Wałbrzych 21.03.2018 r.

DZPZ-530-Zp/22/PN-16/18

ZMIANA TREŚCI SIWZ

Dotyczy: przetarg nieograniczony na **„Dostawa sprzętu komputerowego wraz z oprogramowaniem tj.: serwerów, zestawów komputerowych, laptopów, tabletów, drukarek wraz z oprogramowaniem oraz rozbudowa obecnej infrastruktury macierzy i przełączników dla poprawy dostępności i skuteczności leczenia onkologicznego na terenie województwa dolnośląskiego na potrzeby Specjalistycznego Szpitala im. dra. Alfreda Sokołowskiego w Wałbrzychu"** *– Zp/22/PN-16/18*

Specjalistyczny Szpital im. dra Alfreda Sokołowskiego w Wałbrzychu zgodnie z art. 38 ust. 4 ustawy Pzp zmienia treść SIWZ tj. zmienia treść następujących pkt.:

IV. Wymagania od Wykonawców

O zamówienie mogą ubiegać się Wykonawcy, którzy:

a) nie podlegają wykluczeniu zgodnie z art. 24 ust. 1 pkt. 12-23 i ust. 5 pkt. 1, 5, 6 i 8 ustawy Pzp,

b) spełniają warunki udziału w postępowaniu, tj.: posiadają co najmniej dwie dostawy odpowiadającą swoim rodzajem przedmiotowi zamówienia, w szczególności :

- dostawę, uruchomienie macierzy dyskowych oraz serwerów wraz z oprogramowaniem do wirtualizacji, o wartości co najmniej 600 000,00 zł. (słownie: sześćset tysięcy złotych) brutto każda z dostaw (dot. pakietu nr 1) – każda z dostaw.

- dostawę sprzętu komputerowego o wartości co najmniej 150 000,00 zł. (słownie: sto pięćdziesiąt tysięcy złotych) brutto każda z dostaw (dot. pakietu nr 2) – każda z dostaw.

- systemów zabezpieczeń klasy UTM o wartości co najmniej 100 000,00 zł. (słownie sto tysięcy złotych) brutto każda z dostaw (dot. pakietu nr 3) – każda z dostaw.

W celu potwierdzenia spełniania warunku udziału w postępowaniu, dla pakietu nr 1, Zamawiający żąda od Wykonawcy wykazania, że dysponuje lub będzie dysponował zespołem osób posiadających kwalifikacje
i doświadczenie niezbędne do wykonania przedmiotu zamówienia, w skład którego wchodzą:

a. co najmniej jedna osoba w roli kierownika projektu posiadająca znajomość zasad zarządzania projektami potwierdzoną ważnym certyfikatem PRINCE 2 na poziomie „Practitioner" lub równoważny,
b. co najmniej jedna osoba posiadająca certyfikat techniczny producenta min. na poziomie zaawansowanym, potwierdzający kompetencje we wdrażaniu i konfiguracji oferowanych serwerów,
c. co najmniej jedna osoba posiadająca certyfikat techniczny producenta min. na poziomie zaawansowanym, potwierdzający kompetencje we wdrażaniu i konfiguracji oferowanych macierzy dyskowych,

d. co najmniej jedna osoba posiadająca certyfikat techniczny potwierdzający kompetencje we wdrażaniu oferowanego oprogramowania do wirtualizacji,
e. co najmniej jedna osoba posiadająca certyfikat techniczny producenta min. na poziomie zaawansowanym, potwierdzający kompetencje we wdrażaniu i konfiguracji oferowanych przełączników.

V. Sposób oceny warunków udziału w postępowaniu

L.p.	Nazwa warunku	Sposób oceny warunku
1.	**Potwierdzenie spełniania przez Wykonawcę warunków udziału w postępowaniu**	**na podstawie załączonego do oferty przetargowej Jednolitego Europejskiego Dokumentu Zamówienia (JEDZ) oraz dokumentów do których przekazania zostanie wezwany Wykonawca, którego oferta zostanie uznana za najkorzystniejszą tj. :** **1) Posiadanie zdolności zawodowych w zakresie świadczenia dostaw odpowiadających swoim rodzajem przedmiotowi zamówienia** - na podstawie wykazu dostaw odpowiadających swoim rodzajem przedmiotowi zamówienia, wykonanych, a w przypadku świadczeń okresowych lub ciągłych również wykonywanych, w okresie ostatnich 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, wraz z podaniem ich wartości, przedmiotu, dat wykonania i podmiotów, na rzecz których dostawy zostały wykonane, oraz załączeniem dowodów określających, czy te dostawy zostały wykonane lub są wykonywane należycie, przy czym dowodami, o których mowa są referencje bądź inne dokumenty wystawione przez podmiot, na rzecz którego dostawy były wykonywane, a w przypadku świadczeń okresowych lub ciągłych są wykonywane, a jeżeli z uzasadnionej przyczyny o obiektywnym charakterze wykonawca nie jest w stanie uzyskać tych dokumentów- oświadczenie wykonawcy; w przypadku świadczeń okresowych lub ciągłych nadal wykonywanych referencje bądź inne dokumenty potwierdzające uch należyte wykonywanie powinny być wydane nie wcześniej niż 3 miesiące przed upływem terminu składania ofert o dopuszczenie do udziału w postępowaniu, tj.: posiadają co najmniej dwie dostawy odpowiadającą swoim rodzajem przedmiotowi zamówienia, w szczególności : - dostawę, uruchomienie macierzy dyskowych oraz serwerów wraz z oprogramowaniem do wirtualizacji, o wartości co najmniej 600.000,00 zł. (słownie: sześćset tysięcy złotych) brutto każda z dostaw (dot. pakietu nr 1) – każda z dostaw - dostawę sprzętu komputerowego o wartości co najmniej 150 000 zł. (słownie: sto pięćdziesiąt tysięcy złotych) brutto każda z dostaw (dot. pakietu nr 2) – każda z dostaw. - systemów zabezpieczeń klasy UTM o wartości co najmniej 100 000 zł. (słownie sto tysięcy złotych) brutto każda z dostaw (dot. pakietu nr 3) – każda z dostaw. **2) posiadanie zdolności technicznych w zakresie pakietu nr 1:** Wykaz osób, które będą uczestniczyć w wykonywaniu zamówienia, w szczególności odpowiedzialnych za świadczenie usługi wraz z informacjami na temat ich kwalifikacji zawodowych, niezbędnych do wykonania zamówienia, tj: a. co najmniej jedna osoba w roli kierownika projektu posiadająca znajomość zasad zarządzania projektami potwierdzoną ważnym certyfikatem PRINCE 2 na poziomie „Practitioner" lub równoważny, b. co najmniej jedna osoba posiadająca certyfikat techniczny producenta min. na poziomie zaawansowanym, potwierdzający kompetencje we wdrażaniu i konfiguracji oferowanych serwerów, c. co najmniej jedna osoba posiadająca certyfikat techniczny producenta min. na poziomie zaawansowanym, potwierdzający kompetencje we wdrażaniu i konfiguracji oferowanych macierzy dyskowych, d. co najmniej jedna osoba posiadająca certyfikat techniczny potwierdzający kompetencje we wdrażaniu oferowanego oprogramowania do wirtualizacji,

		e. co najmniej jedna osoba posiadająca certyfikat techniczny producenta min. na poziomie zaawansowanym, potwierdzający kompetencje we wdrażaniu i konfiguracji oferowanych przełączników.
2.	**Potwierdzenie braku podstaw do wykluczenia zgodnie z art. 24 ust. 1 pkt. 12-23 oraz ust. 5 pkt. 1, 5, 6 i 8**	**<u>na podstawie załączonego do oferty przetargowej Jednolitego Europejskiego Dokumentu Zamówienia (JEDZ) oraz dokumentów do których zostanie wezwany Wykonawca, którego oferta zostanie uznana za najkorzystniejszą tj. :</u>** **1) posiadanie odpisu z właściwego rejestru** – na podstawie odpisu z właściwego rejestru lub z centralnej ewidencji i informacji o działalności gospodarczej, jeżeli odrębne przepisy wymagają wpisu do rejestru lub ewidencji, w celu potwierdzenia braku podstaw wykluczenia na podstawie art. 24 ust. 5 pkt. 1 ustawy; **2) posiadanie zaświadczenia właściwego naczelnika urzędu skarbowego potwierdzającego że Wykonawca nie zalega z uiszczaniem podatków** – na podstawie zaświadczenia właściwego naczelnika urzędu skarbowego potwierdzającego, że Wykonawca nie zalega z opłacaniem podatków, wystawionego nie wcześniej niż 3 miesiące przed upływem terminu składania ofert lub innego dokumentu potwierdzającego, że wykonawca zawarł porozumienie z właściwym organem podatkowym w sprawie spłat tych należności wraz z ewentualnymi odsetkami lub grzywnami, w szczególności uzyskał przewidziane prawem zwolnienie, odroczenie lub rozłożenie na raty zaległych płatności lub wstrzymanie w całości wykonania decyzji właściwego organu. **3) posiadanie zaświadczenia właściwej terenowej jednostki organizacyjnej ZUS lub KRUS potwierdzającego, że Wykonawca nie zalega z opłacaniem składek na ubezpieczenie zdrowotne lub społeczne -** na podstawie zaświadczenia właściwej terenowej jednostki organizacyjnej ZUS lub KRUS albo innego dokumentu potwierdzającego, że wykonawca nie zalega z opłacaniem składek na ubezpieczenie społeczne lub zdrowotnie, wystawione nie wcześniej niż 3 miesiące przed upływem terminu składania ofert, lub innego dokumentu potwierdzającego, że wykonawca zawarł porozumienie z właściwym organem w sprawie spłat tych należności wraz z ewentualnymi odsetkami lub grzywnami, w szczególności uzyskał przewidziane prawem zwolnienie, odroczenie lub rozłożenie na raty zaległych płatności lub wstrzymanie w całości wykonania decyzji właściwego organu. **4) posiadanie informacji z Krajowego Rejestru Karnego:** –na podstawie informacji z Krajowego Rejestru Karnego w zakresie określonym w art. 24 ust. 1 pkt. 13, 14 i 21 Pzp oraz odnośnie skazania za wykroczenie na karę aresztu, w zakresie określonym przez Zamawiającego na podstawie art. 24 ust. 5 pkt. 5 i 6 Pzp, wystawionej nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert, - na podstawie oświadczenia Wykonawcy o braku orzeczenia wobec niego tytułem środka zapobiegawczego zakazu ubiegania sie o zamówienie publiczne oraz o braku wydania prawomocnego wyroku sądowego za wykroczenie na karę ograniczenia wolności lub grzywny w zakresie określonym przez Zamawiającego na podstawie art. 24 ust. 5 pkt. 5 i 6 Pzp

A) Jeżeli Wykonawca ma siedzibę lub miejsce zamieszkania poza terytorium Rzeczypospolitej Polskiej w celu wykazania spełniania warunków udziału w postępowaniu zamiast dokumentów wymienionych w:

<u>- pkt. 2 tabeli:</u>

a) ppkt. 1, 2, 3, 4 - składa dokument lub dokumenty wystawione w kraju, w którym ma siedzibę lub miejsce zamieszkania, potwierdzające odpowiednio, że :

- **ppkt. 1-** nie otwarto jego likwidacji ani nie ogłoszono upadłości (wystawiony nie wcześniej niż 6 m-cy przed upływem terminu składania ofert),

- **ppkt. 2, 3 -** nie zalega z opłacaniem podatków, opłat, składek na ubezpieczenie społeczne lub zdrowotne albo że zawarł porozumienie z właściwym organem w sprawie spłat tych należności wraz z ewentualnymi odsetkami lub grzywnami, w szczególności uzyskał przewidziane prawem zwolnienie, odroczenie lub rozłożenie na raty zaległych płatności lub wstrzymanie w całości wykonania decyzji właściwego organu (wystawiony nie wcześniej niż 3 m-ce przed upływem terminu składania ofert),

- ppkt. 4 – składa informację z odpowiedniego rejestru albo, w przypadku takiego rejestru , inny równoważny dokument wydany przez właściwy organ sądowy lub administracyjny kraju, w którym Wykonawca ma siedzibę lub miejsce zamieszkania lub miejsce zamieszkania ma osoba, której dotyczy informacja albo dokument w zakresie określonym w art. 24 ust. 1 pkt. 13, 14 i 21 oraz ust. 5 pkt. 5 i 6 ustawy Pzp.

B. Jeżeli w kraju, w którym wykonawca ma siedzibę lub miejsce zamieszkania lub miejsce zamieszkania ma osoba, której dokument dotyczy, nie wydaje się w/w dokumentów, zastępuje się je dokumentem zawierającym odpowiednio oświadczenie wykonawcy, ze wskazaniem osoby albo osób uprawnionych do jego reprezentacji, lub oświadczenie osoby, której dokument miał dotyczyć, złożone przed notariuszem lub przed organem sądowym, administracyjnym albo organem samorządu zawodowego lub gospodarczego właściwym ze względu na siedzibę lub miejsce zamieszkania wykonawcy lub miejsce zamieszkania tej osoby.

C. W przypadku wątpliwości co do treści dokumentu złożonego przez wykonawcę, zamawiający może zwrócić się do właściwych organów odpowiednio kraju, w którym wykonawca ma siedzibę lub miejsce zamieszkania lub miejsce zamieszkania ma osoba, której dokument dotyczy, o udzielenie niezbędnych informacji dotyczących tego dokumentu.

VII. Wadium

Kwota wadium wymagana do wzięcia udziału w postępowaniu:

- 36 000,00 zł. – dla Pakietu nr 1

- 10 000,00 zł. – dla Pakietu nr 2

- 6 000,00 zł. – dla Pakietu nr 3

DATĄ UZNANIA WPŁATY BĘDZIE DATA WPŁYWU NA KONTO ZAMAWIAJĄCEGO.

Konto bankowe: Bank Zachodni WBK S.A. o/Wałbrzych 36 1500 1764 1217 6005 2413 0000.

Potwierdzenie wniesienia wadium należy dołączyć do oferty. Na potwierdzeniu wniesienia wadium należy wyszczególnić pakiety oraz kwoty wadium w pakietach na które składana jest oferta. Podać należy również kwotę końcową (za wszystkie pakiety) po podliczeniu kwot jednostkowych.

Oferta nie zabezpieczona akceptowalną formą wadium zostanie odrzucona bez rozpatrywania.

Wadium może być wnoszone w jednej lub kilku następujących formach:

1) pieniądzu,
2) poręczeniach bankowych lub poręczeniach spółdzielczej kasy oszczędnościowo-kredytowej, z tym, że poręczenie kasy jest zawsze poręczeniem pieniężnym,
3) gwarancjach bankowych,
4) gwarancjach ubezpieczeniowych,
5) poręczeniach udzielanych przez podmioty, o których mowa w art. 6b ust. 5 pkt 2 ustawy z dnia 9 listopada 2000 r. o utworzeniu Polskiej Agencji Rozwoju Przedsiębiorczości (tekst jednolity: Dz. U. Nr 109, poz. 1158).

Gwarancja ubezpieczeniowa lub gwarancja bankowa złożona, jako zabezpieczenie wadium musi posiadać okres ważności nie krótszy niż okres związania ofertą.

Informacje dodatkowe:

1) wadium wnosi się przed upływem terminu składania ofert. W przypadku wnoszenia wadium w formie pieniężnej za termin wniesienia wadium przyjmuje się datę uznania rachunku bankowego Zamawiającego,
2) w przypadku wnoszenia wadium w innej formie, kopię dokumentu należy dołączyć do oferty, a oryginał złożyć w osobnej kopercie (która nie zostanie włożona do koperty z ofertą przetargową) w siedzibie Zamawiającego – Dział Zamówień Publicznych i Zaopatrzenia**,** budynek C, opisując

   „NAZWA WYKONAWCY I JEGO ADRES"

   „NAZWA ZAMAWIAJĄCEGO I JEGO ADRES"

   wadium w „TRYB PRZETARGU"

   na „NAZWA (TYTUŁ) POSTĘPOWANIA"

   nie otwierać przed „DATA I GODZINA OTWARCIA OFERT"

3) wadium będzie zwrócone w terminie i na warunkach wskazanych w art. 46 ust.1-4 Pzp,
4) Zamawiający zatrzyma wadium w przypadkach określonych w art. 46 ust. 4a i 5 Pzp.
5) Wadium wniesione na podstawie art. 45 ust. 6 ustawy pzp w innej formie niż pieniądzu, winno zawierać, niebudzące wątpliwości interpretacyjnych zapisy dotyczące wypłaty i zatrzymania wadium przez Zamawiającego. W szczególności dotyczy to przesłanek zawartych w art. 46 ust. 4a i 5 ustawy pzp, poprzez wyszczególnienie w zapisach wszystkich przypadków umożliwiających zatrzymanie Zamawiającemu wadium i jego bezwarunkowej wypłaty, po spełnieniu któregokolwiek z warunków określonych w art. 46 ust. 4a i 5 ustawy pzp.

XI.A Dokumenty, do których przekazania wezwany zostanie Wykonawca, którego oferta zostanie uznana za najkorzystniejszą, zgodnie z art. 26 ustawy Pzp.

Lp.	Nazwa (rodzaj) dokumentu
1.	Odpis z właściwego rejestru lub z centralnej ewidencji i informacji o działalności gospodarczej, jeżeli odrębne przepisy wymagają wpisu do rejestru lub ewidencji, w celu potwierdzenia braku podstaw wykluczenia na podstawie art. 24 ust. 5 pkt. 1 ustawy.
2.	Zaświadczenie właściwego naczelnika urzędu skarbowego potwierdzającego, że wykonawca nie zalega z opłacaniem podatków, wystawionego nie wcześniej niż 3 miesiące przed upływem terminu składania ofert, lub innego dokumentu potwierdzającego, że wykonawca zawarł porozumienie z właściwym organem podatkowym w sprawie spłat tych należności wraz z ewentualnymi odsetkami lub grzywnami, w szczególności uzyskał przewidziane prawem zwolnienie, odroczenie lub rozłożenie na raty zaległych płatności lub wstrzymanie w całości wykonania decyzji właściwego organu.
3.	Zaświadczenie właściwej terenowej jednostki organizacyjnej ZUS lub KRUS albo innego dokumentu potwierdzającego, że wykonawca nie zalega z opłacaniem składek na ubezpieczenie społeczne lub zdrowotnie, wystawione nie wcześniej niż 3 miesiące przed upływem terminu składania ofert, lub innego dokumentu potwierdzającego, że wykonawca zawarł porozumienie z właściwym organem w sprawie spłat tych należności wraz z ewentualnymi odsetkami lub grzywnami, w szczególności uzyskał przewidziane prawem zwolnienie, odroczenie lub rozłożenie na raty zaległych płatności lub wstrzymanie w całości wykonania decyzji właściwego organu.
4.	1) Wykaz dostaw odpowiadających swoim rodzajem przedmiotowi zamówienia wykonanych, a w przypadku świadczeń okresowych lub ciągłych również wykonywanych, w okresie ostatnich 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, wraz z podaniem ich wartości, przedmiotu, dat wykonania i podmiotów, na rzecz których dostawy zostały wykonane, oraz załączeniem dowodów określających, czy te dostawy zostały wykonane lub są wykonywane należycie, przy czym dowodami, o których mowa są referencje bądź inne dokumenty wystawione przez podmiot, na rzecz którego dostawy były wykonywane, a w przypadku świadczeń okresowych lub ciągłych są wykonywane, a jeżeli z uzasadnionej przyczyny o obiektywnym

	charakterze wykonawca nie jest w stanie uzyskać tych dokumentów- oświadczenie wykonawcy; w przypadku świadczeń okresowych lub ciągłych nadal wykonywanych referencje bądź inne dokumenty potwierdzające ich należyte wykonywanie powinny być wydane nie wcześniej niż 3 miesiące przed upływem terminu składania ofert o dopuszczenie do udziału w postępowaniu tj. posiadają co najmniej dwie dostawy odpowiadającą swoim rodzajem przedmiotowi zamówienia, w szczególności : - dostawę, uruchomienie macierzy dyskowych oraz serwerów wraz z oprogramowaniem do wirtualizacji, o wartości co najmniej 600.000,00 zł. (słownie: sześćset tysięcy złotych) brutto każda z dostaw (dot. pakietu nr 1) każda z dostaw. - dostawę sprzętu komputerowego o wartości co najmniej 150 000 zł. (słownie: sto pięćdziesiąt tysięcy złotych) brutto każda z dostaw (dot. pakietu nr 2) każda z dostaw. - systemów zabezpieczeń klasy UTM o wartości co najmniej 100 000 zł. (słownie sto tysięcy złotych) brutto każda z dostaw (dot. pakietu nr 3) każda z dostaw. **2) posiadanie zdolności technicznych w zakresie pakietu nr 1:** Wykaz osób, które będą uczestniczyć w wykonywaniu zamówienia, w szczególności odpowiedzialnych za świadczenie usługi wraz z informacjami na temat ich kwalifikacji zawodowych, niezbędnych do wykonania zamówienia, tj: a. o najmniej jedna osoba w roli kierownika projektu posiadająca znajomość zasad zarządzania projektami potwierdzoną ważnym certyfikatem PRINCE 2 na poziomie „Practitioner" lub równoważny, b. co najmniej jedna osoba posiadająca certyfikat techniczny producenta min. na poziomie zaawansowanym, potwierdzający kompetencje we wdrażaniu i konfiguracji oferowanych serwerów, c. co najmniej jedna osoba posiadająca certyfikat techniczny producenta min. na poziomie zaawansowanym, potwierdzający kompetencje we wdrażaniu i konfiguracji oferowanych macierzy dyskowych, d. co najmniej jedna osoba posiadająca certyfikat techniczny potwierdzający kompetencje we wdrażaniu oferowanego oprogramowania do wirtualizacji, e. co najmniej jedna osoba posiadająca certyfikat techniczny producenta min. na poziomie zaawansowanym, potwierdzający kompetencje we wdrażaniu i konfiguracji oferowanych przełączników.
5.	Informacja z Krajowego Rejestru Karnego w zakresie określonym w art. 24 ust. 1 pkt. 13, 14 i 21 ustawy Pzp oraz odnośnie skazania za wykroczenie na karę aresztu, w zakresie określonym przez Zamawiającego na podstawie art. 24 ust. 5 pkt. 5 i 6 ustawy Pzp, wystawionej nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert
6.	Oświadczenie Wykonawcy o braku orzeczenia wobec niego tytułem środka zapobiegawczego zakazu ubiegania sie o zamówienie publiczne oraz o braku wydania prawomocnego wyroku sądowego za wykroczenie na karę ograniczenia wolności lub grzywny w zakresie określonym przez Zamawiającego na podstawie art. 24 ust. 5 pkt. 5 i 6 Pzp stanowi załącznik nr 5 do SIWZ.
7.	- Oświadczenie o posiadaniu Certyfikatu EPEAT na poziomie co najmniej GOLD (dla pakietu nr 2) - Oświadczenie producenta komputera, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem (dla pakietu nr 2) - Oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii tel.) (dla pakietu nr 3) - Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania (dla pakietu nr 3) - Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań(dla pakietu nr 3) - Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań (pakiet nr 3)

Załącznik nr 1 do SIWZ

Pakiet nr 1.

