**specyfikacja warunków zamówienia**

**zAMAWIAJĄCY:**

Regionalny Zespół Placówek Wsparcia edukacji

Zaprasza do złożenia oferty w postępowaniu o udzielenie zamówienia publicznego prowadzonego w trybie podstawowym bez negocjacji o wartości zamówienia nie przekraczającej progów unijnych o jakich stanowi art. 3 ustawy z 11 września 2019 r. - Prawo zamówień publicznych (Dz. U. z 2022 r. poz. 1710) – dalej p.z.p.

**na dostawę infrastruktury serwerowej na potrzeby Regionalnego Zespołu Placówek Wsparcia Edukacji**

**Przedmiotowe postępowanie prowadzone jest przy użyciu środków komunikacji elektronicznej.**

Nr postępowania 9/ZP/RZPWE/2023

**12.04.2023**r**.**

**Niniejszą SWZ przedkłada do akceptacji Komisja Przetargowa w następującym składzie:**

|  |  |
| --- | --- |
| **Funkcja w Komisji Przetargowej:** | **Imię i Nazwisko:** |
| Przewodniczący Komisji | Artur Nowak |
| Członek Komisji | Krzysztof Sielchanowicz |
| Sekretarz Komisji | Bogusława Pater |

**Zatwierdzam:**

mgr Bartłomiej Piechaczek

(Kierownik Zamawiającego)

1. **NAZWA ORAZ ADRES ZAMAWIAJĄCEGO**

Regionalny Zespół Placówek Wsparcia Edukacji, ul. Głogowska 27, 45-315 Opole

tel. +48 77 404 75 30, fax +48 77 404 75 35

NIP:7543125519

http://bip.rzpwe.opolskie.pl

e-mail: [**zp@rzpwe.opolskie.pl**](mailto:zp@rzpwe.opolskie.pl)

**Adres strony internetowej, na której jest prowadzone postępowanie i na której będą dostępne wszelkie dokumenty związane z prowadzoną procedurą:** <https://platformazakupowa.pl/pn/rzpwe>

**2.OCHRONA DANYCH OSOBOWYCH**

1. Zgodnie z art. 13 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o danych) (Dz. U. UE L119 z dnia 4 maja 2016 r., str. 1; zwanym dalej „RODO”) informujemy, że:
2. administratorem Pani/Pana danych osobowych jest Regionalny Zespół Placówek Wsparcia Edukacji, ul. Głogowska 27, 45-315 Opole, tel: +48774047531, fax: +48 774047535, e-mail: [kontakt@rzpwe.opolskie.pl](mailto:kontakt@rzpwe.opolskie.pl).
3. administrator wyznaczył Inspektora Danych Osobowych, z którym można się kontaktować pod adresem e-mail: [anowak@rzpwe.opolskie.pl](mailto:anowak@rzpwe.opolskie.pl)
4. Pani/Pana dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w celu związanym z przedmiotowym postępowaniem o udzielenie zamówienia publicznego, prowadzonym w trybie podstawowym.
5. odbiorcami Pani/Pana danych osobowych będą osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania w oparciu o art. 74 ustawy p.z.p.
6. Pani/Pana dane osobowe będą przechowywane, zgodnie z art. 78 ust. 1 P.Z.P. przez okres 4 lat od dnia zakończenia postępowania o udzielenie zamówienia, a jeżeli czas trwania umowy przekracza 4 lata, okres przechowywania obejmuje cały czas trwania umowy;
7. obowiązek podania przez Panią/Pana danych osobowych bezpośrednio Pani/Pana dotyczących jest wymogiem ustawowym określonym w przepisanych ustawy P.Z.P., związanym z udziałem w postępowaniu o udzielenie zamówienia publicznego.
8. w odniesieniu do Pani/Pana danych osobowych decyzje nie będą podejmowane w sposób zautomatyzowany, stosownie do art. 22 RODO.
9. posiada Pani/Pan:
10. na podstawie art. 15 RODO prawo dostępu do danych osobowych Pani/Pana dotyczących (w przypadku, gdy skorzystanie z tego prawa wymagałoby po stronie administratora niewspółmiernie dużego wysiłku może zostać Pani/Pan zobowiązana do wskazania dodatkowych informacji mających na celu sprecyzowanie żądania, w szczególności podania nazwy lub daty postępowania o udzielenie zamówienia publicznego lub konkursu albo sprecyzowanie nazwy lub daty zakończonego postępowania o udzielenie zamówienia);
11. na podstawie art. 16 RODO prawo do sprostowania Pani/Pana danych osobowych (*skorzystanie z prawa do sprostowania nie może skutkować zmianą wyniku postępowania o udzielenie zamówienia publicznego ani zmianą postanowień umowy w zakresie niezgodnym z ustawą PZP oraz nie może naruszać integralności protokołu oraz jego załączników*);
12. na podstawie art. 18 RODO prawo żądania od administratora ograniczenia przetwarzania danych osobowych z zastrzeżeniem okresu trwania postępowania o udzielenie zamówienia publicznego lub konkursu oraz przypadków, o których mowa w art. 18 ust. 2 RODO (*prawo do ograniczenia przetwarzania nie ma zastosowania w odniesieniu do przechowywania, w celu zapewnienia korzystania ze środków ochrony prawnej lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego Unii Europejskiej lub państwa członkowskiego*);
13. prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, że przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO;
14. nie przysługuje Pani/Panu:
15. w związku z art. 17 ust. 3 lit. b, d lub e RODO prawo do usunięcia danych osobowych;
16. prawo do przenoszenia danych osobowych, o którym mowa w art. 20 RODO;
17. na podstawie art. 21 RODO prawo sprzeciwu, wobec przetwarzania danych osobowych, gdyż podstawą prawną przetwarzania Pani/Pana danych osobowych jest art. 6 ust. 1 lit. c RODO;
18. przysługuje Pani/Panu prawo wniesienia skargi do organu nadzorczego na niezgodne z RODO przetwarzanie Pani/Pana danych osobowych przez administratora. Organem właściwym dla przedmiotowej skargi jest Urząd Ochrony Danych Osobowych, ul. Stawki 2, 00-193 Warszawa.

