

5. Przetwarzający zobowiązuje się zastosować do zaleceń Administratora, dotyczących poprawy jakości zabezpieczenia powierzonych do przetwarzania Danych Osobowych.

§9

1. Przetwarzający odpowiada za szkody spowodowane swoim działaniem w związku z niedopełnieniem obowiązków, które RODO nakłada bezpośrednio na Przetwarzającego lub gdy działał poza zgodnymi z prawem instrukcjami Administratora lub wbrew tym instrukcjom. Przetwarzający odpowiada za szkody spowodowane zastosowaniem lub niezastosowaniem właściwych środków bezpieczeństwa.
2. Jeżeli Podprzetwarzający nie wywiąże się ze spoczywających na nim obowiązków ochrony danych, pełna odpowiedzialność wobec Administratora i osób trzecich za wypełnienie obowiązków przez Podprzetwarzającego spoczywa na Przetwarzającym.

§10

1. Niniejsza Umowa zostaje zawarta na czas trwania Umowy podstawowej.
2. Administrator może wypowiedzieć niniejszą Umowę ze skutkiem natychmiastowym w przypadku naruszenia przez Przetwarzającego postanowień Umowy, przepisów Ustawy lub Rozporządzenia, w szczególności w przypadku udostępniania Danych Osobowych osobom nieuprawnionym, a także w przypadku, gdy:
    a. organy administracji państwowej odpowiedzialne za nadzór nad przestrzeganiem zasad przetwarzania danych osobowych stwierdzą, że Przetwarzający nie przestrzega tych zasad;
    b. Administrator, w wyniku przeprowadzenia kontroli stwierdzi, że Przetwarzający nie przestrzega zasad przetwarzania Danych Osobowych lub przepisów Rozporządzenia;
    c. Przetwarzający utrudnia lub uniemożliwia przeprowadzenie kontroli o której mowa w niniejszej umowie.
3. Przetwarzający zobowiązuje się do natychmiastowego rozwiązania umowy z podmiotem Podprzetwarzajacym w przypadku, gdy zażąda tego Administrator, a w szczególności w sytuacji, gdy Podprzetwarzający nie przestrzega zasad przetwarzania danych osobowych wynikających z obowiązujących przepisów prawa

§11

1. Z chwilą rozwiązania Umowy Przetwarzający nie ma prawa do dalszego przetwarzania powierzonych Danych Osobowych i jest zobowiązany do:
    1) usunięcia Danych Osobowych,
    2) usunięcia wszelkich istniejących kopii lub zwrotu Danych Osobowych, chyba że Administrator postanowi inaczej lub prawo Unii Europejskiej lub prawo państwa członkowskiego nakazują dalsze przechowywanie Danych Osobowych.

§12

1. Przetwarzający odpowiada za wszelkie zawinione szkody, jakie powstaną u Administratora lub osób trzecich w wyniku niezgodnego z Umową przetwarzania przez Przetwarzającego i Podprzetwarzającego Danych Osobowych.
2. W przypadku, gdy:
    a. Przetwarzający lub Podprzetwarzający przekroczy zakres upoważnienia do przetwarzania Danych Osobowych określony w Umowie;

b. Przetwarzający lub Podprzetwarzający nie wykonuje, lub nienależycie wykonuje którykolwiek z obowiązków wynikający z Umowy lub przepisów o ochronie danych osobowych, czego konsekwencją jest postępowanie administracyjne, cywilne lub karne w związku z powierzeniem przetwarzania danych osobowych, Przetwarzający zapłaci Administratorowi karę umowną w wysokości 0,5% wartości brutto Umowy Podstawowej za każde stwierdzone naruszenie, oraz pokryje wszelkie ewentualne kary nałożone na Administratora.

§13

1. Wszelkie zmiany Umowy wymagają, pod rygorem nieważności, formy pisemnej.
2. Spory, które wynikną w związku z niniejszą Umową rozstrzygane będą przez sąd właściwy dla siedziby Administratora.
3. Niniejsza Umowa podlega prawu polskiemu.
4. Niniejsza Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach w języku polskim, po jednym egzemplarzu dla każdej ze Stron.

Administrator | Przetwarzający

_____ | _____

Załącznik Nr 8 do SIWZ, nr sprawy PN-135/MS/ZS/UE

Oświadczenie Wykonawcy

pieczęć Wykonawcy

Oświadczenie Wykonawcy/Podwykonawcy/Konsorcjum/Podmiot użyczający*
Potwierdzające brak podstaw do wykluczenia z postępowania

w imieniu ……
(pełna nazwa/firma, adres, w zależności od podmiotu: NIP/PESEL, KRS/CEiDG)

uczestniczący w postępowaniu w sprawie udzielenia zamówienia publicznego w trybie przetargu nieograniczonego na dostawę:
urządzeń peryferyjnych i komputerów dla Centrum Onkologii – Instytut Marii Skłodowskiej Curie" dla projektu: „Nowoczesny Szpital, Nowoczesny ZOZ" realizowanego w ramach RPMA.02.01.01-14-2641/15-00"

1. Oświadczam, że wobec ww. wykonawcy/ firmy nie orzeczono tytułem środka zapobiegawczego zakazu ubiegania się o zamówienie publiczne.

....., dnia ..... r. .....
podpis i pieczątka imienna osoby upoważnionej do reprezentowania firmy lub podpis osoby fizycznej

2. Oświadczam, że ww. wykonawca/ firma w rozumieniu ustawy z dnia 12 stycznia 1991 r. *o podatkach i opłatach lokalnych* **nie zalega z opłacaniem podatków i opłat lokalnych**.

....., dnia ..... r. .....
podpis i pieczątka imienna osoby upoważnionej do reprezentowania firmy lub podpis osoby fizycznej

3. Oświadczam, że wobec ww. wykonawcy/ firmy:
- **nie wydano prawomocnego wyroku sądu lub ostatecznej decyzji administracyjnej** o zaleganiu z uiszczaniem podatków, opłat lub składek na ubezpieczenia społeczne lub zdrowotne*
- **wydano wyrok lub decyzję***
  Jeśli tak: Wykonawca zobowiązany jest do przedstawienia dokumentów potwierdzających dokonanie płatności tych należności wraz z ewentualnymi odsetkami lub grzywnami lub informacja o zawarciu wiążącego porozumienia w sprawie spłat tych należności.

**niepotrzebne skreślić*

....., dnia ..... r. .....
podpis i pieczątka imienna osoby upoważnionej do reprezentowania firmy lub podpis osoby fizycznej