Modernizacja infrastruktury serwerowo – sieciowej.

L.p.	Rodzaj	ILOŚĆ	Typ/model/ producent	Cena netto	Wartość netto	Podatek VAT	Wartość brutto
1	Serwery wirtualizacyjne	2					
2	Modernizacja istniejącej infrastruktury						
3	Urządzenia składujące dla systemu backupu	1					
4	Rozbudowa macierzy dyskowych	2					
5	Oprogramowanie do zabezpieczenia środowiska wirtualizacyjnego						
6	System operacyjny dla serwera backupu						
7	Rozbudowa obecnych przełączników rdzeniowych						
8	Przełącznik dystrybucyjny	2					
9	Przełącznik dostępowy	8					
Razem:							

Opis przedmiotu zamówienia:

- Serwery wirtualizacyjne

Wymagane dostarczenie 2 szt. serwerów SRV1 spełniających poniżej opisane minimalne parametry funkcjonalne.

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne	Spełnienie wymaganego parametru: Tak/Nie
1	**Obudowa**	Maksymalnie 2U RACK 19 cali (wraz z szynami montażowymi oraz ramieniem do prowadzenia kabli, umożliwiającymi serwisowanie serwera w szafie rack bez wyłączania urządzenia). Serwer musi mieć możliwość zamontowania czujnika otwarcia obudowy współpracującego z BIOS. Wymagane dostarczenie wszystkich elementów niezbędnych do montażu serwera oraz kabli zasilających z wtykiem C14.	
2	**Procesor**	Minimum dwa procesory dziesięciordzeniowe, x86-64 bity, o wydajności pozwalającej na osiągnięcie w testach SPECfp_rate2006 wyniku nie mniejszego niż 804 punktów. Wynik testu musi być opublikowany na stronie www.spec.org Zamawiający nie wymaga złożenia wraz z ofertą wyników w/w testów. Płyta główna wspierająca zastosowanie procesorów do 28 rdzeniowych.	
3	**Pamięć operacyjna**	Minimum 256GB RDIMM DDR4 2666 MT/s w modułach o pojemności 32GB każdy. Płyta główna z minimum 24 slotami na pamięć i umożliwiająca instalację do minimum 3TB. Obsługa zabezpieczeń: Advanced ECC i Online Spare. Serwer z obsługą pamięci typu NVDIMM	
4	**Sloty rozszerzeń**	Minimum 3 sloty PCI-Express Generacji 3 pełnej wysokości.	

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne	Spełnienie wymaganego parametru: Tak/Nie
		Serwer musi zapewniać możliwość rozbudowy do minimum 6 slotów PCI-Express Generacji 3 pełnej wysokości (full-height). Wymagany jest minimum jeden wolny (nieobsadzony) slot PCI-Express Generacji 3 po instalacji wymaganych interfejsów LAN/SAN.	
5	**Dysk twardy**	Zatoki dyskowe gotowe do zainstalowania 8 dysków SFF typu Hot Swap, SAS/SATA/SSD, 2,5" i opcja rozbudowy/rekonfiguracji serwera o dodatkowe 16 dysków typu Hot Swap, SAS/SATA/SSD, 2,5" montowane z przodu obudowy oraz możliwość zainstalowania 6 dysków SFF SAS/SATA/SSD, 2,5" z tyłu serwera. Zainstalowane min. 2 dyski 300GB SAS 10K HDD. W przypadku braku opcji rozbudowy/rekonfiguracji o dodatkowe zatoki dyskowe, serwer standardowo wyposażony w minimum 30 zatok dyskowych SFF gotowych do instalacji dysków SAS/SATA/SSD 2,5"typu Hot Swap. Serwer umożliwiający instalację pamięci flash w postaci kart microSD/SD zapewniających minimalną pojemność dla pojedynczej karty 8GB i redundancję danych RAID-1. Zastosowane rozwiązanie musi posiadać gwarancję producenta serwera.	
6	**Kontroler**	Wbudowany kontroler macierzowy SATA 6Gb zapewniający obsługę min. 12 napędów dyskowych SATA oraz obsługujący poziomy: RAID 0/1/5/10 Serwer wyposażony w kontroler sprzętowy zapewniający obsługę min. 30 napędów dyskowych SAS oraz obsługujący poziomy: RAID 0/1/5/10. Kontroler umożliwiający pracę z dyskami w trybach RAID i JBOD jednocześnie. Serwer musi mieć możliwość rozbudowy o sprzętowy kontroler RAID zapewniający obsługę RAID 0/1/5/6/10/50/60 z 4GB pamięci cache z podtrzymywaniem bateryjnym lub typu flash.	
7	**Interfejsy LAN / SAN**	Minimum 4 wbudowane porty Ethernet 100/1000 Mb/s RJ-45 z funkcją Wake-On-LAN, wsparciem dla PXE, które nie zajmują gniazd PCIe opisanych w sekcji „Sloty rozszerzeń".	

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne	Spełnienie wymaganego parametru: Tak/Nie
		Opcja rozbudowy o dodatkowe 2 porty obsługujące prędkości 10/40 Gb/s (możliwość konfiguracji pracy z prędkościami 10 i 40Gb/s), przez zastosowanie karty nie zajmującej gniazd PCIe opisanych w sekcji „Sloty rozszerzeń”. Wymagane są: • dwa interfejsy 10Gb/s Ethernet SFP+, • dwa karty jednoportowe FC HBA, każda o prędkości 16Gb/s z wkładkami 16Gb FC	
8	**Karta graficzna**	Zintegrowana karta graficzna	
9	**Porty**	• 5 x USB 3.0 (w tym 2 porty wewnętrzne) • 1x VGA • Wewnętrzny slot na kartę micro SD. Możliwość rozbudowy o: - dodatkowy port typu DisplayPort dostępny z przodu serwera - port szeregowy typu DB9/DE-9 (9 pinowy), wyprowadzony na zewnątrz obudowy bez pośrednictwa portu USB/RJ45	
10	**Zasilacz**	Minimum 2 szt., typu Hot-plug, redundantne, każdy o mocy minimum 500W.	
11	**Chłodzenie**	Zestaw wentylatorów redundantnych typu hot-plug	
12	**Zarządzanie i obsługa techniczna**	Niezależna od system operacyjnego, zintegrowana z płytą główną serwera lub jako dodatkowa karta w slocie PCI Express, jednak nie może ona powodować zmniejszenia minimalnej liczby gniazd PCIe w serwerze, posiadająca minimalną funkcjonalność: • monitorowanie podzespołów serwera: temperatura, zasilacze, wentylatory, procesory, pamięć RAM, kontrolery macierzowe i dyski(fizyczne i logiczne), karty sieciowe • wparcie dla agentów zarządzających oraz możliwość pracy w trybie bez agentowym – bez agentów zarządzania instalowanych w	

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne	Spełnienie wymaganego parametru: Tak/Nie
		systemie operacyjnym z generowaniem alertów SNMP • dostęp do karty zarządzającej poprzez - dedykowany port RJ45 z tyłu serwera lub - przez współdzielony port zintegrowanej karty sieciowej serwera dostęp do karty możliwy - z poziomu przeglądarki webowej (GUI) - z poziomu linii komend zgodnie z DMTF System Management Architecture for Server Hardware, Server Management CommiLine Protocol (SM CLP) - z poziomu skryptu (XML/Perl) - poprzez interfejs IPMI 2.0 (Intelligent Platform Management Interface) • wbudowane narzędzia diagnostyczne • zdalna konfiguracji serwera(BIOS) i instalacji systemu operacyjnego • obsługa mechanizmu remote support - automatyczne połączenie karty z serwisem producenta sprzętu, automatyczne przesyłanie alertów, zgłoszeń serwisowych i zdalne monitorowanie • wbudowany mechanizm logowania zdarzeń serwera i karty zarządzającej w tym włączanie/wyłączanie serwera, restart, zmiany w konfiguracji, logowanie użytkowników • przesyłanie alertów poprzez e-mail oraz przekierowanie SNMP (SNMP passthrough) • obsługa zdalnego serwera logowania (remote syslog) • wirtualna zdalna konsola, tekstowa i graficzna, z dostępem do myszy i klawiatury i możliwością podłączenia wirtualnych napędów FDD, CD/DVD i USB i i wirtualnych folderów • mechanizm przechwytywania, nagrywania i odtwarzania sekwencji video dla ostatniej awarii i ostatniego startu serwera a także nagrywanie na żądanie	

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne	Spełnienie wymaganego parametru: Tak/Nie
		• funkcja zdalnej konsoli szeregowej - Textcons przez SSH (wirtualny port szeregowy) z funkcją nagrywania i odtwarzania sekwencji zdarzeń i aktywności • monitorowanie zasilania oraz zużycia energii przez serwer w czasie rzeczywistym z możliwością graficznej prezentacji • konfiguracja maksymalnego poziomu pobieranej mocy przez serwer (capping) • zdalna aktualizacja oprogramowania (firmware) • zarządzanie grupami serwerów, w tym: - tworzenie i konfiguracja grup serwerów - sterowanie zasilaniem (wł/wył) - ograniczenie poboru mocy dla grupy (power caping) - aktualizacja oprogramowania (firmware) - wspólne wirtualne media dla grupy • możliwość równoczesnej obsługi przez 6 administratorów • autentykacja dwuskładnikowa (Kerberos) • wsparcie dla Microsoft Active Directory • obsługa SSL i SSH • enkrypcja AES/3DES oraz RC4 dla zdalnej konsoli • wsparcie dla IPv4 oraz iPv6, obsługa SNMP v3 oraz RESTful API • wsparcie dla Integrated Remote Console for Windows clients • możliwość autokonfiguracji sieci karty zarządzającej (DNS/DHCP)	
13	**Wsparcie dla Systemów Operacyjnych i Systemów Wirtualizacyjnych**	• Microsoft Windows Server 2012 R2, 2016 • Red Hat Enterprise Linux (RHEL) 6.9 oraz 7.3 • SUSE Linux Enterprise Server (SLES) 11 SP4 oraz 12 SP2 • ClearOS • CentOS • VMware ESXi 6.0 • VMware ESXi 6.5	

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne	Spełnienie wymaganego parametru: Tak/Nie
14	**Wsparcie techniczne**	Wymagane 5 letnie wsparcie techniczne z możliwością zgłaszania problemów w dni robocze w godzinach 8-17 i z czasem reakcji w następnym dniu roboczym. Wsparcie musi obejmować wszystkie komponenty oferowanych urządzeń, nie dopuszcza się stosowania różnych poziomów wsparcia w zależności od tego jak krytyczny jest problem. Wsparcie musi być oferowane w języku polskim przez polski oddział serwisowy producenta.	

- Modernizacja istniejącej infrastruktury

Wymagane jest dostarczenie niżej wymienionych elementów oraz wsparcia do posiadanej przez Zamawiającego infrastruktury.

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne	Spełnienie wymaganego parametru: Tak/Nie
1	**Rozbudowa serwerów DL380 Gen8**	• Moduł pamięci RAM HP 16GB 2Rx4 PC3-14900R-13 Kit do serwera HP DL380 Gen8 – sztuk 16 • Karta LAN 10Gb/s - HPE Ethernet 10Gb 2P 560SFP+ Adptr dla serwera HP DL380 Gen8 - sztuk 2 • Rozszerzenie ilości slotów w serwerze HP DL380 Gen8 (HP DL380p/560 G8 3Slot PCIe Rsr Kit) – sztuk 2	
2	**Rozbudowa serwera backupu IBM x3650 M3**	• Karta dwuportowa LAN 10Gb/s SFP+, oficjalnie wspierana przez producenta serwera IBM x3650 M3, gwarancja min 1 rok • Dwa dyski 600GB 10K 6Gbps SAS 2.5in SFF wraz kieszeniami zapewniającymi instalację w serwerze x3650 M3, gwarancja min 1 rok	
3	**Rozbudowa przełączników SAN HPE 8/8 (P/N: AM867B)**	• Licencja aktywacyjna dodatkowych 8 portów w przełączniku – sztuk 2 • Wkładki HPE 8Gb Short Wave B-Series SFP+ - sztuk 8	

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne	Spełnienie wymaganego parametru: Tak/Nie
4	**Wsparcie serwisowe dla posiadanej infrastruktury**	Dla wymienionego sprzętu wymagane jest przedłużenie wsparcia serwisowego do dnia minimum 31.01.2023, obsługa 8-17, czas reakcji Następny Dzień Roboczy, wsparcie dla sprzętu świadczone przez producenta urządzeń • Przełącznik sieci SAN HP 8/8 (8)-ports Enabled SAN Switch, PN: AM867B, SN: CZC421TW0W • Przełącznik sieci SAN HP 8/8 (8)-ports Enabled SAN Switch, PN: AM867B, SN: CZC421TW0T • Serwer HP DL380 Gen8, PN: 653200-B21, SN: CZ34247EES • Serwer HP DL380 Gen8, PN: 653200-B21, SN: CZ34247EEV	
5	**Okablowanie FC**	Wymagane jest dostarczenie następującego okablowania FC: • Patchord FC LC/LC OM4 – 3m – sztuk 4 • Patchord FC LC/LC OM4 – 5m – sztuk 8 • Patchord FC LC/LC OM4 – 10m – sztuk 8	
6	**Wkładki SFP+ do serwerów**	Wymagane jest dostarczenie 12 szt. wkładek 10Gb SFP+ SR kompatybilnych z kartami Ethernet 10Gb zainstalowanych w: • dwóch serwerach SRV1, • dodatkowych kartach w posiadanych serwerach DL380 Gen8, • serwerze backupu BCK x3620 M3	

- Urządzenie składujące dla systemu backupu

Wymagane dostarczenie 1 szt. urządzenia do backupu dyskowego spełniającego poniżej opisane minimalne parametry funkcjonalne.

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne	Spełnienie wymagane parametru: Tak/Nie
1	**Definicja**	Przez urządzenie do backupu dyskowego z deduplikacją danych Zamawiający rozumie rozwiązanie charakteryzujące się jednolitą budową typu „appliance" pochodzące od jednego producenta i realizujące wszystkie wymagane funkcjonalności. Nie dopuszcza się rozwiązania zbudowanego z niezależnych komponentów sprzętowo-programowych. Urządzenie powinno być oficjalnie dostępne w ofercie producenta przed ukazaniem się niniejszego postępowania.	
2	**Typ obudowy**	Urządzenie musi być przystosowana do montażu w szafie rack 19".	
3	**Przestrzeń dyskowa**	Urządzenie musi oferować minimum 14 TB przestrzeni użytkowej dla danych (bez deduplikacji).	
4	**Bezpieczeństwo danych**	Dane przechowywane w obrębie podsystemu dyskowego urządzenia muszą być chronione za pomocą technologii RAID 6. Urządzenie musi weryfikować ewentualne przekłamanie danych w wyniku działań systemu plików / mechanizmów RAID zaimplementowanych w urządzeniu. Wymaga się, aby urządzenie sprawdzało sumy kontrolne zapisywanych fragmentów danych po przejściu danych przez system plików / mechanizmy RAID. Urządzenie musi automatycznie rozpoznawać i naprawiać błędy w locie.	
5	**Możliwość rozbudowy**	Urządzenie musi umożliwiać rozbudowę pojemności użytkowej dla danych (bez deduplikacji) do co najmniej 28 TB bez uwzględniania mechanizmów protekcji.	
6	**Interfejsy do hostów**	Urządzenie musi posiadać minimum: • 4 porty Ethernet 1 Gb/s z możliwością obsługi każdym portem Ethernet protokołów CIFS i NFS oraz deduplikacji na źródle, • 2 porty Ethernet 10 Gb/s SFP+ z możliwością obsługi każdym portem Ethernet protokołów CIFS i NFS oraz	

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne	Spełnienie wymagane parametru: Tak/Nie
		deduplikacji na źródle, porty muszą być obsadzone wkładkami 10Gb/s SFP+ SR. Oferowane urządzenie musi posiadać możliwość rozbudowy o dodatkowe 6 portów FC 16 Gb/s lub 6 portów Ethernet 10 Gb/s bez konieczności wymiany jakichkolwiek komponentów sprzętowych.	
7	**Wydajność**	Urządzenie musi osiągać w maksymalnej konfiguracji zagregowaną wydajność backupu protokołami CIFS / NFS / VTL co najmniej 4 TB/h (dane podawane przez producenta) oraz co najmniej 10 TB/h z wykorzystaniem deduplikacji na źródle (dane podawane przez producenta). Urządzenie nie może zmniejszać swojej wydajności w czasie przybywania kolejnych danych.	
8	**Sposób udostępniania zasobów**	Urządzenie musi umożliwiać jednoczesny dostęp do całej pojemności urządzenia wszystkimi poniższymi protokołami: • CIFS, NFS i deduplikacja na źródle (OST/Boost/Catalyst) dla interfejsów Ethernet, • VTL i deduplikacja na źródle (OST/Boost/Catalyst) dla interfejsów FC. Urządzenie musi posiadać obsługę mechanizmów deduplikacji dla danych otrzymywanych wszystkimi protokołami (CIFS, NFS, VTL, deduplikacja na źródle) przechowywanych w obrębie urządzenia. Oferowane urządzenie musi mieć możliwość emulacji napędów taśmowych LTO oraz emulacji bibliotek taśmowych. Urządzenie musi umożliwiać przyporządkowanie minimum 128 napędów do pojedynczej biblioteki taśmowej. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.	
9	**Partycjonowanie**	Urządzenie musi umożliwiać podział na minimum 22 partycje logiczne w taki sposób, aby każdy z podłączonych systemów backupowych mógł pracować na osobnym urządzeniu logicznym. Jeżeli	

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne	Spełnienie wymagane parametru: Tak/Nie
		do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.	
10	**Deduplikacja danych**	Urządzenie musi deduplikować dane inline przed zapisem na nośnik dyskowy. Technologia deduplikacji musi wykorzystywać algorytm bazujący na zmiennym, dynamicznym bloku. Algorytm ten musi samoczynnie i automatycznie dopasowywać się do otrzymywanego strumienia danych. Oznacza to, że urządzenie musi dzielić otrzymany pojedynczy strumień danych na bloki o różnej długości. Średnia wielkość bloku 4kB. Proces deduplikacji musi odbywać się inline – w pamięci urządzenia, przed zapisem danych na nośnik dyskowy. Rozwiązanie nie może w żadnej fazie korzystać (w całości lub częściowo) z dodatkowego bufora na składowanie danych w postaci oryginalnej (niezdeduplikowanej). Wszystkie unikalne, zdeduplikowane bloki przed zapisaniem na dysk muszą być kompresowane. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.	
11	**Replikacja danych**	Urządzenie musi umożliwiać replikację danych do drugiego urządzenia. Replikacja musi się odbywać w trybie asynchronicznym. Transmitowane muszą być tylko te fragmenty danych (bloki), które nie znajdują się na docelowym urządzeniu. W przypadku wykorzystania portów Ethernet do replikacji urządzenie musi umożliwiać przyjmowanie backupów, odtwarzanie danych, przyjmowanie strumienia replikacji, wysyłanie strumienia replikacji tymi samymi portami. Musi istnieć możliwość ograniczenia pasma używanego do replikacji między dwoma urządzeniami.	