**3.TRYB UDZIELENIA ZAMÓWIENIA**

1. Niniejsze postępowanie prowadzone jest w trybie podstawowym o jakim stanowi art. 275 pkt 1 p.z.p. oraz niniejszej Specyfikacji Warunków Zamówienia, zwaną dalej „SWZ”.
2. Zamawiający nie przewiduje wyboru najkorzystniejszej oferty z możliwością prowadzenia negocjacji.
3. Szacunkowa wartość przedmiotowego zamówienia nie przekracza progów unijnych o jakich mowa w art. 3 ustawy p.z.p.
4. Zamawiający nie przewiduje aukcji elektronicznej.
5. Zamawiający nie przewiduje złożenia oferty w postaci katalogów elektronicznych.
6. Zamawiający nie prowadzi postępowania w celu zawarcia umowy ramowej.
7. Zamawiający nie zastrzega możliwości ubiegania się o udzielenie zamówienia wyłącznie przez wykonawców, o których mowa w art. 94 p.z.p.
8. Zamawiający nie dopuszcza rozliczeń w walucie obcej.
9. Zamawiający nie określa wymagań związanych z zatrudnianiem osób, o których mowa w art. 96 ust. 2 pkt 2 p.z.p.
10. Uzasadnienie braku podziału na części: Dokonanie podziału na części nie jest możliwe ze względu na charakter i rodzaj zamówienia, ze względów technicznych i logistycznych zamówienie tworzy nierozerwalną całość. Podział na części mógłby spowodować nadmierne trudności techniczne, np. związane z potrzebą skoordynowania działań różnych wykonawców realizujących poszczególne zakresy zamówienia, co zagrażałoby jego właściwemu wykonaniu. Zbyt duże rozdrobnienie dla Zamawiającego mogłoby dodatkowo skutkować otrzymaniem wysokich cenowo ofert, dla sfinansowania których, nie byłoby pokrycia w zaplanowanym budżecie.
11. Zamawiający nie przewiduje udzielania zamówień, o których mowa w art. 214 ust. 1 pkt 7 i 8.
12. **OPIS PRZEDMIOTU ZAMÓWIENIA**
13. Wspólny Słownik Przedmiotem zamówienia jest **dostawa infrastruktury serwerowej na potrzeby Regionalnego Zespołu Placówek Wsparcia Edukacji**
14. Zamówienie nie jest podzielone na części.
15. Zamawiający nie dopuszcza składnia ofert częściowych.
16. Szczegółowy opis przedmiotu zamówienia znajduje się w załączniku nr 1 do SWZ.
17. Wymagania ogólne:
18. Zamawiający wymaga, aby dostawa sprzętu została wykonana osobiście przez Wykonawcę (osobę wyznaczoną przez Wykonawcę i działającą w jego imieniu) i odbywała się w obecności wyznaczonej osoby po stronie Zamawiającego
19. Zamawiający wymaga, aby wyposażenie dostarczone w ramach realizacji zamówienia posiadało odpowiednie certyfikaty, atesty i deklarację zgodności CE.
20. Wszystkie elementy dostarczonego sprzętu muszą być:

- fabrycznie nowe, nieużywane czy powystawowe, nieregenerowane (za materiały fabrycznie nowe uznawać należy materiały, do których produkcji zostały wykorzystane produkty w 100% nowe, nie prefabrykowane, bez śladów poprzedniego używania i uszkodzenia);

- pozbawiony wad fizycznych i prawnych oraz nie noszący śladów ich wcześniejszego używania lub uszkodzenia;

- w zakresie sprzętu komputerowego - pochodzący z montażu z linii produkcyjnej – żaden z elementów dostawy nie może być refabrykowany;

- kompletny, tj. posiadający wszelkie akcesoria, przewody, kable niezbędne do ich użytkowania oraz gotowy do użytkowania;

- gatunku „I”;

- dopuszczony do obrotu.