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne	Spełnienie wymagane parametru: Tak/Nie
		Zarządzanie całym procesem kopiowania danych oraz wszystkimi kopiami musi być możliwe z poziomu oprogramowania backupowego. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, dostarczenie ich nie jest aktualnie wymagane.	
12	**Szyfrowanie danych**	Urządzenie musi mieć zaimplementowaną funkcjonalność wewnętrznego mechanizmu szyfrowania danych AES-256 realizowaną na poziomie urządzenia zgodnie ze standardem FIPS 140-2. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, dostarczenie ich nie jest aktualnie wymagane.	
13	**Usuwanie przeterminowanych danych**	Urządzenie musi automatycznie usuwać przeterminowane dane (bloki danych nienależące do backupów o aktualnej retencji) w procesie czyszczenia. Proces usuwania przeterminowanych danych (czyszczenia) nie może uniemożliwiać pracy procesów backupu i odtwarzania danych. Musi istnieć możliwość zdefiniowania czasu, w którym wykonywany jest proces usuwania przeterminowanych danych (czyszczenia).	
14	**Bezpieczne usuwanie danych**	Urządzenie musi umożliwiać bezpieczne kasowanie składowanych danych zgodnych ze standardem NIST SP 800-88. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, dostarczenie ich nie jest aktualnie wymagane.	
15	**Sposób zarządzania**	Urządzenie musi mieć możliwość zarządzania poprzez interfejs graficzny dostępny z przeglądarki internetowej oraz poprzez linię komend (CLI) dostępną z poziomu SSH (Secure Shell). Oprogramowanie do zarządzania musi rezydować oferowanym na urządzeniu deduplikacyjnym.	

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne	Spełnienie wymagane parametru: Tak/Nie
		Urządzenie musi umożliwiać ustawienie powiadomień administratora o problemach w urządzeniu za pomocą poczty elektronicznej.	
16	**Kompatybilność**	Urządzenie musi wspierać (wymagane formalne wsparcie producenta urządzenia) co najmniej następujące aplikacje backupujące bezpośrednio na oferowane urządzenie: EMC Networker, HPE Data Protector, IBM BRMS, IBM Spectrum Protect, Veeam, Veritas NetBackup, Microsoft SQL, Oracle RMAN, SAP i SAP HANA. W przypadku przyjmowania backupów od aplikacji: HPE Data Protector, Veeam, Veritas NetBackup, Microsoft SQL, Oracle RMAN, SAP/Oracle i SAP HANA urządzenie musi umożliwiać deduplikację na źródle i przesłanie tylko nowych, unikalnych bloków danych poprzez sieć FC i Ethernet.	
17	**Redundancja**	Redundantne zasilacze i wentylatory.	
18	**Gwarancja**	Wymagane 5 letnie wsparcie techniczne z możliwością zgłaszania problemów w dni robocze w godzinach 8-17 i z czasem reakcji w następnym dniu roboczym. Wsparcie musi obejmować wszystkie komponenty oferowanych urządzeń, nie dopuszcza się stosowania różnych poziomów wsparcia w zależności od tego jak krytyczny jest problem. Wsparcie musi być oferowane w języku polskim przez polski oddział serwisowy producenta.	
19	**Szkolenie**	Wykonawca zapewni autoryzowane szkolenie z w/w produktu dla min 2 os. trwające min. 3 dni, zapewniające certyfikat oraz niezbędną wiedzę umożliwiającą pracę z oferowanym produktem. Wszelkie koszty z tym związane leża po stronie Wykonawcy.	

- Rozbudowa macierzy dyskowych

Wymagana jest rozbudowa dwóch macierzy dyskowych HPE StoreServ 3PAR 7200

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne	Spełnienie wymaganego parametru: Tak/Nie
1	**Rozbudowa macierzy 3PAR1**	Wymagana rozbudowa posiadanej macierzy 3PAR 7200 o dodatkową półkę dyskową wyposażoną w minimum 24 dyski 3,5" o pojemości minimum 4TB każdy, dyski wyposażone w interfejs SAS i pracujące z prędkością obrotową minimum 7.2K wraz z licencjami na funkcjonalności posiadane przez macierz: • HPE 3PAR 7200 Replic SuiteDrive LTU Supp • HPE 3PAR 7200 OS Suite Drive LTU Support	
2	**Rozbudowa macierzy 3PAR2**	Wymagana rozbudowa posiadanej macierzy 3PAR 7200 o 12 dysków 3,5" o pojemości minimum 4TB każdy, dyski wyposażone w interfejs SAS i pracujące z prędkością obrotową minimum 7.2K wraz z licencjami na funkcjonalności posiadane przez macierz: • HPE 3PAR 7200 Replic SuiteDrive LTU Supp • HPE 3PAR 7200 OS Suite Drive LTU Support	
20	Wsparcie serwisowe	W ramach rozbudowy wymagane jest przedłużenie wsparcia serwisowego dla rozbudowywanych macierzy dyskowych HPE 3PAR 7200 o numerach seryjnych: CZ34241717, CZ34241716 oraz elementów rozbudowy do dnia 21.01.2023. Wsparcie techniczne z możliwością zgłaszania problemów w trybie 24/7 i z czasem reakcji maksymalnie do 4h. Wsparcie musi obejmować wszystkie komponenty oferowanych urządzeń, nie dopuszcza się stosowania różnych poziomów wsparcia w zależności od tego jak krytyczny jest problem. Wsparcie musi być oferowane w języku polskim przez polski oddział serwisowy producenta macierzy.	
		Wykonawca zapewni autoryzowane szkolenie z w/w produktu dla min 2 os. trwające min. 3 dni, zapewniające certyfikat oraz niezbędną wiedzę umożliwiającą pracę z oferowanym produktem.	

		Wszelkie koszty z tym związane leża po stronie Wykonawcy.	

- Oprogramowanie wirtualizacyjne

W ramach realizacji przedmiotowego zamówienia Wykonawca zobowiązany jest wykonać modernizację posiadanego przez Zamawiającego oprogramowania wirtualizacyjnego w skład którego wchodzą następujące licencje:

- VMware vSphere 5.5 Enterprise - sztuk 4
- VMware vSphere 5.5 Enterprise Plus - sztuk 6
- VMware vCenter 5.5 Standard – sztuk 1

Modernizacja oprogramowania musi zapewnić realizację funkcjonalności wymienionych w poniższej tabeli dla każdej z lokalizacji tj:

1. Lokalizacja 1 - w oparciu o dwa serwery dwu procesorowe
2. Lokalizacja 2 – w oparciu o dwa serwery dwu procesorowe

Nr	Wymagane minimalne parametry techniczne	Spełnienie wymaganego parametru: Tak/Nie
1.	Warstwa wirtualizacji musi być rozwiązaniem systemowym tzn. musi być zainstalowana bezpośrednio na sprzęcie fizycznym.	
2.	Rozwiązanie musi zapewnić możliwość obsługi wielu instancji systemów operacyjnych na jednym serwerze fizycznym i powinno się charakteryzować maksymalnym możliwym stopniem konsolidacji sprzętowej.	
3.	Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością dostępu do 6TB pamięci operacyjnej.	
4.	Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych do 128 procesorów wirtualnych każda z krokiem co jeden wirtualny procesor.	
5.	Rozwiązanie musi umożliwiać łatwą i szybką rozbudowę infrastruktury o nowe usługi bez spadku wydajności i dostępności pozostałych wybranych usług.	

6.	Rozwiązanie powinno w możliwie największym stopniu być niezależne od producenta platformy sprzętowej.	
7.	Rozwiązanie powinno wspierać następujące systemy operacyjne: Windows XP, Windows Vista, Windows 7, Windows 8, Windows Server 2003R2, Windows Server 2008, Windows Server 2008R2, SLES 12, SLES11, SLES10, RHEL 7, RHEL 6, RHEL 6, RHEL4, Solaris 11 x86, Solaris 10 x86, Debian, CentOS, FreeBSD, Asianux, Ubuntu, SCO OpenServer, SCO Unixware.	
8.	Rozwiązanie musi umożliwiać przydzielenie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera w celu osiągnięcia maksymalnego współczynnika konsolidacji.	
9.	Rozwiązanie musi umożliwiać przydzielenie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera w celu osiągnięcia maksymalnego współczynnika konsolidacji.	
10.	Rozwiązanie musi zapewnić możliwość monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej.	
11.	Oprogramowanie do wirtualizacji musi zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy.	
12.	Oprogramowanie do wirtualizacji musi zapewnić możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi.	
13.	Oprogramowanie zarządzające musi posiadać możliwość przydzielania i konfiguracji uprawnień z możliwością integracji z usługami katalogowymi Microsoft Active Directory.	
14.	Oprogramowanie do wirtualizacji musi obsługiwać przełączenie ścieżek SAN (bez utraty komunikacji) w przypadku awarii jednej z dwóch ścieżek.	
15.	Rozwiązanie musi umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych aniżeli fizycznie zarezerwowane.	
16.	System powinien posiadać funkcjonalność wirtualnego przełącznika (switch) umożliwiającego tworzenie sieci wirtualnej w obszarze hosta i pozwalającego połączyć maszyny wirtualne w obszarze jednego hosta.	
17.	Rozwiązanie musi zapewniać przenoszenie maszyn wirtualnych w czasie ich pracy pomiędzy serwerami fizycznymi.	

18.	Rozwiązanie musi zapewniać wysoką dostępność maszyn wirtualnych rozumianą jako automatyczne uruchomienie tych maszyn na innych serwerach fizycznych w razie awarii serwera fizycznego.	
19.	Rozwiązanie powinno umożliwiać łatwe i szybkie ponowne uruchomienie systemów/usług w przypadku awarii poszczególnych elementów infrastruktury.	
20.	Rozwiązanie musi zapewniać mechanizm bezpiecznego uaktualniania warstwy wirtualizacyjnej, hostowanych systemów operacyjnych (np. wgrywania patch-y) i aplikacji tak aby zminimalizować ryzyko awarii systemu na skutek wprowadzenia zamiany.	
21.	Rozwiązanie musi zapewnić możliwość szybkiego wykonywania kopii zapasowych oraz odtwarzania maszyn wirtualnych. Proces ten nie powinien mieć wpływu na utylizację zasobów fizycznych infrastruktury wirtualnej.	
22.	Rozwiązanie musi zapewniać pracę bez przestojów dla wybranych maszyn wirtualnych, niezależnie od systemu operacyjnego oraz aplikacji, podczas awarii serwerów fizycznych, bez utraty danych i dostępności danych podczas awarii serwerów fizycznych.	
23.	Rozwiązanie musi umożliwiać dodawanie i rozszerzanie dysków wirtualnych, procesorów i pamięci RAM podczas pracy wybranych maszyn wirtualnych.	
24.	Rozwiązanie musi zapewniać przenoszenie dysków maszyn wirtualnych pomiędzy różnymi zasobami dyskowymi serwera fizycznego bez powodowania przerw w pracy systemu wirtualnego.	
25.	Rozwiązanie powinno zapewnić możliwość szybkiego tworzenia i uruchamiania nowych maszyn wirtualnych wraz z ich pełną konfiguracją i preinstalowanymi narzędziami systemowymi w celu efektywnej obsługi wymagań biznesowych.	
26.	Oprogramowanie musi zapewniać funkcjonalność automatycznego równoważenia obciążenia serwerów fizycznych pracujących jak platforma dla infrastruktury wirtualnej. Nie jest wymagane dostarczenie licencji na opisaną funkcjonalność.	
27.	Oprogramowanie musi zapewnić migrację w trybie online (bez wyłączania maszyn wirtualnych) z obecnej platformy wykorzystywanej przez Zamawiającego opartej na rozwiązaniu VMware vSphere 5.5.	

28.	Rozwiązanie musi zapewniać przenoszenie maszyn wirtualnych w czasie ich pracy pomiędzy serwerami fizycznymi w obrębie lokalizacji 1 i 2, jak i pomiędzy lokalizacjami 1 i 2.	
29.	Wsparcie serwisowe na okres 5 lat zapewniające: • Obsługa zgłoszeń w dni robocze w trybie minimum 8-17. • Nielimitowana liczba zgłoszeń serwisowych. • Dostęp do aktualizacji oprogramowania. • Możliwość instalacji nowych wersji oprogramowania.	

- Oprogramowanie do zabezpieczenia środowiska wirtualizacyjnego

Należy dostarczyć licencje na oprogramowanie do zabezpieczenia środowiska wirtualnego spełniającego poniższe minimalne wymagania funkcjonalne.

Nr	Wymagane minimalne parametry techniczne	Spełnienie wymaganego parametru: Tak/Nie
1.	Wymagane jest dostarczenie licencji zapewniających zabezpieczenie środowiska wirtualnego pracującego na czterech serwerach dwuprocesorowych.	
2.	Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 4.1, 5.0, 5.1, 5.5, 6.0, 6.5 oraz Microsoft Hyper-V 2012 i 2012 R2. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej	
3.	Oprogramowanie musi współpracować z hostami zarządzanymi przez VMware vCenter oraz pojedynczymi hostami	
4.	Oprogramowanie musi współpracować z hostami zarządzanymi przez System Center Virtual Machine Manger, klastrami hostów oraz pojedynczymi hostami.	
5.	Oprogramowanie musi zapewniać tworzenie kopii zapasowych wszystkich systemów operacyjnych maszyn wirtualnych wspieranych przez vSphere i Hyper-V	
6.	Oprogramowanie musi być licencjonowanie w modelu “per-CPU”. Wszystkie funkcjonalności zawarte w tym dokumencie powinny być zapewnione w tej licencji. Jakiekolwiek dodatkowe licencjonowanie (per zabezpieczony TB, dodatkowo płatna deduplikacja) nie jest dozwolone	
7.	Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej	

8.	Oprogramowanie musi tworzyć “samowystarczalne” archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków	
9.	Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji	
10.	Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu.	
11.	Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania	
12.	Oprogramowanie musi zapewniać backup jednoprzebiegowy - nawet w przypadku wymagania granularnego odtworzenia	
13.	Oprogramowanie musi zapewniać mechanizmy informowania o wykonaniu/błędzie zadania poprzez email lub SNMP. W środowisku VMware musi mieć możliwość aktualizacji pola „notatki” na wirtualnej maszynie	
14.	Oprogramowanie musi mieć możliwość uruchamiania dowolnych skryptów przed i po zadaniu backupowym lub przed i po wykonaniu zadania snapshota w środowisku VMware.	
15.	Musi też umożliwiać odtwarzanie tych metadanych do vCD	
16.	Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji	
17.	Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji	
18.	Oprogramowanie musi wspierać backup maszyn wirtualych używających współdzielonych dysków VHDX na Hyper-V (shared VHDX)	
19.	Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.	
20.	Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych.	

	Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej	
21.	Oprogramowanie musi automatycznie wykrywać i usuwać snapshoty-sieroty (orphaned snapshots), które mogą zakłócić poprawne wykonanie backupu. Proces ten nie może wymagać interakcji administratora	
22.	Oprogramowanie musi wspierać kopiowanie plików na taśmy	
23.	Oprogramowanie musi mieć możliwość kopiowania backupów do lokalizacji zdalnej	
24.	Oprogramowanie musi mieć możliwość replikacji włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere, pomiędzy hostami ESXi, włączając asynchroniczną replikacją ciągłą. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji.	
25.	Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik	
26.	Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding)	
27.	Oprogramowanie musi posiadać takie same funkcjonalności replikacji dla Hyper-V	
28.	Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN)	
29.	Oprogramowanie musi dawać możliwość tworzenia backupów ad-hoc z konsoli jak i z klienta webowego vSphere	
30.	Oprogramowanie musi przetwarzać wiele wirtualnych dysków jednocześnie (parallel processing)	
31.	Oprogramowanie musi umożliwić uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana niezależnie od rodzaju storage'u użytego do przechowywania kopii zapasowych. Dla środowiska vSphere powinien być wykorzystany wbudowany w oprogramowanie serwer NFS. Dla Hyper-V powinna być zapewniona taka sama funkcjonalność realizowana wewnętrznymi mechanizmami oprogramowania	
32.	Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się	

	mechanizmami wbudowanymi w hypervisor. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie musi realizować jaką migrację swoimi mechanizmami.	
33.	Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków	
34.	Oprogramowanie musi umożliwić odtworzenie plików na maszynę operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików	
35.	Oprogramowanie musi mieć możliwość odtworzenia plików przy pomocy VMware VIX API	
36.	Oprogramowanie musi wspierać odtwarzanie plików z następujących systemów plików: • Linux - ext, ext2, ext3, ext4, ReiserFS (Reiser3), JFS, XFS, Btrfs • BSD - UFS, UFS2 • Solaris - ZFS • Mac - HFS, HFS+ • Windows - NTFS, FAT, FAT32, ReFS	
37.	Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM	
38.	Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej.	
39.	Oprogramowanie musi wspierać granularne odtwarzanie obiektów Active Directory włączając konta użytkowników i hasło. Funkcjonalność ta nie może wymagać pełnego odtworzenia wirtualnej maszyny ani jej uruchomienia.	
40.	Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2010 i nowszych. Funkcjonalność ta nie może wymagać pełnego odtworzenia wirtualnej maszyny ani jej uruchomienia.	
41.	Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2005 i nowsze. Funkcjonalność ta nie może wymagać pełnego odtworzenia wirtualnej maszyny ani jej uruchomienia.	
42.	Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2010 i nowsze. Funkcjonalność ta nie może wymagać pełnego odtworzenia wirtualnej maszyny ani jej uruchomienia.	

43.	Oprogramowanie musi indeksować pliki Windows i Linux w celu szybkiego wyszukiwania plików w plikach backupowych.	
44.	Oprogramowanie musi używać mechanizmów VSS wbudowanych w system operacyjny Microsoft Windows	
45.	Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN	
46.	Wymagana integracja z deduplikacyjną macierzą dyskową minimum mechanizmami: Dell EMC Data Domain Boost, HPE StoreOnce Catalyst, ExaGrid Accelerated Data Mover)	
47.	Dostarczone licencje muszą posiadać wsparcie producenta przez okres 5 lat. Wsparcie musi zapewniać możliwość aktualizacji oraz instalacji nowych wersji oprogramowania, dostęp do baz wiedzy i zgłaszanie problemów. Obsługa zgłoszeń w godzinach 8:00-20:00 w dni robocze.	
48.	Wykonawca zapewni autoryzowane szkolenie z w/w produktu dla min 2 os. trwające min. 3 dni, zapewniające certyfikat oraz niezbędną wiedzę umożliwiającą pracę z oferowanym produktem. Wszelkie koszty z tym związane leża po stronie Wykonawcy.	

- System operacyjny dla serwera backupu

W środowisku Zamawiającego funkcjonują usługi oparte o usługi katalogowe Active Directory oparte o systemy z rodziny Windows Server. Mając ten fakt na uwadze Wykonawca w ramach realizacji zamówienia dostarczy poniższe licencje systemowe:

Nr	Wymagane minimalne parametry techniczne	Spełnienie wymagane parametru: Tak/Nie
1.	WinSvrSTDCore 2016 OLP 16Lic NL Gov CoreLic – 1 szt.	
2.	Wykonawca zapewni autoryzowane szkolenie z w/w produktu dla min 2 os. trwające min. 3 dni, zapewniające certyfikat oraz niezbędną wiedzę umożliwiającą pracę z oferowanym produktem. Wszelkie koszty z tym związane leża po stronie Wykonawcy.	

- Rozbudowa obecnych przełączników rdzeniowych

Wymagane jest dostarczenie niżej wymienionych elementów do posiadanej przez Zamawiającego infrastruktury sieciowej.

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne	Spełnienie wymaganego parametru: Tak/Nie
1	**Rozbudowa przełączników HP 5500**	• Moduł HPE 5500/5120 2-port 10GbE SFP+ Module – sztuk 5 • Karta LAN 10Gb/s - HPE Ethernet 10Gb 2P 560SFP+ Adptr dla serwera HP DL380 Gen8 - sztuk 4 • Rozszerzenie ilości slotów w serwerze HP DL380 Gen8 (HP DL380p/560 G8 3Slot PCIe Rsr Kit) – sztuk 2	
2	**Wkładki SFP+ do przełączników HP 5500**	Wymagane jest dostarczenie 12 szt. wkładek 10Gb SFP+ LR kompatybilnych z przełącznikami HP 5500. Wymagane jest dostarczenie 16 szt. wkładek 10Gb SFP+ SR kompatybilnych z przełącznikami HP 5500.	
3	**Modernizacja traktu światłowodowego**	Wykonawca zrealizuje modernizację sześciu traktów światłowodowych na OM3 SM po ok. 100 m każdy w istniejących traktach światłowodowych.	

- Przełącznik dystrybucyjny

Wymagane dostarczenie 2 szt. przełączników dystrybucyjnych spełniających poniżej opisane minimalne parametry funkcjonalne.

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne	Spełnienie wymaganego parametru: Tak/Nie
1	Ilość portów	Przełącznik musi posiadać minimum 4 karty liniowe z następującymi portami: • Jedna karta 8 portów 1G/10GbE SFP+ • Trzy karty 20 portów 10/100/1000BASE-T PoE+, 4 porty SFP+	
2	Obudowa	Obudowa modularna z 6 slotami na karty liniowe, wysokość maksymalna 4U	
3	Rozmiar tablicy adresów MAC	Minimum 64000 pozycji	

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne	Spełnienie wymaganego parametru: Tak/Nie
4	Rozmiar tablicy Routingu	10000 (IPv4), 5000 (IPv6)	
5	Pamięć	Minimum 4GB DDR3 SDRAM; Pamięć nieulotna minimum 1GB	
6	Zarządzanie	CLI, WWW, telnet, poza pasmowe (port szeregowy RS-232C/USB), przypisywanie dowolnych nazw dla portów, Multiple configuration files, dual flash images	
7	Warstwa przełączania	2, 3, 4	
8	Funkcje warstwy 3	static IP routing, RIPv1, RIPv2, OSPF, routing multicastów PIM Sparse/Dense, BGP, Policy Based Routing, Route Maps	
9	Przepustowość rutowania /przełączania	Minimum 960 Gbps	
10	Prędkość matrycy przełączającej	Minimum 1000 Gbps	
11	Przepustowość	Minimum 571,4 Mpps	
12	Opóźnienia	Opóźnienie 1000 Mb: maksymalnie 2,8 µs (FIFO 64-byte packets), Opóźnienie 10 Gb/s: maksymalnie 1,8 µs (FIFO 64-byte packets)	
13	Ilość obsługiwanych VLAN-ów	Minimalnie. 2048 (802.1q) wsparcie dla QinQ	
14	Funkcje wysokiej dostępności	Spanning Tree (802.1d), Rapid Convergence Spanning Tree (802.1w), Muliple Spanning Tree (802.1s), VRRP	
16	Bezpieczeństwo	Radius/TACACS+,DHCP Protection, SNMPv3, SSL, SSHv2, 802.1x (możliwość jednoczesnej autentykacji dwoma sposobami np. 802.1x oraz MAC lub 802.1x lub WWW, obsługa do 32 autentykowanych stacji na jednym porcie, wsparcie dla voice vlanów), Access control lists (ACLs), Identity-driven ACL, DHCP Snooping, Dynamic ARP Protection, BPDU Protection,	

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne	Spełnienie wymaganego parametru: Tak/Nie
		Dynamic IP Lockdown, MAC adres lockout, Secure FTP, USB Secure Autorun	
16	Auto MDIX	autonegocjacja prędkości, duplex-u oraz połączenia (MDI/MDIX)	
17	Agregacja portów	zgodna z 802.3ad LACP	
18	QoS	prioryteryzacja zgodna z 802.1p, ToS, TCP/UDP, DiffServ; klasyfikacja ruchu w czasie rzeczywistym na 8 poziomów priorytetów, odwzorowanych w postaci 8 kolejek; stosuje reguły jakości usług, między innymi ustalanie poziomu priorytetu i ograniczanie ruchu, do ruchu w wybranym porcie lub VLAN, kształtowanie pasma	
19	Monitorowanie	RMON, XRMON 4 grupy statistics, history, alarm, events, SFLOW, zdalny port mirroring poprzez tunel UDP (możliwość śledzenia całego portu, w oparciu o vlan bądź ACL); Uni-Directional Link Detection (UDLD) - monitorowanie przewodu, jeśli kabel jest uszkodzony obraca łącze dwukierunkowe w jednokierunkowe	
20	Oprogramowanie	Aktualizacje dostępne na stronie producenta.	
21	Pozostałe funkcje	LLDP,LLDP-MED, dual flash images, CPU protection, Virus Throttling, ICMP throttling, obsługa ramek typu Jumbo, support OpenFlow 1.0 i 1.3, Smart Link, RPVST+	
22	Zasilanie wewnętrzne	Dwa oryginalne zasilacze 230V AC do wyżej wymienionego przełącznika o mocy minimum 1100W każdy posiadający wsparcie dla funkcjonalności PoE+.	
23	Wsparcie serwisowe	Wymagana dożywotnia gwarancja producenta, obowiązująca przez cały okres posiadania urządzeń przez Zamawiającego, wymiana następnego dnia roboczego na sprawne urządzenie. Wsparcie musi obejmować wszystkie komponenty oferowanych urządzeń, nie dopuszcza się stosowania różnych poziomów wsparcia w zależności od tego jak krytyczny jest problem. Wsparcie musi być oferowane w języku polskim przez polski oddział serwisowy producenta. Urządzenie musi pochodzić z legalnego źródła,	

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne	Spełnienie wymaganego parametru: Tak/Nie
		zakupione w autoryzowanym kanale sprzedaży producenta w Polsce.	
24	Szkolenie	Wykonawca zapewni autoryzowane szkolenie z w/w produktu dla min 2 os. trwające min. 3 dni, zapewniające certyfikat oraz niezbędną wiedzę umożliwiającą pracę z oferowanym produktem. Wszelkie koszty z tym związane leża po stronie Wykonawcy.	

Wraz z przełącznikami dystrybucyjnymi wymagane jest dostarczenie wkładek światłowodowych SFP+ spełniających poniżej opisane minimalne parametry funkcjonalne.

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne	Spełnienie wymaganego parametru: Tak/Nie
1	Wkładki FO typu SFP+ SM	• 40 sztuk - wkładka (Transceiver) typu SFP+ umożliwiająca transmisję z prędkością 10Gb, kompatybilna z portami w karcie liniowej dostarczonego przełącznika i umożliwiająca transmisję do 10 km przez jednomodowe łącze światłowodowe. • 4 sztuk - wkładka (Transceiver) typu SFP+ umożliwiająca transmisję z prędkością 10Gb, kompatybilna z portami w karcie liniowej dostarczonego 300m przez wielomodowe łącze światłowodowe.	
2	Gwarancja	Minimum 24 miesiące	

- Przełącznik dostępowy

Wymagane dostarczenie 8 szt. przełączników dostępowych spełniających poniżej opisane minimalne parametry funkcjonalne.

Lp.	Wymagane minimalne parametry techniczne	Spełnienie wymaganego parametru: Tak/Nie
1.	Minimum 48 portów gigabitowych w standardzie 100/1000BaseT ze wsparciem dla standardu 802.3at (PoE+)	

2.	Minimum 4 porty 10Gb SFP+, pozwalające na instalację wkładek 10Gb (SFP+) i Gigabitowych (SFP).	
3.	Przepustowość: minimum 176 Gb/s	
4.	Wydajność: minimum 112 Mp/s	
5.	Tablica adresów MAC o wielkości minimum 32000 pozycji	
6.	Obsługa ramek Jumbo	
7.	Routing IPv4 – minimum: statyczny, RIPv2, OSPF	
8.	Routing IPv6 – minimum: statyczny, RIPng, OSPFv3	
9.	Wielkość tablicy rutingu: minimum 10000 wpisów dla IPv4, 5000 wpisów dla IPv6	
10.	Obsługa ruchu Multicast: IGMP Snooping; MLD Snooping	
11.	Obsługa VxLAN	
12.	Obsługa IEEE 802.1s Multiple SpanningTree / MSTP oraz IEEE 802.1w Rapid Spanning Tree Protocol	
13.	Obsługa 4094 tagów IEEE 802.1Q oraz minimum 2000 jednoczesnych sieci VLAN	
14.	Funkcja Root Guard oraz BPDU protection	
15.	Przełączniki tego samego typu muszą posiadać funkcję łączenia w stos (wirtualny przełącznik) złożony z minimum 4 urządzeń. Zarządzanie stosem musi odbywać się z jednego adresu IP. Z punktu widzenia zarządzania przełączniki muszą tworzyć jedno logiczne urządzenie (nie dopuszcza się rozwiązań typu klaster).	
16.	Realizacja łączy agregowanych (LACP) w ramach różnych przełączników będących w stosie	
17.	Wsparcie dla funkcji DHCP server, DHCP Relay oraz DHCP Snooping (wszystkie dla IPv4 i IPv6)	
18.	Obsługa list ACL na bazie informacji z warstw 2/3/4 modelu OSI	
19.	Obsługa standardu 802.1p – min. 8 kolejek na porcie	
20.	Funkcja mirroringu portów	
21.	Obsługa IEEE 802.1AB Link Layer Discovery Protocol (LLDP) i LLDP Media Endpoint Discovery (LLDP-MED)	
22.	Funkcja autoryzacji użytkowników zgodna z 802.1x	
23.	Funkcja autoryzacji logowania do urządzenia za pomocą serwerów RADIUS albo TACACS+	
24.	RADIUS Accounting	
25.	Wsparcie dla protokołu OpenFlow w wersji 1.0 oraz 1.3	
26.	OpenFlow musi posiadać możliwość konfiguracji przetwarzania pakietów przez przełącznik w oparciu o ciąg tablic.	

27.	Musi być możliwe wielotablicowe przetwarzanie zapytań OpenFlow zawierająca następujące tablice do przetwarzania reguł sprzętowo w oparciu o: źródłowe i docelowe adresy MAC, źródłowy i docelowy adres IP oraz nr portu, numer portu wejściowego (pole IP DSCP oraz VLAN PCP)	
28.	Musi być możliwe przypisywanie więcej niż jednej akcji zadanemu wpisowi OpenFlow.	
29.	Musi być możliwe tworzenie logicznych tuneli poprzez komunikaty SNMP i możliwość ich wykorzystania w kierowaniu ruchem w sposób sterowany za pomocą protokołu OpenFlow.	
30.	Wsparcie dla Energy-efficient Ethernet (EEE) IEEE 802.3az	
31.	Zarządzanie poprzez port konsoli (pełne), SNMP v.1, 2c i 3, Telnet, SSH v.2, http i https	
32.	Syslog	
33.	SNTPv4	
34.	Musi być możliwość przechowywania co najmniej dwóch wersji oprogramowania na przełączniku	
35.	Musi być możliwość przechowywania co najmniej trzech plików konfiguracyjnych na przełączniku, możliwość wgrywania i zgrywania pliku konfiguracyjnego w postaci tekstowej do stacji roboczej	
36.	Wsparcie dla funkcji Private VLAN lub równoważnego	
37.	Obsługa mechanizmu wykrywania łączy jednokierunkowych typu Uni-Directional Link Detection (UDLD), Device Link Detection Protocol (DLDP) lub równoważnego	
38.	Minimalny zakres pracy od 0°C do 45°C	
39.	Wysokość w szafie 19” – 1U, głębokość nie większa niż 32 cm	
40.	Wewnętrzny zasilacz 230V zapewniający budżet mocy PoE na poziomie nie niższym niż 370W	
41.	Maksymalny pobór mocy (bez PoE) nie większy niż 100W	
42.	Wymagana dożywotnia gwarancja producenta, obowiązująca przez cały okres posiadania urządzeń przez Zamawiającego, wymiana następnego dnia roboczego na sprawne urządzenie. Wsparcie musi obejmować wszystkie komponenty oferowanych urządzeń, nie dopuszcza się stosowania różnych poziomów wsparcia w zależności od tego jak krytyczny jest problem. Wsparcie musi być oferowane w języku polskim przez polski oddział serwisowy producenta. Urządzenie musi pochodzić z legalnego źródła, zakupione w autoryzowanym kanale sprzedaży producenta w Polsce.	

43.	Wykonawca zapewni autoryzowane szkolenie z w/w produktu dla min 2 os. trwające min. 3 dni, zapewniające certyfikat oraz niezbędną wiedzę umożliwiającą pracę z oferowanym produktem. Wszelkie koszty z tym związane leżą po stronie Wykonawcy.	

Wraz z przełącznikami dostępowymi wymagane jest dostarczenie wkładek światłowodowych SFP+ spełniających poniżej opisane minimalne parametry funkcjonalne.

Lp.	**Nazwa komponentu**	**Wymagane minimalne parametry techniczne**	Spełnienie wymaganego parametru: Tak/Nie
1	Wkładki FO typu SFP+ SM	• 32 sztuki - wkładka (Transceiver) typu SFP+ umożliwiająca transmisję z prędkością 10Gb, kompatybilna z portami w karcie liniowej dostarczonego przełącznika i umożliwiająca transmisję do 10 km przez jednomodowe łącze światłowodowe.	
2	Gwarancja	Minimum 24 miesiące	

- Zakres usług

W ramach postępowania wymagane jest wykonanie następujących usług:

Instalacja fizyczna dostarczonego sprzętu

1. Przygotowanie planu instalacji.
    - Zestawienie dostarczanych urządzeń.
    - Propozycję rozmieszczenia elementów w istniejących szafach rackowych.
    - Propozycję testów odbiorczych.
2. Instalacja, montaż i uruchomienie serwerów wirtualizacyjnych
    - Montaż serwera w istniejącej szafie rackowej.
    - Podłączenie serwera do sieci LAN oraz SAN.
    - Podłączenie serwera do zasilania.
    - Inicjalne uruchomienie serwera.
    - Testy działania serwera oraz weryfikacja parametrów.
3. Instalacja, montaż i uruchomienie infrastruktury backupowej
    - Montaż urządzeń w istniejącej szafie rackowej.
    - Podłączenie urządzeń do sieci LAN oraz SAN.
    - Podłączenie urządzeń do zasilania.

- Inicjalne uruchomienie urządzeń.
- Testy działania oraz weryfikacja parametrów.

4. Instalacja, montaż i rozbudowa macierzy dyskowych
    - Montaż dodatkowych półek dyskowych oraz dysków w macierzach
    - Testy działania macierzy oraz weryfikacja parametrów.
5. Instalacja, montaż i uruchomienie przełączników dystrybucyjnych i dostępowych
    - Montaż przełączników w szafie rackowej
    - Podłączenie przełączników do sieci LAN.
    - Inicjalne uruchomienie przełączników.
    - Testy działania przełączników oraz weryfikacja parametrów.
6. Rozbudowa serwerów DL380 Gen8
7. Rozbudowa przełączników SAN
8. Rozbudowa przełączników HP 5500

Konfiguracja macierzy dyskowych

1. Przygotowanie planu rozbudowy.
    - Zestawienie stosowanej nomenklatury.
    - Zestawienie serwerów, które będą korzystać z wystawianych zasobów.
    - Weryfikacja poziomów mikrokodów.
    - Zestawienie wymaganych wersji oprogramowania / łat systemowych po stronie serwerów.
    - Przygotowanie szczegółowej koncepcji konfiguracji dysków macierzy odzwierciedlającej potrzeby biznesowe.
    - Zestawienie zakupionego oprogramowania.
    - Propozycja testów odbiorczych.
2. Implementacja zgodna z projektem.
    - Instalacja sprzętowa.
    - Aktywacja zakupionego oprogramowania.
    - Konfiguracja replikacji synchronicznej
    - Implementacja zaakceptowanej konfiguracji logicznej macierzy.
3. Testy odbiorcze.
    - Zestawienie stosowanej nomenklatury.
    - Weryfikację zgodności z planem wdrożenia.
    - Przeprowadzenie testów potwierdzających poprawność instalacji macierzy.
4. Przygotowanie dokumentacji powykonawczej.
    - Zestawienie stosowanej nomenklatury.
    - Zestawienie serwerów korzystających z wystawianych zasobów.

- Zestawienie poziomów mikrokodów.
- Zestawienie wymaganych wersji oprogramowania / łat systemowych po stronie serwerów.
- Zestawienie konfiguracji dysków macierzy .
- Zestawienie mapowania udostępnionych zasobów.
- Zestawienie zakupionego i aktywowanego oprogramowania.
- Definicje testów odbiorczych.

Konfiguracja sieci SAN

1. Inwentaryzacja stanu obecnego.
    - Rysunki połączeń logicznych istniejących urządzeń.
    - Zestawienie nazewnictwa poszczególnych istniejących urządzeń, stref (o ile ma to zastosowanie).
    - Definicje poszczególnych stref (o ile ma to zastosowanie).
    - Rysunki połączeń fizycznych ze wskazaniem portów w urządzeniach.
    - Tabelaryczne zestawienie oznaczeń połączeń fizycznych.
    - Tabelaryczne zestawienie połączeń ze wskazaniem identyfikatorów WWN odpowiednich portów.
    - Tabelaryczne zestawienie parametrów konfiguracyjnych stosowanych przełączników
    - Zestawienie wersji oprogramowania wbudowanego przełączników FC
    - Zestawienie oznaczeń połączeń fizycznych.
2. Przygotowanie projektu technicznego.
    - Zestawienie stosowanej nomenklatury.
    - Rysunki połączeń logicznych objętych urządzeń z uwzględnieniem istniejących urządzeń i zaznaczeniem koniecznych zmian/przepięć.
    - Propozycję nazewnictwa poszczególnych urządzeń, stref (o ile ma to zastosowanie)
    - Definicje poszczególnych stref (o ile ma to zastosowanie).
    - Rysunki połączeń fizycznych ze wskazaniem portów w urządzeniach (z uwzględnieniem istniejących połączeń) i z oznaczeniem koniecznych zmian/przepięć.
    - Propozycję oznaczeń połączeń fizycznych.
    - Zestawienie wymagań odnośnie wersji oprogramowania wbudowanego przełączników FC.
    - Zestawienie wymagań odnośnie konfiguracji urządzeń podłączanych do sieci SAN.
    - Propozycję testów odbiorczych.
3. Przeprowadzenie testów odbiorczych.
    - Zestawienie stosowanej nomenklatury.

- Weryfikację zgodności konfiguracji poszczególnych urządzeń z projektem technicznym.
- Weryfikację zgodności połączeń fizycznych z projektem technicznym.
- Weryfikację zgodności przyjętych oznaczeń połączeń fizycznych z projektem technicznym.
- Weryfikację dostępności zasobów udostępnionych w sieci SAN.

4. Przygotowanie dokumentacji powykonawczej.
    - Zestawienie stosowanej nomenklatury.
    - Rysunki połączeń logicznych objętych urządzeń.
    - Tabelaryczne zestawienie nazewnictwa poszczególnych urządzeń, stref (o ile ma to zastosowanie).
    - Definicje poszczególnych stref (o ile ma to zastosowanie).
    - Rysunki połączeń fizycznych ze wskazaniem odpowiednich portów w odpowiednich urządzeniach.
    - Tabelaryczne zestawienie oznaczeń połączeń fizycznych.
    - Tabelaryczne zestawienie połączeń ze wskazaniem identyfikatorów WWN odpowiednich portów.
    - Tabelaryczne zestawienie parametrów konfiguracyjnych stosowanych przełączników.
    - Zestawienie wersji oprogramowania wbudowanego przełączników FC.
    - Zestawienie wymagań odnośnie konfiguracji urządzeń podłączanych do sieci SAN.

Konfiguracja sieci LAN

1. Analiza przedwdrożeniowa
2. Koncepcja rozwiązania sieci LAN
3. Przeanalizowanie adresacji sieci LAN
4. Konfiguracja dostarczanych przełączników, w skład której wejdzie:
    - konfiguracja ACL,
    - konfiguracja urządzenia umożliwiająca dostęp poprzez SSH i HTTPS,
    - konfiguracja protokołu trasowania
    - aktualizacja oprogramowania na wszystkich urządzeniach sieciowych dostarczonych jak i obecnie posiadanych (jeżeli będą takie przeciwskazania)
    - konfiguracja SNMP
    - konfiguracja redundancji na przełącznikach w rdzeniu sieci
    - konfiguracja STP na przełącznikach
5. Wykonanie dokumentacji powykonawczej dla dostarczanej infrastruktury LAN
6. Podłączenie przełączników do systemu zarządzania

Instalacja i konfiguracja oprogramowania do wykonywania kopii bezpieczeństwa .