1. Wszystkie urządzenia muszą być oryginalnie zapakowane przez producenta, nie wycofane z produkcji. Zamawiający wymaga, by system operacyjny nie był wcześniej aktywowany lub używany na innym urządzeniu. Zamawiający wymaga, by oprogramowanie systemowe było fabrycznie zainstalowane przez producenta komputera. Zamawiający wymaga, by oprogramowanie było dostarczone wraz ze stosownymi, oryginalnymi atrybutami legalności, np. certyfikatami autentyczności.
2. Oferowany przedmiot zamówienia winien współpracować z siecią energetyczną o parametrach 230V ± 10%, 50Hz.
3. Zamawiający wymaga od Wykonawcy podania w ofercie pełnych nazw oferowanego sprzętu (producent, typ, model) wraz z jego faktycznymi parametrami technicznymi w taki sposób, by Zamawiający był w stanie stwierdzić czy zaoferowane elementy przedmiotu zamówienia spełniają wymagania określone w specyfikacji.
4. Sprzęt powinien być dostarczony, wniesiony, uruchomiony, skonfigurowany, przez Wykonawcę (osobę wyznaczoną przez Wykonawcę i działającą w jego imieniu) do siedziby Zamawiającego w Opolu (45-315) przy ul. Głogowskiej 27.
5. Zamówień: CPV: 48000000-8 - Pakiety oprogramowania i systemy informatyczne, 30200000-1 Różny sprzęt komputerowy, 48820000-2 Serwery, 31231300-0 Monitory ekranowe
6. Gwarancja min. 36 miesięcy na elementy infrastruktury wymienione w pozycjach: Grupa I: poz. 1 – serwer, poz. 2 – macierz dyskowa, poz. 4 – zapasowa macierz dyskowa, poz. 5 – serwer NAS przeznaczony do archiwizacji danych. Termin gwarancji stanowi jednocześnie kryterium pozacenowe.
7. Gwarancja min. 12 miesięcy na elementy infrastruktury wymienione w pozycjach: Grupa II: 6 zasilacz awaryjny UPS oraz poz. 10 – system zarządzania infrastrukturą sieciową. Termin gwarancji stanowi jednocześnie kryterium pozacenowe.
8. Gwarancja na pozostałe elementy nie wymienione wyżej zgodnie z opisem przedmiotu zamówienia.
9. Zamawiający wymaga aby Wykonawca udzielił Zamawiającemu serwisu technicznego/wsparcia technicznego w zakresie dostarczonego rozwiązania na min. 30 dni. Termin serwisu technicznego/wsparcia technicznego stanowi jednocześnie kryterium pozacenowe.
10. Zamawiający nie dopuszcza składania ofert wariantowych.
11. **MIEJSCE I TERMIN WYKONANIA ZAMÓWIENIA**
12. Termin realizacji zamówienia:
13. Etap I: dostawa, montaż, konfiguracja/wdrożenie i uruchomienie infrastruktury serwerowej: do 20 tygodni od dnia podpisania umowy. Termin wykonania etapu I jest jednocześnie kryterium pozacenowym.
14. Etap II: Migracja serwerów wirtualnych Windows Server w terminie do 30 dni od zakończenia prac wdrożeniowych, tj. montażu i uruchomienia infrastruktury oraz odbioru protokołem wykonanych prac wdrożeniowych.
15. Miejsce wykonania dostawy: Regionalny Zespół Placówek Wsparcia Edukacji, ul. Głogowska 27, 45-315 Opole.
16. Szczegółowe zagadnienia dotyczące realizacji umowy uregulowane są we wzorze umowy stanowiącej **załącznik nr 4 do SWZ**.
17. **WARUNKI UDZIAŁU W POSTĘPOWANIU**
18. O udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy nie podlegają wykluczeniu na zasadach określonych w Rozdziale VIII SWZ, oraz spełniają określone przez Zamawiającego warunki udziału w postępowaniu.
19. O udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy spełniają warunki dotyczące:
20. **zdolności do występowania w obrocie gospodarczym:** Zamawiający nie stawia warunku w powyższym zakresie.
21. **uprawnień do prowadzenia określonej działalności gospodarczej lub zawodowej, o ile wynika to z odrębnych przepisów:** Zamawiający nie stawia warunku w powyższym zakresie.
22. **sytuacji ekonomicznej lub finansowej:** Zamawiający nie stawia warunku w powyższym zakresie.

**zdolności technicznej lub zawodowej:** Zamawiający uzna, że Wykonawca spełnia warunek, jeżeli wykaże, że: w okresie ostatnich trzech lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy - w tym okresie, wykonał co najmniej 1 dostawę (objęta jedną umową) polegającą na dostawie infrastruktury serwerowej wraz z konfiguracją/ustawieniem i uruchomieniem dostarczonego sprzętu, o wartości (wraz z podatkiem VAT), nie mniejszej niż 700.000,00 zł (słownie: siedemset tysięcy złotych 00/100),

1. Wykonawca może polegać na zdolnościach zawodowych innych podmiotów, niezależnie od charakteru prawnego łączących go z nim stosunków prawnych.
2. Wykonawca nie może, po upływie terminu składania ofert, powoływać się na zdolności lub sytuację podmiotów udostępniających zasoby, jeżeli na etapie składania ofert nie polegał on w danym zakresie na zdolnościach lub sytuacji podmiotów udostępniających zasoby.
3. Zamawiający może na każdym etapie postępowania, uznać że wykonawca nie posiada wymaganych zdolności, jeżeli posiadanie przez wykonawcę sprzecznych interesów, w szczególności zaangażowanie zasobów technicznych lub zawodowych wykonawcy w inne przedsięwzięcia gospodarcze wykonawcy może mieć negatywny wpływ na realizację zamówienia.
4. **PODSTAWY WYKLUCZENIA Z POSTĘPOWANIA**
5. Z postępowania o udzielenie zamówienia wyklucza się Wykonawców, w stosunku do których zachodzi którakolwiek z okoliczności wskazanych: w art. 108 ust. 1, w art. 109 ust. 1 pkt. 4) ustawy pzp oraz art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego (Dz.U. poz. 835).
6. Wykluczenie Wykonawcy następuje zgodnie z art. 111 p.z.p.
7. **OŚWIADCZENIA I DOKUMENTY, JAKIE ZOBOWIĄZANI SĄ DOSTARCZYĆ WYKONAWCY W CELU POTWIERDZENIA SPEŁNIANIA WARUNKÓW UDZIAŁU W POSTĘPOWANIU ORAZ WYKAZANIA BRAKU PODSTAW WYKLUCZENIA (PODMIOTOWE ŚRODKI DOWODOWE)**
8. Do oferty Wykonawca zobowiązany jest dołączyć:
   * 1. Formularz rzeczowy stanowiący załącznik nr 2a do SWZ
     2. aktualne na dzień składania ofert oświadczenie o braku podstaw do wykluczenia z postępowania i spełnianiu warunków udziału w postępowaniu– zgodnie z Załącznikiem nr 3 do SWZ;
     3. dowód wniesienia wadium;
     4. przedmiotowe środki dowodowe,
     5. Zobowiązanie podmiotu udostępniającego zasoby do oddania mu do dyspozycji niezbędnych zasobów na potrzeby realizacji zamówienia (wzór zobowiązania stanowi załącznik nr 7 do SWZ) lub inny podmiotowy środek dowodowy potwierdzający, że wykonawca realizując zamówienie, będzie dysponował niezbędnymi zasobami tych podmiotów.
     6. oświadczenie podmiotu udostępniającego zasoby, potwierdzające brak podstaw wykluczenia tego podmiotu oraz odpowiednio spełnianie warunków udziału w postępowaniu, zgodnie z załącznikiem nr 3 do SWZ
9. Informacje zawarte w oświadczeniu, o którym mowa w pkt 1 ppkt b) stanowią wstępne potwierdzenie, że Wykonawca nie podlega wykluczeniu.
10. Zamawiający, przed wyborem najkorzystniejszej oferty wzywa wykonawcę, którego oferta została najwyżej oceniona, do złożenia w wyznaczonym terminie, nie krótszym niż 5 dni, aktualnych na dzień złożenia podmiotowych środków dowodowych:

1/ Oświadczenie wykonawcy w zakresie art. 108 ust. 1 pkt 5 ustawy Pzp, o braku przynależności do tej samej grupy kapitałowej, w rozumieniu ustawy z dnia 16.02.2017 r. o ochronie konkurencji i konsumentów (Dz. U. z 2021 r. poz. 275), z innym wykonawcą, który złożył odrębną ofertę, ofertę częściową lub wniosek o dopuszczenie do udziału w postępowaniu, albo oświadczenia o przynależności do tej samej grupy kapitałowej wraz z dokumentami lub informacjami potwierdzającymi przygotowanie oferty, oferty częściowej lub wniosku o dopuszczenie do udziału w postępowaniu niezależnie od innego wykonawcy należącego do tej samej grupy kapitałowej – załącznik nr 5 do SWZ;

2/ Odpis lub informacja z Krajowego Rejestru Sądowego lub z Centralnej Ewidencji i Informacji o Działalności Gospodarczej, w zakresie art. 109 ust. 1 pkt 4 ustawy, sporządzonych nie wcześniej niż 3 miesiące przed jej złożeniem, jeżeli odrębne przepisy wymagają wpisu do rejestru lub ewidencji.

3/ Wykaz dostaw, zgodnie z załącznikiem nr 6, wykonanych nie wcześniej niż w okresie ostatnich 3 lat, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, wraz z podaniem ich rodzaju, wartości, daty i miejsca wykonania oraz podmiotów, na rzecz których dostawy te zostały wykonane oraz załączeniem dowodów określających, czy te dostawy zostały wykonane należycie.