1. Inwentaryzacja stanu obecnego.
    - Zestawienie nazewnictwa poszczególnych elementów istniejącego systemu.
    - Zestawienie zainstalowanych łat systemu operacyjnego.
    - Zestawienie zainstalowanych wersji oprogramowania.
    - Zestawienie istniejących konfiguracji poszczególnych rozszerzeń systemu (o ile ma to zastosowanie).
2. Przygotowanie projektu technicznego.
    - Zestawienie stosowanej nomenklatury.
    - Rysunki logicznej struktury systemu wykonywania kopii zapasowych.
    - Propozycję nazewnictwa poszczególnych elementów systemu.
    - Zestawienie wymaganych łat systemu operacyjnego (ang. Patch Management).
    - Zestawienie wymaganych wersji oprogramowania.
    - Propozycje konfiguracji systemu wykonywania kopii bezpieczeństwa.
    - Zestawienie propozycji konfiguracji poszczególnych rozszerzeń systemu.
    - Propozycję testów odbiorczych.
3. Implementacja zgodna z przyjętym projektem.
    - Instalacja licencji.
    - Konfiguracja systemu z uwzględnieniem pracy w dwóch lokalizacjach.
4. Przeprowadzenie testów odbiorczych. Winny obejmować:
    - Zestawienie stosowanej nomenklatury.
    - Weryfikację zgodności konfiguracji poszczególnych elementów systemu z projektem
    - Weryfikację poprawności wykonania kopii zapasowych zgodnie z podstawową konfiguracją jak również w ramach każdego ze scenariuszy opcjonalnych (związanych ze konfigurowanymi rozszerzeniami).
5. Przygotowanie dokumentacji powykonawczej. Winna zawierać:
    - Zestawienie stosowanej nomenklatury.
    - Rysunki logicznej struktury systemu wykonywania kopii zapasowych.
    - Zestawienie nazewnictwa poszczególnych elementów systemu.
    - Zestawienie zainstalowanych łat systemu operacyjnego (ang. Patch Management)
    - Zestawienie wersji zainstalowanego oprogramowania.
    - Zestawienie konfiguracji systemu wykonywania kopii bezpieczeństwa.
    - Zestawienie konfiguracji poszczególnych rozszerzeń systemu (o ile ma to zastosowanie).
    - Procedury backupowe (stworzenie, dodanie)
    - Test backupu

Aktualizacja oraz instalacja oprogramowania wirtualizacyjnego

1. Inwentaryzacja stanu obecnego.
    - Zestawienie nazewnictwa poszczególnych elementów istniejącego systemu.
    - Zestawienie zainstalowanych łat systemu operacyjnego.
    - Zestawienie zainstalowanych wersji oprogramowania.
    - Zestawienie istniejących konfiguracji poszczególnych rozszerzeń systemu (o ile ma to zastosowanie).
2. Przygotowanie projektu technicznego.
    - Zestawienie stosowanej nomenklatury.
    - Rysunki logicznej struktury systemu.
    - Propozycję nazewnictwa poszczególnych elementów systemu wirtualizacji.
    - Zestawienie wymaganych łat systemu operacyjnego (ang. Patch Management).
    - Zestawienie wymaganych wersji oprogramowania.
    - Propozycje konfiguracji systemu wirtualizacji.
    - Zestawienie propozycji konfiguracji poszczególnych rozszerzeń systemu.
    - Propozycję testów odbiorczych.
3. Implementacja zgodna z przyjętym projektem.
    - Instalacja oprogramowania wirtualizacyjnego.
    - Konfiguracja oprogramowania wirtualizacyjnego.
    - Aktywacja zakupionego oprogramowania.
4. Przeprowadzenie testów odbiorczych. Winny obejmować:
    - Zestawienie stosowanej nomenklatury.
    - Weryfikację zgodności konfiguracji poszczególnych elementów systemu z projektem.
5. Przygotowanie dokumentacji powykonawczej. Winna zawierać:
    - Zestawienie stosowanej nomenklatury.
    - Rysunki logicznej struktury systemu wirtualizacji.
    - Zestawienie nazewnictwa poszczególnych elementów systemu.
    - Zestawienie konfiguracji systemu wirtualizacji.
    - Zestawienie zainstalowanych łat systemu operacyjnego (ang. Patch Management)
    - Zestawienie wersji zainstalowanego oprogramowania.
    - Opracowanie scenariuszy przełączania systemów.

Inne.

1. Przygotowanie całościowej analizy przedwdrożeniowej
   a. Analizę przedwdrożeniową obecnego stanu usług.
2. Modyfikacja m.in. usług katalogowych, dns, mail, dhcp, radiusa z wykorzystaniem wdrażanego sprzętu.
3. Wdrożenie Vlanów-według sugestii Zamawiającego

Pakiet nr 2.

Dostawa sprzętu komputerowego.

L.p.	Rodzaj	Producent/typ/ model	ILOŚĆ	Cena netto	Wartość netto	Podatek VAT	Wartość brutto
1	Zestaw komputerowy		70				
2	Monitor		70				
3	Laptop typ 1		30			----------	----------
4	Laptop typ 2		2			----------	----------
5	Tablet typ 1		2			----------	----------
6	Zestaw komputerowy typ 2		5				
7	Drukarka ze skanerem		30				
8	Oprogramowanie biurowe		10				
Razem:							

Cenę oferty, należy ustalić w złotych polskich z dokładnością do dwóch miejsc po przecinku, w następujący sposób:

1) Wykonawca określi ceny jednostkowe brutto na wszystkie pozycje asortymentowe (za wyjątkiem laptopów i tabletów, dla których Wykonawca poda tylko ceny netto),

2) Wykonawca zliczy i poda wartość brutto za całość zamawianego asortymentu – tak wyliczona kwota brutto będzie stanowić cenę oferty. Zamawiający doliczy do podanych cen netto laptopów i tabletów podatek VAT, następnie zsumuje otrzymane ceny brutto dla laptopów i tabletów z podanymi cenami brutto dla pozostałego asortymentu i otrzymaną ogólną kwotę brutto przyjmie do oceny ofert.

Opis przedmiotu zamówienia:

- Zestawy komputerowe szt. 70

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne	Spełnienie wymaganeg parametru: Tak/Nie
1	**Typ**	Komputer stacjonarny	
2	**Zastosowanie**	Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, dostęp do systemów dziedzinowych, stacja programistyczna	
3	**Wydajność obliczeniowa**	Procesor klasy x86, zaprojektowany do pracy w komputerach stacjonarnych, osiągający w teście Passmark CPU Mark wynik min.: 7400 punktów (wynik zaproponowanego procesora musi znajdować się na stronie http://www.cpubenchmark.net).	
4	**Pamięć operacyjna**	Min. 8GB DDR4 min. przepustowość 17GB/s możliwość rozbudowy do min. 32GB	
5	**Parametry pamięci masowej**	Min. 1 TB SATA III, min. 7200 obr./min, zawierający partycję RECOVERY umożliwiającą odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii bez dodatkowych nośników.	
6	**Wydajność grafiki**	Grafika zintegrowana z procesorem powinna umożliwiać pracę dwumonitorową ze wsparciem dla DirectX 12, Open CL 2.0, Open GL 4.4, Shader 5.1 – z możliwością dynamicznego przydzielenia do 1 GB pamięci	

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne	Spełnienie wymaganeg parametru: Tak/Nie
7	**Wyposażenie multimedialne**	Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition	
8	**Obudowa**	• Typu SFF z obsługą kart PCI Express wyłącznie o niskim profilu profilu, wyposażona w min: 1 szt. 3,5” zewnętrzna. • Zasilacz pracujący w sieci 230V 50/60Hz prądu zmiennego i efektywności min. 85%, przy 50% obciążeniu. • W celu szybkiej weryfikacji usterki w obudowę komputera musi być wbudowany akustyczny system diagnostyczny, służący do sygnalizowania i diagnozowania problemów z komputerem i jego komponentami;	
9	**System operacyjny**	Microsoft Windows 10 Professional 64 PL lub system równoważny oraz zestaw płyt umożliwiający przywrócenie systemu. System równoważny powinien posiadać następujące cechy: 1. wsparcie dla architektury 32 i 64 bitowej, 2. obsługa procesorów wielordzeniowych, 3. graficzny okienkowy interfejs użytkownika, 4. obsługa co najmniej 8 GB RAM, 5. pełna obsługa sprzętu będącego przedmiotem zamówienia (kompatybilność sterowników, w tym sterowników do urządzeń peryferyjnych), 6. współpraca z Active Directory, możliwość pracy sieciowej, 7. możliwość darmowej aktualizacji poprzez sieć, posiadający wsparcie pomocy technicznej producenta.	

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne	Spełnienie wymaganeg parametru: Tak/Nie
	Porty	4 x USB 3.0 6 x USB 2.0 1 x wejście liniowe 1 x wyjście liniowe 1 x wyjście na słuchawki 1 x wejście na mikrofon 1 x RJ-45 (LAN) 1 x DVI-D 1 x DisplayPort 2 x PS/2 Dodatkowe informacje o portach USB 2.0/3.0/3.1 2 x USB 2.0 (przedni panel) 2 x USB 3.0 (przedni panel) 2 x USB 2.0 (tylny panel) 2 x USB 3.0 (tylny panel) 2 x USB 2.0 (wewnętrzny)	
10	**Certyfikaty i standardy**	• Certyfikat ISO9001:2000 dla producenta sprzętu • Certyfikat ISO 14001 dla producenta sprzętu • Certyfikat EnergyStar 5.0 • z jednoczesnym dopuszczeniem możliwości składania dokumentów równoważnych, czyli wydawanych przez podmiot uprawniony do kontroli jakości w zakresie usług lub dostawy będącej przedmiotem zamówienie • Deklaracja zgodności oferowanego sprzętu z wymaganiami zasadniczymi (Deklaracja CE)	
11	**Ergonomia**	• Głośność jednostki centralnej mierzona zgodnie z normą ISO 7779 oraz wykazana zgodnie z normą ISO 9296 z jednoczesnym dopuszczeniem	

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne	Spełnienie wymaganeg parametru: Tak/Nie
		możliwości składania dokumentów równoważnych, czyli wydawanych przez podmiot uprawniony do kontroli jakości w zakresie usług lub dostawy będącej przedmiotem zamówienie, w pozycji obserwatora w trybie jałowym (IDLE) wynosząca maksymalnie 20 dB • Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej lub kłódki (oczko w obudowie do założenia kłódki). • Suma wymiarów obudowy (wysokość + szerokość + głębokość mierzona po krawędziach zewnętrznych) nie może wynosić więcej niż 800 mm.	

13	**Bezpieczeństwo**	BIOS musi posiadać następujące cechy:
		• Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o:
		  • wersji BIOS,
		  • ilości i sposobu obłożenia slotów pamięciami RAM,
		  • typie procesora wraz z informacją o ilości rdzeni, wielkości pamięci cache L1, L2 i L3, pojemności zainstalowanego dysku twardego
		  • rodzajach napędów optycznych
		  • MAC adresie zintegrowanej karty sieciowej
		  • kontrolerze audio
		• Funkcja blokowania wejścia do BIOS oraz blokowania startu systemu operacyjnego, (gwarantujący utrzymanie zapisanego hasła nawet w przypadku odłączenia wszystkich źródeł zasilania i podtrzymania BIOS)
		• Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z zewnętrznych urządzeń
		• Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych, ustawienia hasła na poziomie systemu, administratora oraz dysku twardego oraz możliwość ustawienia następujących zależności pomiędzy nimi: brak możliwości zmiany hasła pozwalającego na uruchomienie systemu bez podania hasła administratora.	

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne	Spełnienie wymaganeg parametru: Tak/Nie
		• Musi posiadać możliwość ustawienia zależności pomiędzy hasłem administratora a hasłem systemowy tak, aby nie było możliwe wprowadzenie zmian w BIOS wyłącznie po podaniu hasła systemowego. • Możliwość włączenia/wyłączenia zintegrowanej karty dźwiękowej, karty sieciowej z poziomu BIOS, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych. • Możliwość ustawienia portów USB w trybie „no BOOT", czyli podczas startu komputer nie wykrywa urządzeń bootujących typu USB, natomiast po uruchomieniu systemu operacyjnego porty USB są aktywne. • Możliwość wyłączania portów USB w tym: wszystkich portów, tylko portów znajdujących się na przedzie obudowy, tylko tylnich portów.	
15	**Warunki gwarancji**	Min. 3-letnia gwarancja producenta świadczona na miejscu u klienta. Przyjmowanie zgłoszeń w dni robocze w godzinach 8:00-16:00 telefonicznie, e-mail. Gwarantowany czas reakcji serwisu – max. następny dzień roboczy. W przypadku naprawy przekraczającej jeden dzień roboczy wymagane dostarczenie w tym samym dniu urządzenia zastępczego do czasu zakończenia naprawy. Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta komputera. Serwis urządzeń musi być realizowany przez producenta lub autoryzowanego partnera serwisowego producenta – wymagane dołączenie do oferty oświadczenia podmiotu realizującego serwis lub producenta sprzętu o spełnieniu tego warunku.	
16	**Wsparcie techniczne**	Ogólnopolska, telefoniczna infolinia/linia techniczna producenta komputera, (ogólnopolski numer o zredukowanej odpłatności 0-800/0-801 – w ofercie należy podać numer telefonu) dostępna w czasie	

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne	Spełnienie wymaganeg parametru: Tak/Nie
		obowiązywania gwarancji na sprzęt i umożliwiająca po podaniu numeru seryjnego urządzenia: a) weryfikację konfiguracji fabrycznej wraz z wersją fabrycznie dostarczonego oprogramowania (system operacyjny, szczegółowa konfiguracja sprzętowa - CPU, HDD, pamięć) b) czasu obowiązywania i typ udzielonej gwarancji Możliwość aktualizacji i pobrania sterowników do oferowanego modelu komputera w najnowszych certyfikowanych wersjach przy użyciu dedykowanego darmowego oprogramowania producenta lub bezpośrednio z sieci Internet za pośrednictwem strony www producenta komputera po podaniu numeru seryjnego komputera lub modelu komputera. Możliwość weryfikacji czasu obowiązywania i reżimu gwarancji bezpośrednio z sieci Internet za pośrednictwem strony www producenta komputera	
17	**Inne**	Patchcord UTP min 3m	

- MONITOR – 70 szt.

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne	Spełnienie wymaganego parametru: Tak/Nie
1	**Typ ekranu**	Panoramiczny, ciekłokrystaliczny z aktywną matrycą min. 22” z podświetlaniem LED	
2	**Jasność**	min. 250 cd/m2	
3	**Kontrast dynamiczny**	min. 1000:1	
4	**Kąty widzenia**	min. 178°/178° (pion/poziom)	
5	**Czas reakcji matrycy**	max 5ms	
6	**Kolory**	min. 16.7mln	

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne	Spełnienie wymaganego parametru: Tak/Nie
7	**Rozdzielczość minimalna**	min. 1920x1080	
8	**Powłoka powierzchni ekranu**	Przeciwodblaskowa, 3H	
9	**Zakres pochylenia monitora**	Od -5,0° do +35,0°	
10	**Złącza**	Min. 1 szt. D-Sub Min. 1 szt. DVI-D Min. 1 szt. HDMI	
11	**Inne**	Monitor musi posiadać usuwalną podstawę montażową.	
12	**Normy i standardy**	Monitory muszą być wykonane zgodnie normami i posiadać Certyfikaty: CE, TCO Display 6.0 z jednoczesnym dopuszczeniem możliwości składania dokumentów równoważnych, czyli wydawanych przez podmiot uprawniony do kontroli jakości w zakresie usług lub dostawy będącej przedmiotem zamówienie	
13	**Gwarancja**	Min. 36 miesięcy - świadczona w siedzibie Zamawiającego, chyba że niezbędne będzie naprawa sprzętu w siedzibie producenta lub autoryzowanym przez niego punkcie serwisowym - wówczas koszt transportu do i z naprawy pokrywa Wykonawca, Czas reakcji na zgłoszoną reklamację gwarancyjną - do końca następnego dnia roboczego	

- Laptop typ 1 szt. 30

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne komputerów	Spełnienie wymaganego parametru: Tak/Nie

1.	Komputer	Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna. W ofercie należy podać nazwę producenta, typ, model, oraz numer katalogowy oferowanego sprzętu umożliwiający jednoznaczną identyfikację oferowanej konfiguracji w oparciu o materiały i systemy dostępne na stronie producenta – załączyć link do strony/systemu gdzie można dokonać weryfikacji.	
2.	Ekran	Matryca TFT, 15,6” z podświetleniem w technologii LED, powłoka antyrefleksyjna Anti-Glare- rozdzielczość: - FHD 1920x1080, 250nits	
3.	Obudowa	Obudowa komputera matowa, wyposażona w dock serwisowy umozliwiająca łatwy dostęp do pamięci RAM, dysków M.2 oraz 2,5” i karty WIFi. Zawiasy metalowe.	
4.	Chipset	Dostosowany do zaoferowanego procesora	
5.	Płyta główna	Zaprojektowana i wyprodukowana przez producenta komputera wyposażona w min. dwa złącza dla dysków z czego min. jedno M.2 z obsługą dysków PCIe NVMe. Płyta główna umożliwiająca konfiguracje wielodyskową.	
6.	Procesor	Procesor klasy x86, 2 rdzeniowy, zaprojektowany do pracy w komputerach przenośnych, taktowany zegarem co najmniej 2,5 GHz, pamięcią cache L3 co najmniej 3 MB lub równoważny wydajnościowo osiągający wynik co najmniej 4660 pkt w teście SysMark w kategorii PassMark CPU Mark, według wyników opublikowanych na stronie http://www.cpubenchmark.net	
7.	Pamięć operacyjna	Min 8GB z możliwością rozbudowy do 32GB, rodzaj pamięci DDR4, 2133MHz. Komputer wyposażony w minimum dwa banki pamięci umożliwiające pracę w trybie dual-channel.	
8.	Dyski	Wyposażony w dwa dyski z czego jeden przeznaczony na system operacyjny z Min 1TB HDD, prędkość obrotowa min 5400rpm zawierający partycję	

		RECOVERY umożliwiającą odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii. Przygotowana zatoka dyskowa wraz ramką montażową gotową do zainstalowania drugiego dysku.	
9.	Zabezpieczenie dysku twardego	Komputer wyposażony w systemem automatycznego parkowania głowicy w przypadku zastosowania dysku talerzowego.	
10.	Karta graficzna	Zintegrowana karta graficzna wykorzystująca pamięć RAM systemu dynamicznie przydzielaną na potrzeby grafiki. Obsługująca funkcje: • DirectX XX • OGL XX • Shader Model XX	
11.	Audio/Video	Wbudowana, zgodna z HD Audio, wbudowane głośniki stereo min 2x 2W, wbudowane dwa mikrofony, sterowanie głośnością głośników za pośrednictwem wydzielonych klawiszy funkcyjnych na klawiaturze, wydzielony przycisk funkcyjny do natychmiastowego wyciszania głośników oraz mikrofonu (mute), kamera HD720p pracująca przy niskim oświetleniu.	
12.	Karta sieciowa	10/100/1000 – RJ 45 wspierająca technologia PXE i WoL.	
13.	Porty/złącza	Min. 1xUSB-C, 2xUSB 3.0, 1xUSB 2.0 w wersji Power On USB, złącze słuchawek i złącze mikrofonu typu COMBO, VGA, HDMI ver. 1.4, RJ-45, czytnik kart multimedialnych (min SD/SDHC/SDXC/MMC).	
14.	Klawiatura	Klawiatura odporna na zalanie, układ US, z wbudowanym joystikiem do obsługi wskaźnika myszy z dedykowanymi 3 klawiszami. Klawiatura z wydzielonym blokiem numerycznym.	
15.	WiFi	Wbudowana karta sieciowa, pracująca w standardzie AC 2x2 lub 1x1	