1. Jeżeli wykonawca ma siedzibę lub miejsce zamieszkania poza granicami Rzeczypospolitej Polskiej zamiast odpisu lub informacji z Krajowego Rejestru Sądowego lub z Centralnej Ewidencji i Informacji o Działalności Gospodarczej, o których mowa w pkt 3.2 składa dokument lub dokumenty wystawione w kraju, w którym wykonawca ma siedzibę lub miejsce zamieszkania, potwierdzające, że nie otwarto jego likwidacji, nie ogłoszono upadłości, jego aktywami nie zarządza likwidator lub sąd, nie zawarł układu z wierzycielami, jego działalność gospodarcza nie jest zawieszona ani nie znajduje się on w innej tego rodzaju sytuacji wynikającej z podobnej procedury przewidzianej w przepisach miejsca wszczęcia tej procedury, sporządzonych nie wcześniej niż 3 miesiące przed jej złożeniem.
2. Jeżeli w kraju, w którym wykonawca ma siedzibę lub miejsce zamieszkania, nie wydaje się dokumentów, o których mowa w 4, lub gdy dokumenty te nie odnoszą się do wszystkich przypadków wskazanych w SWZ, zastępuje się je odpowiednio w całości lub w części dokumentem zawierającym odpowiednio oświadczenie wykonawcy, ze wskazaniem osoby albo osób uprawnionych do jego reprezentacji, lub oświadczenie osoby, której dokument miał dotyczyć, złożone pod przysięgą, lub, jeżeli w kraju, w którym wykonawca ma siedzibę lub miejsce zamieszkania nie ma przepisów o oświadczeniu pod przysięgą, złożone przed organem sądowym lub administracyjnym, notariuszem, organem samorządu zawodowego lub gospodarczego, właściwym ze względu na siedzibę lub miejsce zamieszkania wykonawcy.
3. W odniesieniu do warunków dotyczących wykształcenia, kwalifikacji zawodowych lub doświadczenia Wykonawcy wspólnie ubiegający się o udzielenie zamówienia mogą polegać na zdolnościach tych z Wykonawców, którzy wykonają usługi, do realizacji których te zdolności są wymagane.
4. Wykonawca może w celu potwierdzenia spełniania warunków udziału w postępowaniu, w stosownych sytuacjach oraz w odniesieniu do konkretnego zamówienia, lub jego części, polegać na zdolnościach technicznych lub zawodowych podmiotów udostępniających zasoby, niezależnie od charakteru prawnego łączących go z nimi stosunków prawnych
5. W odniesieniu do warunków dotyczących wykształcenia, kwalifikacji zawodowych lub doświadczenia, Wykonawcy mogą polegać na zdolnościach podmiotów udostępniających zasoby, jeśli podmioty te wykonają usługi, do realizacji których te zdolności są wymagane.
6. Wykonawca nie jest zobowiązany do złożenia podmiotowych środków dowodowych, które zamawiający posiada, jeżeli wykonawca wskaże te środki oraz potwierdzi ich prawidłowość i aktualność.
7. Zamawiający nie wzywa do złożenia podmiotowych środków dowodowych, jeżeli:
   * 1. może je uzyskać za pomocą bezpłatnych i ogólnodostępnych baz danych, w szczególności rejestrów publicznych w rozumieniu ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, o ile wykonawca wskazał w oświadczeniu, o którym mowa w art. 125 ust. 1 p.z.p dane umożliwiające dostęp do tych środków;
     2. podmiotowym środkiem dowodowym jest oświadczenie, którego treść odpowiada zakresowi oświadczenia, o którym mowa w art. 125 ust. 1.
8. W zakresie nieuregulowanym ustawą p.z.p. lub niniejszą SWZ do oświadczeń i dokumentów składanych przez Wykonawcę w postępowaniu zastosowanie mają w szczególności przepisy rozporządzenia Ministra Rozwoju Pracy i Technologii z dnia 23 grudnia 2020 r. w sprawie podmiotowych środków dowodowych oraz innych dokumentów lub oświadczeń, jakich może żądać zamawiający od wykonawcy oraz rozporządzenia Prezesa Rady Ministrów z dnia 30 grudnia 2020 r. w sprawie sposobu sporządzania i przekazywania informacji oraz wymagań technicznych dla dokumentów elektronicznych oraz środków komunikacji elektronicznej w postępowaniu o udzielenie zamówienia publicznego lub konkursie.
9. **PRZEDMIOTOWE ŚRODKI DOWODOWE**
10. Zamawiający wymaga złożenia wraz z ofertą następujących przedmiotowych środków dowodowych: opisów technicznych sporządzonych przez producenta i/lub wydruki ze stron internetowych producenta, bądź katalogi producentów pozwalające na ocenę zgodności oferowanych materiałów oraz ich parametrów z wymaganiami SWZ. Wykonawca winien w niniejszych materiałach jednoznacznie wskazać której pozycji dotyczą materiały.
11. Zamawiający zaakceptuje równoważne przedmiotowe środki dowodowe, jeśli potwierdzą one, że oferowane dostawy spełniają określone przez zamawiającego wymagania.
12. Jeżeli wykonawca nie złożył przedmiotowych środków dowodowych lub złożone przedmiotowe środki dowodowe są niekompletne, zamawiający wzywa do ich złożenia lub uzupełnienia w wyznaczonym terminie.
13. Przepisu ust. 2 nie stosuje się, jeżeli przedmiotowy środek dowodowy służy potwierdzeniu zgodności z cechami lub kryteriami określonymi w opisie kryteriów oceny ofert lub, pomimo złożenia przedmiotowego środka dowodowego, oferta podlega odrzuceniu albo zachodzą przesłanki unieważnienia postępowania.
14. Zamawiający może żądać od wykonawców wyjaśnień dotyczących treści przedmiotowych środków dowodowych.
15. **INFORMACJA DLA WYKONAWCÓW WSPÓLNIE UBIEGAJĄCYCH SIĘ O UDZIELENIE ZAMÓWIENIA (SPÓŁKI CYWILNE/ KONSORCJA)**
16. Wykonawcy mogą wspólnie ubiegać się o udzielenie zamówienia. W takim przypadku Wykonawcy ustanawiają pełnomocnika do reprezentowania ich w postępowaniu albo do reprezentowania i zawarcia umowy w sprawie zamówienia publicznego. Pełnomocnictwowinno być załączone do oferty.
17. W przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia, oświadczenia, o których mowa w Rozdziale VIII ust. 1 SWZ, składa każdy z wykonawców. Oświadczenia te potwierdzają brak podstaw wykluczenia oraz spełnianie warunków udziału w zakresie, w jakim każdy z wykonawców wykazuje spełnianie warunków udziału w postępowaniu.
18. Oświadczenia i dokumenty potwierdzające brak podstaw do wykluczenia z postępowania składa każdy z Wykonawców wspólnie ubiegających się o zamówienie.
19. W terminie określonym w Rozdziale VIII ust. 3, każdy z wykonawców wspólnie ubiegających się o udzielenie zamówienia składa oddzielnie:
    * 1. oświadczenie wykonawcy w zakresie art. 108 ust. 1 pkt 5 ustawy Pzp, o braku przynależności do tej samej grupy kapitałowej (pkt 8.3.1 SWZ),
      2. odpis lub informacja z Krajowego Rejestru Sądowego lub z Centralnej Ewidencji i Informacji o Działalności Gospodarczej, w zakresie art. 109 ust. 1 pkt 4 ustawy, sporządzonych nie wcześniej niż 3 miesiące przed jej złożeniem, jeżeli odrębne przepisy wymagają wpisu do rejestru lub ewidencji
20. Zgodnie z art. 117 ust. 4, wykonawcy wspólnie ubiegający się o udzielenie zamówienia w treści formularza ofertowego wskazują, które usługi wykonają poszczególni wykonawcy.
21. Zamawiający przed zawarciem umowy w sprawie zamówienia publicznego żąda kopii umowy regulującej współpracę wykonawców wspólnie ubiegających się o udzielenie zamówienia
22. **SPOSÓB KOMUNIKACJI ORAZ WYJAŚNIENIA TREŚCI SWZ**
23. Komunikacja w postępowaniu o udzielenie zamówienia, w tym składanie ofert w postępowaniu, wymiana informacji oraz przekazywanie dokumentów lub oświadczeń między zamawiającym a wykonawcą, z uwzględnieniem wyjątków określonych w ustawie p.z.p., odbywa się przy użyciu środków komunikacji elektronicznej, tj. przy użyciu Platformy zakupowej, która jest dostępna pod adresem: <https://platformazakupowa.pl/pn/rzpwe> oraz poczty elektronicznej [zp@rzpwe.opolskie.pl](mailto:zp@rzpwe.opolskie.pl)
24. Zamawiający będzie przekazywał Wykonawcom informacje w formie elektronicznej za pośrednictwem Platformy. Informacje dotyczące odpowiedzi na pytania, zmiany SWZ, zmiany terminu składania i otwarcia ofert Zamawiający będzie zamieszczał na Platformie w sekcji „Komunikaty”. Korespondencja, której zgodnie z obowiązującymi przepisami adresatem jest konkretny Wykonawca, będzie przekazywana w formie elektronicznej za pośrednictwem Platformy do konkretnego Wykonawcy.
25. Ofertę, oświadczenia, o których mowa w art. 125 ust. 1 p.z.p., przedmiotowe środki dowodowe, pełnomocnictwa, zobowiązanie podmiotu udostępniającego zasoby sporządza się w postaci elektronicznej, w ogólnie dostępnych formatach danych, w szczególności w formatach .txt, .rtf, .pdf, .doc, .docx, .odt. Ofertę, a także oświadczenie o jakim mowa w Rozdziale VIII ust. 1 SWZ składa się, pod rygorem nieważności, w formie elektronicznej lub w postaci elektronicznej opatrzonej podpisem zaufanym lub podpisem osobistym.
26. Wymagania techniczne i organizacyjne wysyłania i odbierania dokumentów elektronicznych, elektronicznych kopii dokumentów i oświadczeń oraz informacji przekazywanych przy ich użyciu opisane zostały w zakładce „Instrukcje dla Wykonawców” na stronie internetowej pod adresem: <https://platformazakupowa.pl/strona/45-instrukcje>
27. Osobą uprawnioną do porozumiewania się z Wykonawcami jest:

a) w zakresie merytorycznym: Artur Nowak, e-mail: [anowak@rzpwe.opolskie.pl](mailto:anowak@rzpwe.opolskie.pl), tel. 774047540 i proceduralnym: Bogusława Pater, e-mail: [bpater@rzpwe.opolskie.pl](mailto:bpater@rzpwe.opolskie.pl); tel.: 774047537

1. W korespondencji kierowanej do Zamawiającego Wykonawcy powinni posługiwać się numerem przedmiotowego postępowania.
2. Wykonawca może zwrócić się do zamawiającego z wnioskiem o wyjaśnienie treści SWZ.
3. Zamawiający jest obowiązany udzielić wyjaśnień niezwłocznie, jednak nie później niż na 2 dni przed upływem terminu składania odpowiednio ofert, pod warunkiem że wniosek o wyjaśnienie treści SWZ wpłynął do zamawiającego nie później niż na 4 dni przed upływem terminu składania odpowiednio ofert.
4. Jeżeli zamawiający nie udzieli wyjaśnień w terminie, o którym mowa w ust. 9, przedłuża termin składania ofert o czas niezbędny do zapoznania się wszystkich zainteresowanych wykonawców z wyjaśnieniami niezbędnymi do należytego przygotowania i złożenia ofert. W przypadku gdy wniosek o wyjaśnienie treści SWZ nie wpłynął w terminie, o którym mowa w ust. 9, zamawiający nie ma obowiązku udzielania wyjaśnień SWZ oraz obowiązku przedłużenia terminu składania ofert.
5. Przedłużenie terminu składania ofert, o których mowa w ust. 10, nie wpływa na bieg terminu składania wniosku o wyjaśnienie treści SWZ.
6. **OPIS SPOSOBU PRZYGOTOWANIA OFERT ORAZ WYMAGANIA FORMALNE DOTYCZĄCE SKŁADANYCH OŚWIADCZEŃ I DOKUMENTÓW**
7. Wykonawca może złożyć tylko jedną ofertę.
8. Treść oferty musi odpowiadać treści SWZ.
9. Ofertę składa się na Formularzu Ofertowym – zgodnie z **Załącznikiem nr 2 do SWZ**. Wraz z ofertą Wykonawca jest zobowiązany złożyć:
10. oświadczenia, o których mowa w Rozdziale VIII ust. 1 SWZ;
11. dowód wniesienia wadium,
12. formularz rzeczowy (zał. 2a do SWZ),
13. przedmiotowe środki dowodowe,
14. zobowiązanie podmiotu udostępniającego zasoby (zał. Nr 7 do SWZ)
15. dokumenty, z których wynika prawo do podpisania oferty; odpowiednie pełnomocnictwa (jeżeli dotyczy).;
16. Oferta powinna być podpisana przez osobę upoważnioną do reprezentowania Wykonawcy, zgodnie z formą reprezentacji Wykonawcy określoną w rejestrze lub innym dokumencie, właściwym dla danej formy organizacyjnej Wykonawcy albo przez upełnomocnionego przedstawiciela Wykonawcy. W celu potwierdzenia, że osoba działająca w imieniu wykonawcy jest umocowana do jego reprezentowania, zamawiający żąda od wykonawcy odpisu lub informacji z Krajowego Rejestru Sądowego, Centralnej Ewidencji i Informacji o Działalności Gospodarczej lub innego właściwego rejestru.
17. Oferta oraz pozostałe oświadczenia i dokumenty, dla których Zamawiający określił wzory w formie formularzy zamieszczonych w załącznikach do SWZ, powinny być sporządzone zgodnie z tymi wzorami.
18. **Ofertę składa się pod rygorem nieważności w formie elektronicznej lub w postaci elektronicznej opatrzonej podpisem zaufanym lub podpisem osobistym.**
19. Oferta powinna być sporządzona w języku polskim.
20. Jeśli oferta zawiera informacje stanowiące tajemnicę przedsiębiorstwa w rozumieniu ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2022 r. poz. 1233), Wykonawca w celu utrzymania w poufności tych informacji, przekazuje je w wydzielonym i odpowiednio oznaczonym pliku, wraz z jednoczesnym zastrzeżeniem polecenia „ Załącznik stanowiący tajemnicę przedsiębiorstwa”, a następnie wraz z plikami stanowiącymi jawną część oferty, należy ten plik zaszyfrować.
21. Przed upływem terminu składania ofert, Wykonawca może wprowadzić zmiany do złożonej oferty lub wycofać ofertę. W tym celu należy w systemie Platformy kliknąć przycisk „Wycofaj ofertę”. Zmiana oferty następuje poprzez wycofanie oferty oraz jej ponownym złożeniu.
22. Oferta może być złożona do upływu terminu składania ofert.
23. Podmiotowe środki dowodowe lub inne dokumenty, w tym dokumenty potwierdzające umocowanie do reprezentowania, sporządzone w języku obcym przekazuje się wraz z tłumaczeniem na język polski.
24. Wszystkie koszty związane z uczestnictwem w postępowaniu, w szczególności z przygotowaniem i złożeniem oferty ponosi Wykonawca składający ofertę. Zamawiający nie przewiduje zwrotu kosztów udziału w postępowaniu.
25. **SPOSÓB OBLICZENIA CENY OFERTY**
26. Wykonawca podaje cenę za realizację przedmiotu zamówienia zgodnie ze wzorem Formularza Ofertowego, stanowiącego **Załącznik nr 2 do SWZ.**
27. Cena ofertowa brutto musi uwzględniać wszystkie koszty związane z realizacją przedmiotu zamówienia zgodnie z opisem przedmiotu zamówienia oraz istotnymi postanowieniami umowy określonymi w niniejszej SWZ.
28. Cena podana na Formularzu Ofertowym jest ceną ostateczną, niepodlegającą negocjacji i wyczerpującą wszelkie należności Wykonawcy wobec Zamawiającego związane z realizacją przedmiotu zamówienia.
29. Cena oferty powinna być wyrażona w złotych polskich (PLN) z dokładnością do dwóch miejsc po przecinku.
30. Zamawiający nie przewiduje rozliczeń w walucie obcej.
31. Wyliczona cena oferty brutto będzie służyć do porównania złożonych ofert i do rozliczenia w trakcie realizacji zamówienia.
32. Jeżeli została złożona oferta, której wybór prowadziłby do powstania u zamawiającego obowiązku podatkowego zgodnie z ustawą z dnia 11 marca 2004 r. o podatku od towarów i usług (Dz. U. z 2022 r., poz. 931), dla celów zastosowania kryterium ceny lub kosztu zamawiający dolicza do przedstawionej w tej ofercie ceny kwotę podatku od towarów i usług, którą miałby obowiązek rozliczyć.W ofercie, o której mowa w ust. 1, wykonawca ma obowiązek:

1) poinformowania zamawiającego, że wybór jego oferty będzie prowadził do powstania u zamawiającego obowiązku podatkowego;

2) wskazania nazwy (rodzaju) towaru lub usługi, których dostawa lub świadczenie będą prowadziły do powstania obowiązku podatkowego;

3) wskazania wartości towaru lub usługi objętego obowiązkiem podatkowym zamawiającego, bez kwoty podatku;

4) wskazania stawki podatku od towarów i usług, która zgodnie z wiedzą wykonawcy, będzie miała zastosowanie.

1. Wzór Formularza Ofertowego został opracowany przy założeniu, iż wybór oferty nie będzie prowadzić do powstania u Zamawiającego obowiązku podatkowego w zakresie podatku VAT. W przypadku, gdy Wykonawca zobowiązany jest złożyć oświadczenie o powstaniu u Zamawiającego obowiązku podatkowego, to winien odpowiednio zmodyfikować treść formularza.
2. **WYMAGANIA DOTYCZĄCE WADIUM**
   1. Zamawiający wymaga wniesienia wadium w wysokości 7.500,00 zł (słownie: siedem tysięcy pięćset złotych 00/100).
   2. Wadium wnosi się przed upływem terminu składania ofert i utrzymuje nieprzerwanie do dnia upływu terminu związania ofertą, z wyjątkiem przypadków, o których mowa w art. 98 ust. 1 pkt 2 i 3 oraz ust. 2.
   3. Wadium może być wnoszone według wyboru Wykonawcy w jednej lub kilku następujących formach:
      1. pieniądzu;
      2. gwarancjach bankowych;
      3. gwarancjach ubezpieczeniowych;
      4. 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 (Dz. U. z 2022r. poz. 2185 z późn. zm.).
   4. Wadium w formie pieniądza należy wnieść przelewem na konto nr rachunku 41 1160 2202 0000 0003 0943 9087z dopiskiem "Wadium - nr postępowania 9/ZP/RZPWE/2023 pn.: „Dostawa infrastruktury serwerowej na potrzeby RZPWE”. UWAGA: Za termin wniesienia wadium w formie pieniężnej zostanie przyjęty termin uznania rachunku Zamawiającego.
   5. Wadium wnoszone w formie poręczeń lub gwarancji musi spełniać co najmniej poniższe wymagania:

musi obejmować odpowiedzialność za wszystkie przypadki powodujące utratę wadium przez Wykonawcę określone w p.z.p., bez potwierdzania tych okoliczności;

z jej treści powinno jednoznacznie wynikać zobowiązanie gwaranta do zapłaty całej kwoty wadium;

powinno być nieodwołalne i bezwarunkowe oraz płatne na pierwsze żądanie;

termin obowiązywania poręczenia lub gwarancji nie może być krótszy niż termin związania ofertą (z zastrzeżeniem iż pierwszym dniem związania ofertą jest dzień składania ofert);

w treści poręczenia lub gwarancji powinna znaleźć się nazwa oraz numer przedmiotowego postępowania;

beneficjentem poręczenia lub gwarancji jest: Regionalny Zespół Placówek Wsparcia Edukacji, ul. Głogowska 27, 45-315 Opole

w przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia (art. 58 p.z.p.), Zamawiający wymaga aby poręczenie lub gwarancja obejmowała swą treścią (tj. zobowiązanych z tytułu poręczenia lub gwarancji) wszystkich Wykonawców wspólnie ubiegających się o udzielenie zamówienia lub aby z jej treści wynikało, że zabezpiecza ofertę Wykonawców wspólnie ubiegających się o udzielenie zamówienia (konsorcjum);

musi zostać złożone w postaci elektronicznej, opatrzone kwalifikowanym podpisem elektronicznym przez wystawcę poręczenia lub gwarancji.

* 1. W przypadku wniesienia wadium w formie:

1) pieniężnej - zaleca się, by dowód dokonania przelewu został dołączony do oferty;

2) poręczeń lub gwarancji - wymaga się, by oryginał dokumentu został złożony wraz z ofertą.

* 1. Oferta wykonawcy, który nie wniesie wadium lub wniesie w sposób nieprawidłowy lub nie utrzyma wadium nieprzerwanie do upływu terminu związania ofertą lub złoży wniosek o zwrot wadium w przypadku, o którym mowa w art. 98 ust. 2 pkt 3 p.z.p. zostanie odrzucona;
  2. Zasady zwrotu oraz okoliczności zatrzymania wadium określa pzp.