16.	Czytnik linii papilarnych	Wbudowany czytnik linii papilarnych.	
17.	Bluetooth	Wbudowany moduł Bluetooth min. 4.0	
18.	Modem WWAN	Brak	
19.	Napęd optyczny	Nagrywarka DVD o wysokości nie większej jak 9mm	
20.	Bateria	Bateria - 4 ogniwa, pozwalająca na nieprzerwaną pracę urządzenia min do 240 minut. Czas pracy na baterii potwierdzony w teście MobileMark® 2014 (MobileMark 2014 Battery Life) – należy dostarczyć wyniki w formatach FDR (Full Disclosure Report) i PDF programu MobileMark® 2014.	
21.	Zasilacz	Zasilacz zewnętrzny max 90W.	
22.	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 CPU • wykonanie testu pamięci RAM • test dysku twardego • test matrycy LCD • test magistrali PCI-e • test portów USB • test napędu optycznego Wizualna lub akustyczna sygnalizacja w przypadku uszkodzenia badź 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, producent oraz numer seryjny poszczególnych kości pamięci • Dysk twardy: model, numer seryjny, wersja firmware, pojemność, prędkość obrotowa, temperatura pracy • LCD: producent, model, rozmiar, rozdzielczość, data produkcji panelu LCD • Napęd optyczny – producent, model, numer seryjny, wersja firmware, obsługiwane standardy w szczególności czy nagrywarka obsługuje płyty dual layer(DL) System Diagnostyczny działający nawet w przypadku uszkodzenia dysku twardego z systemem operacyjnym komputera. .	
23.	BIOS	BIOS zgodny ze specyfikacją UEFI. Możliwość odczytania z BIOS bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych podłączonych do niego urządzeń zewnętrznych następujących informacji: - wersji BIOS wraz z datą, - nr seryjnym komputera - PN producenta sprzętu pozwalający na identyfikację jednostki - ilości pamięci RAM - typie procesora i jego prędkości - MAC adresu zintegrowanej karty sieciowej - unikalnych nr inwentażowych tzw. Asset Tag'ów - nr seryjnym płyty głównej komputera Administrator z poziomu BIOS musi mieć możliwość wykonania poniższych czynności: - Możliwość Wyłączania/Włączania technologii antykradzieżowej	

		- Możliwość ustawienia hasła dla twardego dysku - Możliwość ustawienia hasła na starcie komputera tzw. POWER-On Password - Możliwość ustawienia minimalnych wymagań dotyczących długości hasła POWER-On oraz hasła dysku twardego. - Możliwość włączania/wyłączania wirutalizacji z poziomu BIOSU - Możliwość ustawienia kolejności bootowania - Możliwość Wyłączania/Włączania: zintegrowanej karty sieciowej, zintegrowanej karty WIFI i BT, czytnika linii papilarnych, mikrofonu, zintegrowanej kamery, portów USB, napędu optycznego, czytnika kart multimedialnych	
24.	Bezpieczeństwo	-złącze Kensington Lock, wsparcie dla ochrony antykradzieżowej	
25.	Certyfikaty i standardy	• Certyfikat ISO9001:2000 dla producenta sprzętu z jednoczesnym dopuszczeniem możliwości składania dokumentów równoważnych, czyli wydawanych przez podmiot uprawniony do kontroli jakości w zakresie usług lub dostawy będącej przedmiotem zamówienie - Oświadczenie o posiadaniu Certyfikatu EPEAT na poziomie co najmniej GOLD. Certyfikat ważny w dniu składania oferty i potwierdzony wydrukiem ze strony www.epeat.net – ENERGY STAR 6.1 - Deklaracja zgodności CE (załączyć do oferty) z jednoczesnym dopuszczeniem możliwości składania dokumentów równoważnych, czyli wydawanych przez podmiot uprawniony do kontroli jakości w zakresie usług lub dostawy będącej przedmiotem zamówienie - Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki - Głośność jednostki mierzona z pozycji operatora w trybie IDLE: max 20 dB	
26.	Waga/Wymiary	Waga urządzenia z baterią podstawową max 2,4kg, suma wymiarów urządzenia max 667	

27.	Szyfrowanie	Komputer wyposażony w moduł dTPM 2.0	
28.	System operacyjny	Win 10 PRO lub równoważny	
29.	Gwarancja	3 lata świadczona w miejscu użytkowania sprzętu (on-site) W przypadku awarii dysku twardego dysk uszkodzony pozostaje u Zamawiającego. Oświadczenie producenta komputera, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem.	
30.	Wsparcie techniczne producenta	Dedykowany numer oraz adres email dla wsparcia technicznego i informacji produktowej. - możliwość weryfikacji na stronie producenta konfiguracji fabrycznej zakupionego sprzętu - możliwość weryfikacji na stronie producenta posiadanej/wykupionej gwarancji - możliwość weryfikacji statusu naprawy urządzenia po podaniu unikalnego numeru seryjnego - Naprawy gwarancyjne urządzeń muszą być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta.	
31.	Inne	Patchcord min. 3m, torba na laptopa, mysz b/przewodowa, pendrive z możliwością fizycznego szyfrowania min 16GB.	

- Laptop typ 2 szt. 2

Nazwa parametru	**Wymagana minimalne**	Spełnienie wymaganego parametru: Tak/Nie

Typ	Laptop	
Ekran	Min 13” w rozdzielczości min, 2560 x 1600	
Procesor	Zainstalowany procesor dwurdzeniowy, min. 2200 MHZ, osiągający w testach wydajności PassMark - Passmark CPU Mark nie mniej niż 3400 punktów	
Pamięć RAM	nie mniej niż 8 GB RAM typu DDR3-1600	
Dysk twardy	Zainstalowany dysk twardy o pojemności min 256 GB bez części ruchomych	
Karta graficzna	Karta graficzna zintegrowana , rozdzielczość min. 1440x900	
Komunikacja	WiFi IEEE 802.11 ac/a/b/g/n	
Gwarancja	min. 12 m-cy	
Pozostałe fizyczne	Waga: max 1.4 kg .	
	Suma wymiarów nie większa niż 54 cm	
	USB 3.0 – min 2 szt.	

	Mysz bezprzewodowa bluetooth z technologią multitouch	
	Napęd optyczny kompatybilny z systemem MAC OS,	
	Dedykowana torba	
System operacyjny	Mac OS w najnowszej wersji lub równoważny	
Inne	Dedykowane oprogramowanie biurowe do danego systemu. Oprogramowanie do podglądu badań radiologicznych połączone z Pacsem Zamawiającego	

- Tablet typ 1. Szt. 2

Nazwa parametru	**Wymagania minimalne**	Spełnienie wymaganego parametru: Tak/Nie
Typ	Tablet	
Ekran	Min 5,8 rozdzielczości min, 2436 na 1125	
Procesor	Zainstalowany procesor 64 bit	

Pamięć RAM	Min 3 GB	
Dysk twardy	Min 64 GB	
Komunikacja	M.in. WiFi, Bluetooth, LTE	
Gwarancja	min. 12 m-cy	
Pozostałe fizyczne	Złącze min 1 Lightning Waga do 174g Grubość 7,7 mm	

- Zestaw komputerowy typ 2. szt. 5

Nazwa parametru	**Wymagania minimalne**	Spełnienie wymagane parametru: Tak/Nie
Typ	All-in-one	
Budowa	Wyświetlacz zintegrowany z jednostką	

	centralną, pamięcią masową oraz złączami do podłączania urządzeń peryferyjnych, zawierający dysk twardy	
Procesor	Zainstalowany procesor czterordzeniowy, czterowątkowy, w architekturze x86, osiągający w testach wydajności PassMark - Passmark CPU Mark nie mniej niż 7220 punktów	
Pamięć RAM	nie mniej niż 8 GB RAM typu DDR3-1600	
HDD	Zainstalowany dysk twardy o pojemności min 1000 GB	
Karta graficzna	Karta graficzna zintegrowana	
Ekran	o przekątnej nie mniejszej niż 27 cali i rozdzielczości nie niższej niż 5120 x 2880	
Komunikacja	LAN 1 Gbps WiFi IEEE 802.11 ac/a/b/g/n Bluetooth min 4.0	
Gwarancja	min. 12 m-cy	
System operacyjny	Mac OS X w najnowszej wersji lub równoważny oprogramowanie medyczne umożliwiające podgląd obrazów z podłączonego Pacsa w wersji nieograniczonej w wersji PL	
Pozostałe parametry	Thunderbolt – min 2 szt. Mini DisplayPort – min 1 szt. USB min 3.0 – min 4 szt	

	Gniazdo słuchawkowe/cyfrowe wyjście audio Głośniki stereofoniczne Dwa mikrofony Kamera HD	
Wyposażenie	Klawiatura bezprzewodowa (Polska z polem numerycznym)-dołączona do kompletu Mysz bezprzewodowa bluetooth z technologią multitouch	

- DRUKARKA ZE SKANEREM – 30 szt.

Nazwa parametru	**Wymagane minimalne parametry techniczne**	Spełnienie wymaganego parametru: Tak/Nie
Drukowanie		
Szybkość drukowania	Min. 28 str./min	
Czas pierwszego wydruku	Max 8 sekund	
Rozdzielczość	Min. 1200 x 1200 dpi	
Języki druku	Co najmniej: PCL5e, PCL6,	
Zespół drukowania	Dupleks	
Miesięczne obciążenie	Do 35 tys. stron	
Parametry minimalne	Szybkość procesora min. 360 Mhz, pamięć min 128 MB	
Poziom hałasu	Max 66 dB	
Skanowanie		
Rozdzielczość skanowania	Min. 600 x 600 dpi	
Podawanie dokumentów	Automatyczny podajnik dokumentów wraz z duplexem	
Format	Co najmniej: TIFF, PDF, JPEG	

Nazwa parametru	Wymagane minimalne parametry techniczne	Spełnienie wymaganego parametru: Tak/Nie
Skala szarości	256 poziomy	
Skanowanie do	Co najmniej: FTP, E-mail, Folder	
Kopiowanie		
Ilość kopii na arkusz	Do 4 kopii/arkusz	
Szybkość kopiowania	Min. 30 kopii/min	
Rozdzielczość kopiowania	Min. 1200 x 1200dpi	
Zmniejszanie/powiększanie	Zoom 25-400%	
Automatyczne kopiowanie dwustronne	Tak	
Interfejs i oprogramowanie		
Złącza	Min. 1 szt. Port USB 2.0, Min. 1 szt. Ethernet 10/100BaseTX Min. 1 szt. Wireless 802 11 1/b/gn NFC WIFI Direct	
Kompatybilność z systemami operacyjnymi	Windows 7 / Windows 8 I Windows 10 (32-bit & 64-bit) / Server 2008 i 2012 / Mac OS X 10.8 - 10.11	
Inne	Wyświetlacz LCD, IPP 1.0, Drukowanie znaków wodnych,	
Podawanie papieru		
Pojemność papieru	Podajnik 1: min. 250 arkuszy Maksymalna pojemność podajników do 335 arkuszy	
Format papieru	Podajnik 1: A4, A5, B5, A6, koperty	
Niestandardowe wymiary nośników	Szerokość: min 60 mm-max 216 mm Długość: min 140 mm-max 356 mm	

Nazwa parametru	Wymagane minimalne parametry techniczne	Spełnienie wymaganego parametru: Tak/Nie
Gramatura papieru	Do 162 g/m^2	
Odbiornik papieru	Min. 50 arkuszy	
Gwarancja	Min. 2 lata gwarancji producenta drukarki	
Wymaganie dodatkowe:	Serwis urządzeń musi być realizowany przez producenta lub autoryzowanego partnera serwisowego producenta – wymagane dołączenie do oferty oświadczenia podmiotu realizującego serwis lub producenta sprzętu o spełnieniu tego warunku. Dostarczyć kabel lan min 3 m. dostarczyć dodatkowy toner na min 6400 wydruków a4 przy 5% zadrukowaniu.	

- Oprogramowanie biurowe szt. 10

Microsoft Office 2016 Standard lub wyższy z licencjami przypisanymi do posiadającego przez Zamawiającego konta VLSC lub produkt równoważny z 3 letnim wsparciem technicznym Software Assurance lub równoważnych

Równoważność dla systemu Microsoft Office 2016

Licencja (nieograniczona w czasie oraz przestrzeni) na pakiet oprogramowania biurowego MS Office Standard 2016 PL lub rozwiązanie równoważne (tj. oprogramowanie biurowe wchodzące w skład pakietu, zawierającego co najmniej: edytor tekstu, arkusz kalkulacyjny, narzędzie do tworzenia prezentacji, klienta poczty MAPI w polskiej wersji językowej, wykonujące wszystkie funkcjonalności ww. pakietu oprogramowania biurowego, zapewniające możliwość instalacji i poprawnego działania na zaoferowanym systemie operacyjnym, w pełni obsługujące wszystkie istniejące pliki i dokumenty Zamawiającego, wytworzone przy użyciu oprogramowania Microsoft Office: 2003, 2007, 2010, 2013, 2016 bez utraty jakichkolwiek ich parametrów i cech użytkowych (odpowiednio dla oprogramowania: pliki tekstowe, dokumenty, arkusze kalkulacyjne zawierające makra i formularze, prezentacje multimedialne, itp.), w pełni kompatybilne i zgodne z obecnie zainstalowanym oraz pracującym u Zamawiającego systemem MS Exchange, oprogramowaniem biurowym, antywirusowym, narzędziowym, systemowym, niewymagającym dodatkowych nakładów finansowych ze strony Zamawiającego w celu dostosowania zaoferowanego oprogramowania do ww. systemów). W przypadku zaoferowania przez Wykonawcę rozwiązania równoważnego, Wykonawca jest zobowiązany do pokrycia wszelkich możliwych kosztów, wymaganych w czasie wdrożenia oferowanego rozwiązania, w szczególności związanych z dostosowaniem infrastruktury informatycznej, oprogramowania nią zarządzającego, systemowego i narzędziowego (licencje, wdrożenie), serwisu gwarancyjnego oraz kosztów certyfikowanych szkoleń dla

administratorów i użytkowników oferowanego rozwiązania. Zaoferowane oprogramowanie musi pozwalać na przenoszenie pojedynczych sztuk oprogramowania do jednostek zależnych.

1. Oprogramowanie musi posiadać pełną polską wersję językową interfejsu użytkownika.

2. Możliwość zintegrowania uwierzytelniania użytkowników z usługą katalogową (Active Directory lub funkcjonalnie równoważną) – użytkownik raz zalogowany z poziomu systemu operacyjnego stacji roboczej ma być automatycznie rozpoznawany we wszystkich modułach oferowanego rozwiązania bez potrzeby oddzielnego monitowania go o ponowne uwierzytelnienie się.

3. Narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleceń, język skryptowy – zgodny z Visual Basic for Application).

4. Pakiet musi zawierać: edytor tekstów, arkusz kalkulacyjny, narzędzie do przygotowywania i prowadzenia prezentacji, narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami).

5. Licencja bezterminowa;

6. Edytor tekstów umożliwiając:

a) Edycję i formatowanie tekstu w języku polskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty;

b) wstawianie oraz formatowanie tabel;

c) wstawianie oraz formatowanie obiektów graficznych;

d) wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne);

e) automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków;

f) automatyczne tworzenie spisów treści;

g) formatowanie nagłówków i stopek stron;

h) sprawdzanie pisowni w języku polskim; śledzenie zmian wprowadzonych przez użytkowników;

i) nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności;

j) określenie układu strony (pionowa/pozioma);

k) wydruk dokumentów; wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną;

l) pracę na dokumentach utworzonych przy pomocy posiadanego przez Zamawiającego oprogramowania Microsoft Word w wersjach 2003, 2007, 2010, 2013 i 2016 z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu;

m) zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.

7. Arkusz kalkulacyjny umożliwiający:

a) Tworzenie raportów tabelarycznych; tworzenie wykresów liniowych (wraz z linią trendu), słupkowych, kołowych;

b) tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu;

c) tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych;

d) wyszukiwanie i zamianę danych;

e) wykonywanie analiz danych przy użyciu formatowania warunkowego;

f) nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie;

g) nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności;

h) formatowanie czasu, daty i wartości finansowych z polskim formatem;

i) zapis wielu arkuszy kalkulacyjnych w jednym pliku; zachowanie pełnej zgodności z formatami plików utworzonych za pomocą oprogramowania zachowanie pełnej zgodności z formatami plików utworzonych za pomocą posiadanego przez Zamawiającego oprogramowania Microsoft Excel w wersjach 2003, 2007, 2010, 2013 i 2016 z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń;

j) zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.

8. Narzędzie do przygotowywania i prowadzenia prezentacji umożliwiające:

a) Przygotowywanie prezentacji multimedialnych, które będą:

 prezentowane przy użyciu projektora multimedialnego;

 drukowane w formacie umożliwiającym robienie notatek;

 zapisane jako prezentacja tylko do odczytu;

b) nagrywanie narracji i dołączanie jej do prezentacji;

c) opatrywanie slajdów notatkami dla prezentera;

d) umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo;

e) umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego;

f) odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym;

g) tworzenie animacji obiektów i całych slajdów;

h) prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera, pełna zgodność z formatami plików utworzonych za pomocą posiadanego przez Zamawiającego oprogramowania MS PowerPoint w wersjach 2003, 2007, 2010, 2013 i 2016.

9. Narzędzie do zarządzania informacją prywatną umożliwiające:

a) Pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego;

b) filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców;

c) tworzenie katalogów, pozwalających katalogować pocztę elektroniczną;

d) tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy;

e) oflagowanie poczty elektronicznej z określeniem terminu przypomnienia;

f) zarządzanie kalendarzem;

g) udostępnianie kalendarza innym użytkownikom;

h) przeglądanie kalendarza innych użytkowników;

i) zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach;

j) zarządzanie listą zadań;

k) zlecanie zadań innym użytkownikom;

l) zarządzanie listą kontaktów;

m) udostępnianie listy kontaktów innym użytkownikom;

n) przeglądanie listy kontaktów innych użytkowników;

o) możliwość przesyłania kontaktów innym użytkownikom, pełna zgodność obsługi poczty, kalendarzy, kontaktów i zadań ze wdrażanym u Zamawiającego serwerem (MS Exchange w wersji 2013).

- Inne oprogramowanie

Licencje dostępowe 150 szt. działających z m.in. z Windows Serwerem w wersji 2012 R2, umożliwiające jednoczesną pracę użytkowników w usłudze katalogowej w zakresie pozwalającym na legalny sposób (zgodnie z zasadami licencjonowania producenta) do dostęp do wszystkich serwerów Windows pracujących w domenie active directory.

Pakiet nr 3.

Dostawa systemów zabezpieczeń klasy UTM.

L.p.	Rodzaj	Nazwa/Producent /TYP/Model	Wartość netto	Podatek VAT	Wartość brutto
1	**Dostawa systemów zabezpieczeń klasy UTM**				
2	**System szyfrujący min 30 lic.**				
Razem:					

Opis przedmiotu zamówienia:

- Firewall

Wymagania Ogólne

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

System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

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

System musi wspierać IPv4 oraz IPv6 w zakresie:

- Firewall.
- Ochrony w warstwie aplikacji.
- Protokołów routingu dynamicznego.

Redundancja, monitoring i wykrywanie awarii

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.
2. W ramach postępowania system musi zostać dostarczony w postaci redundantnej.
3. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
4. Monitoring stanu realizowanych połączeń VPN.
5. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.

Interfejsy, Dysk, Zasilanie:

1. System realizujący funkcję Firewall musi dysponować minimum:
   - 18 portami Gigabit Ethernet RJ-45.
   - 4 gniazdami SFP 1 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 musi być wyposażony w zasilanie AC.

Parametry wydajnościowe:

1. W zakresie Firewall'a obsługa nie mniej niż 2 mln jednoczesnych połączeń oraz 135.000 nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 20 Gbps dla pakietów 512 B.
3. Przepustowość Stateful Firewall: nie mniej niż 9 Gbps dla pakietów 64 B.
4. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 3.5 Gbps.
5. Wydajność szyfrowania VPN IPSec dla pakietów 512 B, przy zastosowaniu algorytmu o mocy nie mniejszej niż AES256 – SHA256: nie mniej niż 9 Gbps.
6. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu HTTP - minimum 6 Gbps.
7. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 1.2 Gbps.
8. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL (TLS v1.2 z algorytmem nie słabszym niż AES128-SHA256) dla ruchu http – minimum 1 Gbps.

Funkcje Systemu Bezpieczeństwa:

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

1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3, IMAP.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
11. Analiza ruchu szyfrowanego protokołem SSL.
12. Analiza ruchu szyfrowanego protokołem SSH.

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.
   - Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
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 w trybie pracy Galois/Counter Mode(GCM).
   - Obsługa protokołu Diffie-Hellman grup 19 i 20.

- Wsparcie dla Pracy w topologii Hub iSpoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB iSPOKE.
- Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
- Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
- Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
- Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.
- Mechanizm „Split tunneling" dla połączeń Client-to-Site.

2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:
   - Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.
   - Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta

Routing i obsługa łączy WAN

1. W zakresie routingu rozwiązanie powinno zapewniać obsługę:
   - Routingu statycznego.
   - Policy Based Routingu.

· Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.

2. 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.
3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.

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 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
4. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
5. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.
6. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.

Kontrola aplikacji

1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji powinna zawierać minimum 2100 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
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 40 milionów adresów URL pogrupowanych w kategorie tematyczne.

2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy 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. System musi umożliwiać zdefiniowanie czasu, który użytkownicy sieci mogą spędzać na stronach o określonej kategorii. Musi istnieć również możliwość określenia maksymalnej ilości danych, które użytkownik może pobrać ze stron o określonej kategorii.
6. 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, RSA SecurID) w oparciu o zewnętrzne bazy danych.
2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.
3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.

Zarządzanie

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.

5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. 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 NSS Labs dla funkcji IPS.
- ICSA dla funkcji IPSec VPN.
- ICSA dla funkcji SSL 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:

a) Kontrola 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.

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 z jednoczesnym dopuszczeniem możliwości składania dokumentów równoważnych, czyli wydawanych przez podmiot uprawniony do kontroli jakości w zakresie usług lub dostawy będącej przedmiotem zamówienie, w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 8x5 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim Oferent winien przedłożyć dokumenty:

- 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).
- Certyfikat ISO 9001 z jednoczesnym dopuszczeniem możliwości składania dokumentów równoważnych, czyli wydawanych przez podmiot uprawniony do kontroli jakości w zakresie usług lub dostawy będącej przedmiotem zamówienie podmiotu serwisującego.

Inne.

Wykonawca zapewni autoryzowane szkolenie z w/w produktu dla min 2 os. trwające min. 3 dni, zapewniające certyfikat oraz niezbędną wiedzę umożliwiającą pracę z oferowanym produktem. Wszelkie koszty z tym związane leżą po stronie Wykonawcy.

- Oprogramowanie ochrona mail

Wymagania ogólne
System ochrony poczty musi zapewniać kompleksową ochronę antyspamową, antywirusową oraz antyspyware'ową bez limitu licencyjnego na ilość chronionych kont użytkowników.

Dopuszcza się aby poszczególne elementy wchodzące w skład systemu ochrony były zrealizowane w postaci osobnych, komercyjnych platform wirtualnych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia w środowisku wirtualnym. W przypadku implementacji programowej dostawca musi zapewnić platformę w postaci odpowiednio zabezpieczonego systememu operacyjnego, na którym będzie instalowane rozwiązanie. Platformy muszą mieć możliwość uruchomienia na co najmniej następujących hypervisorach: VMware ESX/ESXi 5.0/5.1/5.5/6.0, Microsoft Hyper-V 2008 R2/2012/2012 R2, Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM.

Dla zapewnienia wysokiej sprawności i skuteczności działania rozwiązanie musi pracować w oparciu o dedykowany system operacyjny oraz komercyjne bazy zabezpieczeń.

Dostarczone rozwiązanie musi mieć możliwość pracy w każdym trybów:

1. Tryb Gateway.
2. Tryb transparentny (nie wymaga rekonfiguracji istniejącego systemu poczty elektronicznej).

Parametry fizyczne systemu antyspamowego

1. System musi obsługiwać co najmniej 4 interfejsy sieciowe oraz wspierać powierzchnię dyskową o pojemności co najmniej 1 TB.

Ogólne funkcje systemu ochrony poczty

Dostarczany system obsługi i ochrony poczty musi zapewniać poniższe funkcje:

1. Wsparcie dla co najmniej 2 domen pocztowych.
2. System musi realizować skanowanie antyspamowe i antywirusowe z wydajnością min. 2,5 tys. wiadomości/godzinę.
3. Polityki filtrowania poczty tworzone co najmniej w oparciu o: adresy mailowe, nazwy domenowe, adresy IP (w szczególności powinna być możliwość definiowania reguł all-all).
4. Email routing w oparciu o reguły lokalne lub w oparciu o zewnętrzny serwer LDAP.
5. Zarządzanie kolejkami wiadomości (np. reguły opóźniania dostarczenia wiadomości).
6. Ochrona i analiza zarówno poczty przychodzącej jak i wychodzącej.
7. Szczegółowe, wielowarstwowe polityki wykrywania spamu oraz wirusów.
8. Możliwość tworzenia polityk kontroli Antywirusowej oraz Antyspamowej w oparciu o użytkownika i atrybuty zwracane z zewnętrznego serwera LDAP.
9. Kwarantanna poczty z dziennym podsumowaniem dla użytkownika z możliwością samodzielnego zwalniania bądź usuwania wiadomości z kwarantanny przez użytkownika.
10. Dostęp do kwarantanny użytkownika możliwy poprzez WebMail oraz POP3.
11. Archiwizacja poczty przychodzącej i wychodzącej w oparciu o polityki.
12. Możliwość przechowywania poczty oraz jej backup realizowany lokalnie na dysku systemu oraz na zewnętrznych zasobach, co najmniej: NFS, iSCSI.
13. Białe i czarne listy adresów mailowych definiowane globalnie oraz dla domen wskazanych przez administratora systemu.
14. Białe i czarne listy adresów mailowych dla poszczególnych użytkowników.
15. Ochrona przed wyciekiem informacji poufnej DLP (Data Leak Preention).

Kontrola antywirusowa i ochrona przed malware

W tym zakresie dostarczony system ochrony poczty musi zapewniać:

1. Skanowanie antywirusowe wiadomości SMTP.
2. Kwarantannę dla zainfekowanych plików.
3. Skanowanie załączników skompresowanych.
4. Definiowanie komunikatów powiadomień w języku polskim.
5. Blokowanie załączników w oparciu o typ pliku.
6. Możliwość zdefiniowania nie mniej niż 15 polityk kontroli antywirusowej.
7. 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. Rozwiązanie musi umożliwiać zatrzymanie poczty w dedykowanej kolejce wiadomości do momentu otrzymania werdyktu.
8. Definiowanie różnych akcji dla poszczególnych metod wykrywania wirusów i malware'u. Powinny one obejmować co najmniej: tagowanie wiadomości, dodanie nowego nagłówka, zastąpienie podejrzanej treści lub załącznika, akcje discard lub reject, dostarczenie do innego serwera, powiadomienie administratora.

Kontrola antyspamowa

System musi zapewniać poniższe funkcje i metody filtrowania spamu:

1. Reputacja adresów źródłowych IP oraz domen pocztowych w oparciu o bazy producenta.
2. Filtrowanie poczty w oparciu o sumy kontrolne wiadomości dostarczane przez producenta rozwiązania.
3. Szczegółowa kontrola nagłówka wiadomości.
4. Analiza Heurystyczna.
5. Współpraca z zewnętrznymi serwerami RBL, SURBL.
6. Filtrowanie w oparciu o filtry Bayes’a z możliwością uczenia przez administratora globalnie dla całego systemu lub poszczególnych chronionych domen.
7. Możliwością dostrajania filtrów Bayes’a przez poszczególnych użytkowników.
8. Wykrywanie spamu w oparciu a analizę plików graficznych oraz plików PDF.
9. Kontrola w oparciu o Greylisting oraz SPF.
10. Filtrowanie treści wiadomości i załączników.
11. Kwarantanna zarówno użytkowników jak i systemowa z możliwością edycji nagłówka wiadomości.
12. Możliwość zdefiniowania nie mniej niż 15 polityk kontroli antyspamowej.
13. Ochrona typu outbrake.
14. Filtrowanie poczty w oparciu o kategorie URL (co najmniej: malware, hacking).

15. Definiowanie różnych akcji dla poszczególnych metod wykrywania spamu. Powinny one obejmować co najmniej: tagowanie wiadomości, dodanie nowego nagłówka, akcje discard lub reject, dostarczenie do innego serwera, powiadomienie administratora.

Ochrona przed atakami na usługę poczty
System musi zapewniać poniższe funkcje i metody filtrowania:

1. Ochrona przed atakami na adres odbiorcy.
2. Definiowanie maksymalnej ilości wiadomości pocztowych otrzymywanych w jednostce czasu.

3. Definiowanie maksymalnej liczby jednoczesnych sesji SMTP w jednostce czasu.

3. Kontrola Reverse DNS (ochrona przed Anty-Spoofing).
4. Weryfikacja poprawności adresu e-mail nadawcy.

Funkcje logowania i raportowania
W tym zakresie dostarczony system ochrony poczty musi zapewniać:

1. Logowanie do zewnętrznego serwera SYSLOG.
2. Logowanie zmian konfiguracji oraz krytycznych zdarzeń systemowych np. w przypadku przepełnienia dysku.
3. Logowanie informacji na temat spamu oraz niedozwolonych załączników.
4. Możliwość podglądu logów w czasie rzeczywistym.
5. Możliwość analizy przebiegu sesji SMTP.
6. Powiadamianie administratora systemu w przypadku wykrycia wirusów w przesyłanych wiadomościach pocztowych.
7. Predefiniowane szablony raportów oraz możliwość ich edycji przez administratora systemu.
8. Możliwość generowania raportów zgodnie z harmonogramem lub na żądanie administratora systemu.

Funkcje pracy w trybie wysokiej dostępności (HA)
System ochrony poczty musi zapewniać poniższe funkcje:

1. Konfigurację HA w każdym z trybów: gateway, transparent.
2. Tryb synchronizacji konfiguracji dla scenariuszy gdy każde z urządzeń występuje pod innym adresem IP.
3. Wykrywanie awarii poszczególnych urządzeń oraz powiadamianie administratora systemu.
4. Monitorowanie stanu pracy klastra.

Aktualizacje sygnatur, dostęp do bazy spamu
W tym zakresie dostarczony system ochrony poczty musi zapewniać:

1. Pracę w oparciu o bazę spamu oraz url uaktualniane w czasie rzeczywistym.
2. Planowanie aktualizacji szczepionek antywirusowych zgodnie z harmonogramem co najmniej raz na godzinę.

Zarządzanie

System ochrony poczty musi zapewniać poniższe funkcje:

1. System musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH.
2. Możliwość modyfikowania wyglądu interfejsu zarządzania oraz interfejsu WebMail z opcją wstawienia własnego logo firmy.
3. Powinna istnieć możliwość zdefiniowania co najmniej 6 lokalnych kont administracyjnych.

Certyfikaty

Dostarczony system powinien posiadać poniższe certyfikaty:

1. VBSpam iVB100 rated lub Common Criteria NDPP, FIPS 140-2 Certified.

Serwisy i licencje

W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:

1. Kontrola Antyspam, URL Filtering, kontrola antywirusowa na okres 60 miesięcy.

Gwarancja oraz wsparcie

1. System musi być objęty serwisem producenta przez okres 60 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 8x5.

Inne.

Wykonawca zapewni autoryzowane szkolenie z w/w produktu dla min 2 os. trwające min. 3 dni, zapewniające certyfikat oraz niezbędną wiedzę umożliwiającą pracę z oferowanym produktem. Wszelkie koszty z tym związane leżą po stronie Wykonawcy.

Wykonawca na etapie analizy przedwdrożeniowej zaproponuje optymalne rozwiązanie wykorzystujące w/w sprzęt.

- Oprogramowanie klienckie

Dostarczony system zarządzania aplikacjami klienckimi musi zapewniać wszystkie wymienione poniżej funkcje. Wymaga się aby elementy wchodzące w skład systemu były zrealizowane w postaci komercyjnych aplikacji instalowanych na systemach : Microsoft Windows Server 2012, 2012 R2 Microsoft Windows Server 2008 R2

W ramach postępowania wymagane jest dostarczenie systemu zarzadzania aplikacjami klienckimi dla stacji roboczych dla systemów operacyjnych: Microsoft Windows 10 (32-bit, 64-bit), Windows 8.1 (32-bit, 64-bit), Windows 8 (32-bit, 64-bit), Windows 7 (32-bit, 64-bit), Windows Vista (32-bit, 64-bit), Windows XP (32-bit), Windows Server 2008 R2 iWindows Server 2012, 2012 R2, Mac OS X v10.11 El Capitan, OS X v10.10 Yosemite, OS X v10.9 Mavericks iOS X v10.8 Mountain Lion

Dostarczony system powinien umożliwiać automatyczne aktualizacje oprogramowania zabezpieczającego na aplikacji klienckich oraz musi zapewniać integracje z sieciowymi systemami bezpieczeństwa.

Producent rozwiązania powinien dostarczać system ochrony dla stacji roboczych który posiada następujące funkcje : antywirus, web filtering, firewall aplikacyjny, analiza podatności, szyfrowane tunele IPSec VPN oraz SSL VPN, mechanizmy uwierzytelniania dwuskładnikowego.

Konsola zarządzająca powinna umożliwiać konfigurowanie wszystkich funkcji klienckiego systemu zabezpieczeń. W szczególności wymagane jest aby system zapewniał:

- integracja z systemami zarządzania tożsamością użytkowników AD,
- definiowanie różnych profil ochrony dla różnych grup użytkowników czerpanych z AD lub definiowanych lokalnie,
- zautomatyzowany proces zarządzania aplikacja kliencką,
- przygotowywanie paczek instalacyjnych w których administrator może określić komponenty dla ochrony stacji roboczych,
- możliwość edycji pliku konfiguracyjnego w zewnętrznym edytorze tekstowym,
- panel w którym wyświetlane są wyniki analizy podatności na stacjach roboczych,
- automatyczne wykrywanie stacji klienckich w grupach roboczych,
- logowanie zdarzeń z aplikacji klienckich , możliwość ich przeglądania z funkcja filtrów oraz możliwością pobierania logów przez administratora,
- generowanie alarmów: związanych z zarządzeniem aplikacją kliencką, w przypadku wykrycia ważnych podatności na stacjach oraz w sytuacji zaistnienia zdarzeń związanych z aktywnością złośliwego kodu, aktywności aplikacji bootnet z wykorzystaniem komunikacji C&C,
- definiowanie grup administratorów lokalnie oraz w oparciu o AD z opcja przypisywania uprawnień do elementów panelu konfiguracyjnego,
- zarządzenie certyfikatami na potrzeby połączeń IPSec VPN oraz SSL VPN.

Administrator musi mieć możliwość wykonywania backupu i odtwarzania bazy danych w oparciu o którą działa system a także możliwość dystrybucji paczek instalacyjnych z lokalnych zasobów w oparciu o adres URL definiowany przez administratora.

W ramach postępowania wraz z konsolą centralnego zarządzania powinna dostarczona licencja na zarządzanie co najmniej 500 aplikacjami na stacjach roboczych.

- Oprogramowanie centralny system logowania

Wymagania Ogólne

W ramach postępowania wymaganym jest dostarczenie centralnego systemu logowania, raportowania i korelacji, umożliwiającego centralizację procesu logowania zdarzeń sieciowych, systemowych oraz bezpieczeństwa w ramach całej infrastruktury zabezpieczeń wraz z ekranem min 55 cali, zamocowaniem naściennym z co najmniej 2x HDMI, LAN, WIFI.

Rozwiązanie musi zostać dostarczone w postaci komercyjnej platformy działającej w środowisku wirtualnym lub w postaci komercyjnej platformy działającej na bazie linux w środowisku wirtualnym, z możliwością uruchomienia na co najmniej następujących hypervisorach: VMware ESX/ESXi 5.0/5.1/5.5/6.0, Microsoft Hyper-V 2008 R2/2012/2012 R2, Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM.

Interfejsy, Dysk:

1. System musi obsługiwać co najmniej 4 interfejsy sieciowe oraz wspierać powierzchnię dyskową o pojemności 500 GB.

Parametry wydajnościowe:

1. System musi być w stanie przyjmować minimum 1 GB logów na dzień.
2. Rozwiązanie musi umożliwiać kolekcjonowanie logów z co najmniej 1000 systemów.

Logowanie

1. Podgląd logowanych zdarzeń w czasie rzeczywistym.
2. Możliwość przeglądania logów historycznych z funkcją filtrowania.
3. System musi oferować predefiniowane (lub mieć możliwość ich konfiguracji) podręczne raporty graficzne lub tekstowe obrazujące stan pracy urządzenia oraz ogólne informacje dotyczące statystyk ruchu sieciowego i zdarzeń bezpieczeństwa. Muszą one obejmować co najmniej:

a. Listę najczęściej wykrywanych ataków.

b. Listę najbardziej aktywnych użytkowników.

c. Listę najczęściej wykorzystywanych aplikacji.

d. Listę najczęściej odwiedzanych stron www.

e. Listę krajów , do których nawiązywane są połączenia.

f. Listę najczęściej wykorzystywanych polityk Firewall.

g. Informacje o realizowanych połączeniach IPSec.

4. Rozwiązanie musi posiadać możliwość przesyłania kopii logów do innych systemów logowania i przetwarzania danych. Musi w tym zakresie zapewniać mechanizmy filtrowania dla wysyłanych logów.
5. Komunikacja systemów bezpieczeństwa (z których przesyłane są logi) z oferowanym systemem centralnego logowania musi być możliwa co najmniej z wykorzystaniem UDP/514 oraz TCP/514.
6. System musi realizować cykliczny eksport logów do zewnętrznego systemu w celu ich długo czasowego składowania. Eksport logów musi być możliwy za pomocą protokołu SFTP lub na zewnętrzny zasób sieciowy.

Raportowanie

W zakresie raportowania system musi zapewniać:

1. Generowanie raportów co najmniej w formatach: HTML, PDF, CSV.
2. Predefiniowane zestawy raportów, dla których administrator systemu może modyfikować parametry prezentowania wyników.
3. Funkcję definiowania własnych raportów.
4. Możliwość spolszczenia raportów.
5. Generowanie raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesłania wyników na określony adres lub adresy email.

Korelacja logów

W zakresie korelacji zdarzeń system musi zapewniać:

1. Korelowanie logów z określeniem urządzeń, dla których ten proces ma być realizowany.
2. Konfigurację powiadomień poprzez: e-mail, SNMP w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa.
3. Wybór kategorii zdarzeń, dla których tworzone będą reguły korelacyjne. System korelować zdarzenia co najmniej dla następujących kategorii zdarzeń:
   - Malware.
   - Aplikacje sieciowe.
   - Email.
   - IPS.
   - Traffic.
   - Systemowe: utracone połączenie vpn, utracone połączenie sieciowe.

Zarządzanie

1. System logowania i raportowania musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH lub producent rozwiązania musi dostarczać dedykowanej konsoli zarządzania, która komunikuje się z rozwiązaniem przy wykorzystaniu szyfrowanych protokołów.

a. Proces uwierzytelniania administratorów musi być realizowany w oparciu o: lokalną bazę, Radius, LDAP, PKI.

2. System musi umożliwiać zdefiniowanie co najmniej 8 administratorów z możliwością określenia praw dostępu do logowanych informacji i raportów z perspektywy poszczególnych systemów, z których przesyłane są logi.

Gwarancja oraz wsparcie

1. Wsparcie: System musi być objęty serwisem producenta przez okres 60 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7.

Inne.

2. Wykonawca zapewni autoryzowane szkolenie z w/w produktu dla min 2 os. trwające min. 3 dni, zapewniające certyfikat producenta oraz niezbędną wiedzę umożliwiającą pracę z oferowanym produktem. Wszelkie koszty z tym związane leżą po stronie Wykonawcy.
3. Wykonawca na etapie analizy przedwdrożeniowej zaproponuje optymalne rozwiązanie wykorzystujące w/w oprogramowanie.

- Oprogramowanie szyfrujące min. 30 szt.

Kontrola pamięci przenośnych, urządzeń, mediów oraz przepływu danych

- blokowanie dowolnego typu napędów (floppy disk, USB, CD/DVD, FireWire itp.)

- blokowanie dowolnych urządzeń przenośnych (smartfony, MP3, kamery, odtwarzacze, tablety itp.)

- definiowanie autoryzowanych urządzeń

- filtrowanie plików

- definiowanie typów plików

- audyt transferu danych

- tworzenie tzw. „shadow copies”

2. Centralne inteligentne zarządzanie

- tworzenie szablonów

- automatyczne uruchamianie skryptów po podłączeniu urządzeń

- uruchamianie ustawień bazujących na aktualnym połączeniu sieciowym

3. Zaawansowane raportowanie

- centralna baza SQL wydarzeń
- tworzenie raportów do zarządzania i identyfikowania ryzyk bezpieczeństwa
- analiza zdarzeń
- wydruk raportów oraz wykresów
- eksportowanie danych z raportów;

4. Kontrola Aplikacji

- audyt wykorzystania aplikacji
- blokowanie aplikacji (blacklist)
- umożliwianie uruchamiania autoryzowanych aplikacji (whitelisting)
- łączenie blacklist i whitelist w celu maksymalizacji bezpieczeństwa i wydajności

5. Pełne szyfrowanie dysków HDD

- szyfrowanie dysków wewnętrznych łącznie z partycją
- certyfikowane FIPS140-2
- uwierzytelnianie pre-boot oraz SSO
- narzędzia do odzyskiwania dostępu do danych na uszkodzonych dyskach oraz awaryjnego dostępu w przypadku zagubienia hasła
- wsparcie dla uwierzytelniania przy użyciu smart cards oraz tokenów

6. Websecurity - Zintegrowany filtr adresów URL

- zapewnia bezpieczeństwo w czasie rzeczywistym zgodnie z zasadami firmowymi dla wszystkich urządzeń używanych przez pracowników – w dowolnym miejscu i we wszystkich sieciach.

7. Działa na systemach Windows minimum 10, 8, 7

Dodatkowo:

1. Graficzny interfejs użytkownika w języku polskim.
2. Instalację i poprawne działanie wykorzystywanych przez Zamawiającego programów wchodzących w skład pakietu biurowego minimum Microsoft Office Proffessional 2010, 2013;
3. Instalację i poprawne działanie wykorzystywanych przez Zamawiającego programów: SINFZ, KS-SIKCH.
4. Dostęp do bezpłatnych aktualizacji i poprawek do systemu, u producenta

systemu z możliwością wyboru instalowanych poprawek.
5. Graficzne środowisko instalacji i konfiguracji systemu.
6. Możliwość wykonania kopii zapasowej systemu wraz z możliwością odzyskania wersji wcześniejszej.
7. Możliwość wykonania kopii zapasowej systemu wraz z ustawieniami systemu, użytkownika, zainstalowanych programów oraz plików;
8. Pełną kompatybilność z oferowanym komputerem;
9. Zintegrowaną zaporę sieciową wraz z konsolą do zarządzania ustawieniami i regułami IP v4 i v6;
10. Możliwość korzystania z funkcjonalności zdalnego pulpitu;
11. Pełną integrację z wykorzystywaną przez Zamawiającego usługą katalogową Active Directory opartą na systemie operacyjnym minimum Windows Serwer 2008 R2;
12. Pełną integrację z wykorzystywanym przez zamawiającego narzędziem Microsoft System Center 2012 Configuration Manager, szczególnie modułem Configuration Manager Remote Control;
13. Możliwość zabezpieczenia hasłem dostępu do systemu, konta i profilu użytkownika;
14. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk sprzętowych (np. przy użyciu numerów identyfikacyjnych sprzętu);
15. Licencje na system operacyjny, która jest nieograniczona w czasie, pozwala na wielokrotne instalowanie systemu na oferowanym sprzęcie bez konieczności kontaktowania się przez Zamawiającego z producentem systemu lub sprzętu.
16. Wymagana gwarancja na prawidłowe działanie oprogramowania – 36 m-cy od dnia dostawy.

- WYMAGANIA DODATKOWE:

Wraz z dostawą urządzeń (serwery, macierze dyskowe, przełączniki, urządzenie do backupu dyskowego) Wykonawca dostarczy oświadczenia producentów tych urządzeń zawierające następujące informacje:

- P/N dostarczonych urządzeń
- numery seryjne dostarczonych urządzeń
- informację jaka firma jest dostawcą dostarczonych urządzeń
- informację jaka firma jest odbiorcą dostarczonych urządzeń
- informację, że urządzenia są objęte gwarancją oraz serwisem i wsparciem producenta na terenie Polski.

WYMAGANIA FORMALNE:

W celu potwierdzenia spełniania warunku udziału w postępowaniu Zamawiający może żądać od Wykonawcy:

a. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.
b. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

zawarta w dniu …… r. pomiędzy:
Specjalistycznym Szpitalem im. dra Alfreda Sokołowskiego z siedzibą w Wałbrzychu przy ul. Sokołowskiego 4, wpisanym do rejestru stowarzyszeń i innych organizacji społecznych i zawodowych, fundacji, publicznych zakładów opieki zdrowotnej, prowadzonego przez Sąd Rejonowy dla Wrocławia-Fabrycznej, IX Wydział Gospodarczy KRS we Wrocławiu- pod numerem KRS 0000046016
zwanym w treści umowy **„Zamawiającym"**
reprezentowanym przez:
mgr Mariolę Dudziak – Dyrektora Szpitala
a
…….....
.....
zwanym w treści umowy **„Wykonawcą"**
reprezentowanym przez:
.....

§ 1

1. Podstawą zawarcia niniejszej umowy jest rozstrzygnięcie przetargu nieograniczonego na **„Dostawa sprzętu komputerowego wraz oprogramowaniem tj.: serwerów, zestawów komputerowych, laptopów, tabletów, drukarek wraz z oprogramowaniem oraz rozbudowa obecnej infrastruktury macierzy i przełączników dla poprawy dostępności i skuteczności leczenia onkologicznego na terenie województwa dolnośląskiego na potrzeby Specjalistycznego Szpitala im. dra. Alfreda Sokołowskiego w Wałbrzychu".**
ogłoszonego w Suplemencie do Dziennika Urzędowego Unii Europejskiej w dniu …….. r., nr ogłoszenia …….
2. Specyfikacja Istotnych Warunków Zamówienia wraz z załącznikami stanowią integralne części umowy.

§ 2

1.Przedmiotem umowy jest dostawa ..... zgodnie z ofertą Wykonawcy z dnia ..... 2018 r. stanowiącą załącznik do niniejszej umowy.
2. Wykonawca oświadcza, iż dostarczony przedmiot umowy pozostaje nowy i wolny od wad.

§ 3

1.Wykonawca zobowiązuje się do realizacji przedmiotu umowy określonego w § 2 tj.: dostarczenia przedmiotu umowy, w terminie do ..... tygodni od daty zawarcia umowy.
2.Wykonawca zobowiązany jest do powiadomienia Zamawiającego o terminie dostawy przedmiotu umowy z co najmniej 3 dniowym wyprzedzeniem.
3. W przypadku dostawy przedmiotu umowy posiadającego wady Zamawiający niezwłocznie zawiadomi o tym Wykonawcę, a ten dokona jego wymiany na pełnowartościowy lub przedmiot umowy zostanie zwrócony Wykonawcy.
4. Termin rozpatrywania przez Wykonawcę ewentualnych reklamacji wynosi 5 dni robocze.
5.Wszelkie koszty związane z postępowaniem reklamacyjnym (w szczególności koszty transportu reklamowanej części lub całego przedmiotu umowy) ponosi Wykonawca.

§ 4

1.Przedmiot umowy, o którym mowa w § 2 dostarczony zostanie przez Wykonawcę transportem na jego koszt i ryzyko, w opakowaniu zabezpieczającym przedmiot dostawy przed uszkodzeniem.
2.Przedmiot umowy będzie dostarczony do siedziby Zamawiającego wraz z instrukcją obsługi i użytkowania w formie papierowej i elektronicznej w języku polskim oraz wszelką konieczną dokumentacją tj. kartą gwarancyjną, wykazem punktów serwisowych, kopiami dokumentów wraz z tłumaczeniem w przypadku oryginału w języku obcym : Certyfikat CE oraz Deklaracja Zgodności – wystawiona przez producenta
3.Dostarczony przedmiot umowy winien posiadać wszelkie świadectwa i atesty dopuszczające do użytku i stosowania na terenie RP zgodnie z obowiązującymi przepisami.
4.Potwierdzeniem wykonania przez Wykonawcę przedmiotu umowy jest protokolarne potwierdzenie przez Zamawiającego jego dostawy.
5. W w/w czynnościach ze strony Zamawiającego uczestniczyć będą:
- ……..
-……...

§ 5

1.Za wykonanie przedmiotu umowy określonego w § 2 umowy Wykonawcy przysługuje:
- wynagrodzenie w wysokości ……zł netto (słownie: ……) + VAT w należnej wysokości. (dot. poz. 1, 2, 6, 7 i 8)
- wynagrodzenie w wysokości ……. zł. (słownie ……..) dot. poz. 3, 4 i 5)
2.Podstawą do wystawienia faktury VAT przez Wykonawcę jest protokół odbioru podpisany przez Zamawiającego, potwierdzający m.in. dostawę.
3. Na fakturze Wykonawca winien wpisać nr umowy przetargowej.
4.Zapłata nastąpi w terminie do **60 dni** od daty doręczenia Zamawiającemu prawidłowo sporządzonej, zgodnie z ust. 2 faktury VAT, przelewem na rachunek bankowy Wykonawcy wskazany na fakturze.
5. Wykonawca oświadcza, że jest płatnikiem podatku od towarów i usług VAT i posiada numer identyfikacyjny NIP: .....
6.Wykonawca nie może przenieść wierzytelności wynikających z niniejszej umowy na stronę trzecią w trybie art. 509 – 518 Kodeksu Cywilnego.

§ 6

1.Wykonawca udziela gwarancji na dostarczony przedmiot umowy na okres wg Załącznika nr 1 SIWZ licząc od daty podpisania przez Zamawiającego protokołu odbioru potwierdzającego jego dostawę
2.Wykonawca na wykonane prace (nie objęte gwarancją producenta sprzętu) udziela gwarancji na okres 24 miesięcy od daty podpisania protokołu odbioru potwierdzającego zakończenie prac związanych z zamówieniem.
3.W przypadku awarii Wykonawca zobowiązuje się przystąpić do jej usunięcia w czasie nie dłuższym niż 72 godziny od daty zgłoszenia awarii.
4. Czas usunięcia awarii nie dłuższy niż 5 dni liczony od momentu podjęcia naprawy.

§ 7

1.W przypadku niewykonania bądź nienależytego wykonania umowy Wykonawca zobowiązany jest do zapłaty Zamawiającemu kary umownej w wysokości:

a) 10 % wartości wynagrodzenia określonego w § 5 ust. 1 umowy – w przypadku odstąpienia Wykonawcy od umowy, bądź odstąpienia od umowy Zamawiającego z winy Wykonawcy.

b) 1 % wartości niewykonanej dostawy – za każdy dzień zwłoki w dostawie przedmiotu umowy lub zwłoki w przystąpieniu do usunięcia awarii,

2. Zamawiający zobowiązany jest do zapłaty na rzecz Wykonawcy kary umownej w wysokości 10 % wartości niewykonanej umowy – w przypadku rozwiązania umowy przez Zamawiającego bądź przez Wykonawcę z winy Zamawiającego.

3.Zamawiającemu przysługuje prawo dochodzenia na zasadach ogólnych odszkodowań przewyższających wysokość kar umownych, o których mowa w 7 ust. 1.

§ 8

1.Zamawiający zastrzega sobie prawo do odstąpienia od umowy w trybie natychmiastowym w przypadku zwłoki Wykonawcy w wykonaniu przedmiotu umowy określonego w § 2 – powyżej 14 dni.

2.Odstąpienie od umowy z przyczyn określonych w ust. 1 uprawnia Zamawiającego od dochodzenia kar umownych i odszkodowania, zgodnie z § 7 ust. 1 i 3 umowy.

§ 9

Zamawiający zastrzega sobie prawo odstąpienia od umowy w oparciu o przepis art. 145 ustawy Prawo Zamówień Publicznych.

§ 10

Wszelkie zmiany i uzupełnienia niniejszej umowy wymagają formy pisemnej w postaci aneksu, pod rygorem nieważności.

§ 11

1. W sprawach nieuregulowanych niniejszą umową mają zastosowanie przepisy:

1) Kodeksu Cywilnego,

2) Ustawy z dnia 29.01.2004 Prawo zamówień publicznych (tekst jednolity Dz. U. z 2017, poz. 1579).

2. Wykonawca oświadcza, że zapoznał się ze standardami akredytacyjnymi Centrum Monitorowania Jakości w Ochronie Zdrowia oraz standardami ISO 9001:2015 i zobowiązuje się do realizowania umowy z zachowaniem tych standardów.

§ 12

Ewentualne spory wynikłe na tle wykonywania postanowień niniejszej umowy strony poddają rozstrzygnięciu Sądu powszechnego właściwego dla siedziby Zamawiającego.

§ 13

Umowę sporządzono w trzech jednobrzmiących egzemplarzach, dwa dla Zamawiającego, jeden dla Wykonawcy.

WYKONAWCA **ZAMAWIAJĄCY**

Załącznik nr 3a do SIWZ (dotyczy Pakiet nr 1 i 3)

UMOWA Nr Zp/22/PN-16/18/…

Projekt współfinansowany przez Unię Europejską z w ramach
Programu Operacyjnego Infrastruktura i Środowisko 2014 - 2020

zawarta w dniu …… r. pomiędzy:
Specjalistycznym Szpitalem im. dra Alfreda Sokołowskiego z siedzibą w Wałbrzychu przy ul. Sokołowskiego 4, wpisanym do rejestru stowarzyszeń i innych organizacji społecznych i zawodowych, fundacji, publicznych zakładów opieki zdrowotnej, prowadzonego przez Sąd Rejonowy dla Wrocławia-Fabrycznej, IX Wydział Gospodarczy KRS we Wrocławiu- pod numerem KRS 0000046016
zwanym w treści umowy **„Zamawiającym"**
reprezentowanym przez:
mgr Mariolę Dudziak – Dyrektora Szpitala
a
……....
.....
zwanym w treści umowy **„Wykonawcą"**
reprezentowanym przez:
.....

§ 1

1. Podstawą zawarcia niniejszej umowy jest rozstrzygnięcie przetargu nieograniczonego na **„Dostawa sprzętu komputerowego wraz oprogramowaniem tj.: serwerów, zestawów komputerowych, laptopów, tabletów, drukarek wraz z oprogramowaniem oraz rozbudowa obecnej infrastruktury macierzy i przełączników dla poprawy dostępności i skuteczności leczenia onkologicznego na terenie województwa dolnośląskiego na potrzeby Specjalistycznego Szpitala im. dra. Alfreda Sokołowskiego w Wałbrzychu".**
ogłoszonego w Suplemencie do Dziennika Urzędowego Unii Europejskiej w dniu …….. r., nr ogłoszenia …….
2. Specyfikacja Istotnych Warunków Zamówienia wraz z załącznikami stanowią integralne części umowy.

§ 2

1.Przedmiotem umowy jest ..... wraz z instalacją, uruchomieniem i przeszkoleniem personelu Zamawiającego zgodnie z ofertą Wykonawcy z dnia ..... 2018 r. stanowiącą załącznik do niniejszej umowy.
2. Wykonawca oświadcza, iż dostarczony przedmiot umowy pozostaje nowy i wolny od wad.

§ 3

1.Wykonawca zobowiązuje się do realizacji przedmiotu umowy określonego w § 2 tj.: dostarczenia przedmiotu umowy, jego instalacji, uruchomienia oraz przeszkolenia personelu Zamawiającego w terminie do ..... tygodni od daty zawarcia umowy.
2.Wykonawca zobowiązany jest do powiadomienia Zamawiającego o terminie dostawy przedmiotu umowy z co najmniej 3 dniowym wyprzedzeniem.
3. W przypadku dostawy przedmiotu umowy posiadającego wady Zamawiający niezwłocznie zawiadomi o tym Wykonawcę, a ten dokona jego wymiany na pełnowartościowy lub przedmiot umowy zostanie zwrócony Wykonawcy.
4. Termin rozpatrywania przez Wykonawcę ewentualnych reklamacji wynosi 5 dni robocze.
5.Wszelkie koszty związane z postępowaniem reklamacyjnym (w szczególności koszty transportu reklamowanej części lub całego przedmiotu umowy) ponosi Wykonawca.

§ 4

1.Przedmiot umowy, o którym mowa w § 2 dostarczony zostanie przez Wykonawcę transportem na jego koszt i ryzyko, w opakowaniu zabezpieczającym przedmiot dostawy przed uszkodzeniem.
2.Przedmiot umowy będzie dostarczony do siedziby Zamawiającego wraz z instrukcją obsługi i użytkowania w formie papierowej i elektronicznej w języku polskim oraz wszelką konieczną dokumentacją tj. kartą gwarancyjną, wykazem punktów serwisowych, kopiami dokumentów wraz z tłumaczeniem w przypadku oryginału w języku obcym : Certyfikat CE oraz Deklaracja Zgodności – wystawiona przez producenta
3.Dostarczony przedmiot umowy winien posiadać wszelkie świadectwa i atesty dopuszczające do użytku i stosowania na terenie RP zgodnie z obowiązującymi przepisami.
4.Potwierdzeniem wykonania przez Wykonawcę przedmiotu umowy jest protokolarne potwierdzenie przez Zamawiającego jego dostawy, instalacji, uruchomienia oraz przeszkolenia personelu Zamawiającego.
5. W w/w czynnościach ze strony Zamawiającego uczestniczyć będą:
- ……..
-……...

§ 5

1.Za wykonanie przedmiotu umowy określonego w § 2 umowy Wykonawcy przysługuje wynagrodzenie w wysokości ……zł netto (słownie: ……) + VAT w należnej wysokości.
2.Podstawą do wystawienia faktury VAT przez Wykonawcę jest protokół odbioru podpisany przez Zamawiającego, potwierdzający m.in. dostawę, instalację, uruchomienie oraz przeszkolenie personelu Zamawiającego.
3. Na fakturze Wykonawca winien wpisać nr umowy przetargowej.
4.Zapłata nastąpi w terminie do **60 dni** od daty doręczenia Zamawiającemu prawidłowo sporządzonej, zgodnie z ust. 2 faktury VAT, przelewem na rachunek bankowy Wykonawcy wskazany na fakturze.
5. Wykonawca oświadcza, że jest płatnikiem podatku od towarów i usług VAT i posiada numer identyfikacyjny NIP: .....
6.Wykonawca nie może przenieść wierzytelności wynikających z niniejszej umowy na stronę trzecią w trybie art. 509 – 518 Kodeksu Cywilnego.

§ 6

1.Wykonawca udziela gwarancji na dostarczony przedmiot umowy na okres wg Załącznika nr 1 SIWZ licząc od daty podpisania przez Zamawiającego protokołu odbioru potwierdzającego jego dostawę, instalację, uruchomienie oraz przeszkolenie personelu medycznego Zamawiającego.
2.Wykonawca na wykonane prace (nie objęte gwarancją producenta sprzętu) udziela gwarancji na okres 24 miesięcy od daty podpisania protokołu odbioru potwierdzającego zakończenie prac związanych z zamówieniem.
3.W przypadku awarii Wykonawca zobowiązuje się przystąpić do jej usunięcia w czasie nie dłuższym niż 72 godziny od daty zgłoszenia awarii.
4. Czas usunięcia awarii nie dłuższy niż 5 dni liczony od momentu podjęcia naprawy.

§ 7

1.W przypadku niewykonania bądź nienależytego wykonania umowy Wykonawca zobowiązany jest do zapłaty Zamawiającemu kary umownej w wysokości:

a) 10 % wartości wynagrodzenia określonego w § 5 ust. 1 umowy – w przypadku odstąpienia Wykonawcy od umowy, bądź odstąpienia od umowy Zamawiającego z winy Wykonawcy.

b) 1 % wartości niewykonanej dostawy – za każdy dzień zwłoki w dostawie przedmiotu umowy lub zwłoki w przystąpieniu do usunięcia awarii,

2. Zamawiający zobowiązany jest do zapłaty na rzecz Wykonawcy kary umownej w wysokości 10 % wartości niewykonanej umowy – w przypadku rozwiązania umowy przez Zamawiającego bądź przez Wykonawcę z winy Zamawiającego.

3.Zamawiającemu przysługuje prawo dochodzenia na zasadach ogólnych odszkodowań przewyższających wysokość kar umownych, o których mowa w 7 ust. 1.

§ 8

1.Zamawiający zastrzega sobie prawo do odstąpienia od umowy w trybie natychmiastowym w przypadku zwłoki Wykonawcy w wykonaniu przedmiotu umowy określonego w § 2 – powyżej 14 dni.

2.Odstąpienie od umowy z przyczyn określonych w ust. 1 uprawnia Zamawiającego od dochodzenia kar umownych i odszkodowania, zgodnie z § 7 ust. 1 i 3 umowy.

§ 9

Zamawiający zastrzega sobie prawo odstąpienia od umowy w oparciu o przepis art. 145 ustawy Prawo Zamówień Publicznych.

§ 10

Wszelkie zmiany i uzupełnienia niniejszej umowy wymagają formy pisemnej w postaci aneksu, pod rygorem nieważności.

§ 11

1. W sprawach nieuregulowanych niniejszą umową mają zastosowanie przepisy:

1) Kodeksu Cywilnego,

2) Ustawy z dnia 29.01.2004 Prawo zamówień publicznych (tekst jednolity Dz. U. z 2017, poz. 1579).

2. Wykonawca oświadcza, że zapoznał się ze standardami akredytacyjnymi Centrum Monitorowania Jakości w Ochronie Zdrowia oraz standardami ISO 9001:2015 i zobowiązuje się do realizowania umowy z zachowaniem tych standardów.

§ 12

Ewentualne spory wynikłe na tle wykonywania postanowień niniejszej umowy strony poddają rozstrzygnięciu Sądu powszechnego właściwego dla siedziby Zamawiającego.

§ 13

Umowę sporządzono w trzech jednobrzmiących egzemplarzach, dwa dla Zamawiającego, jeden dla Wykonawcy.

WYKONAWCA **ZAMAWIAJĄCY**