1. **TERMIN ZWIĄZANIA OFERTĄ**
   1. Wykonawca będzie związany ofertą przez okres **30 dni**, tj. do dnia 19.05.2023r. Bieg terminu związania ofertą rozpoczyna się wraz z upływem terminu składania ofert.
   2. W przypadku gdy wybór najkorzystniejszej oferty nie nastąpi przed upływem terminu związania ofertą wskazanego w ust. 1, Zamawiający przed upływem terminu związania ofertą zwraca się jednokrotnie do wykonawców o wyrażenie zgody na przedłużenie tego terminu o wskazywany przez niego okres, nie dłuższy niż 30 dni.
   3. Przedłużenie terminu związania ofertą wymaga złożenia przez wykonawcę pisemnego oświadczenia o wyrażeniu zgody na przedłużenie terminu związania ofertą.
   4. Odmowa wyrażenia zgody na przedłużenie terminu związania ofertą nie powoduje utraty wadium.
2. **SPOSÓB I TERMIN SKŁADANIA I OTWARCIA OFERT**
   * + 1. Wykonawca składa ofertę za pośrednictwem platformy zakupowej dostępnej pod adresem: <https://platformazakupowa.pl/pn/rzpwe> za pomocą dedykowanych formularzy do złożenia, zmiany wycofania oferty lub wniosku.
       2. Sposób złożenia oferty opisany został w zakładce „Instrukcje dla Wykonawców” na stronie internetowej pod adresem: <https://platformazakupowa.pl/strona/45-instrukcje>
       3. **Ofertę należy złożyć do dnia 20.04.2023r. do godziny 09:00.**
       4. **Otwarcie ofert nastąpi w dniu 20.04.2023r. o godzinie 09:15.**
       5. Najpóźniej przed otwarciem ofert, udostępnia się na stronie internetowej prowadzonego postępowania informację o kwocie, jaką zamierza się przeznaczyć na sfinansowanie zamówienia.
       6. Niezwłocznie po otwarciu ofert, udostępnia się na stronie internetowej prowadzonego postępowania informacje o:
     1. nazwach albo imionach i nazwiskach oraz siedzibach lub miejscach prowadzonej działalności gospodarczej albo miejscach zamieszkania wykonawców, których oferty zostały otwarte;
     2. cenach lub kosztach zawartych w ofertach.
3. **OPIS KRYTERIÓW OCENY OFERT, WRAZ Z PODANIEM WAG TYCH KRYTERIÓW I SPOSOBU OCENY OFERT**

Przy wyborze najkorzystniejszej oferty Zamawiający będzie się kierował następującymi kryteriami oceny ofert:

cena (oferty brutto) - 60 %

cena najniższa spośród złożonych ofert

cena = --------------------------------------------------------- x 60

cena oferty badanej

Liczba punktów badanej oferty w kryterium cenowym (wynosi maksymalnie 60 pkt).

Termin dostawy - realizacji etapu I tj. dostawa, montaż, konfiguracja/wdrożenie i uruchomienie infrastruktury serwerowej – 20%

Wykonawca jest zobowiązany w ofercie podać (w tygodniach) termin dostawy infrastruktury serwerowej - realizacji Etapu I: dostawa, montaż, konfiguracja/wdrożenie.

Maksymalny czas dostawy to 20 tygodni, minimalny możliwy do wpisania termin to 10 tygodni.

Zaproponowanie terminu realizacji w przedziale od 11 do 20 tygodni będzie podlegałopunktacji według poniższego wzoru:

Najkrótszy termin dostawy ofert

nie podlegających odrzuceniu

Liczba punktów = ------------------------------------------------------ x 20

Termin dostawy badanej oferty

Liczba punktów badanej oferty w kryterium: termin dostawy wynosi maksymalnie 20 pkt.

Jeżeli Wykonawca w formularzu oferty nie wpisze żadnej wartości dotyczącej oferowanego terminu dostawy, Zamawiający przyjmie że Wykonawca oferuje maksymalny możliwy termin dostawy tj 20 tygodni i Wykonawca w tym kryterium oceny ofert otrzyma 0 punktów.

Termin gwarancji– 10 %

Wykonawca zobowiązany jest podać w ofercie okres gwarancji jaki udzieli na wykonany przedmiot umowy w miesiącach, na zaoferowany następujący przedmiot zamówienia:

- Gwarancja minimum 36 miesięcy (Grupa I) na elementy infrastruktury wymienione w pozycjach: poz. 1 – serwer,   
poz. 2 – macierz dyskowa, poz. 4 – zapasowa macierz dyskowa, poz. 5 – serwer NAS przeznaczony do archiwizacji danych.

- Gwarancja minimum 12 miesięcy (Grupa II) na elementy infrastruktury wymienione w pozycjach: poz. 6 - zasilacz awaryjny UPS oraz poz. 10 – system zarządzania infrastrukturą sieciową.

W kryterium tym można otrzymać maksymalnie 10 punktów po 5 za gwarancję z każdej grupy (poz. 1,2,4,5 – grupa I; poz 6 i 10 – grupa II). Z dwóch wyników zostanie wyciągnięta średnia arytmetyczna.

UWAGA!! Zaoferowany okres gwarancji, w przypadku większej liczby pozycji urządzeń podlegających punktacji, musi być jednakowy dla wszystkich produktów w wymienionych pozycjach.

W przypadku zaoferowania różnych okresów gwarancji, Zamawiający jako właściwy do punktacji przyjmie najkrótszy okres spośród wymienionych.

Okres gwarancji należy podać w pełnych miesiącach.

Maksymalny okres gwarancji w obu grupach produktów (poz. 1,2,4,5 oraz poz. 6 i 10) wynosi 60 miesięcy od dnia podpisania protokołu odbioru końcowego.

Grupa I: Zaproponowanie okresu gwarancji w przedziale od 37 do 60 miesięcy będzie podlegało punktacji według poniższego wzoru:

Grupa II: Zaproponowanie okresu gwarancji w przedziale od 13 do 60 miesięcy będzie podlegało punktacji według poniższego wzoru:

Okres gwarancji badanej oferty

Liczba punktów = ------------------------------------------------------------------- x 10

Najdłuższy okres gwarancji spośród ofert

nie podlegających odrzuceniu

Jeżeli Wykonawca w formularzu oferty nie wpisze żadnej wartości dotyczącej oferowanego czasu gwarancji, Zamawiający przyjmie że Wykonawca oferuje minimalny wymagany okres gwarancji tj 36 miesięcy (Grupa I: poz. 1,2,4,5) i 12 miesięcy (Grupa II: poz. 6 i 10) i Wykonawca w tym kryterium oceny ofert otrzyma 0 punktów.

Wsparcie techniczne/serwis techniczny – 10%

Wykonawca jest zobowiązany w ofercie podać czas oferowanego wsparcia technicznego/serwisu technicznego, Minimalny czas wsparcia technicznego wynosi: 30 dni. Maksymalny możliwy termin wsparcia technicznego wynosi: 90 dni.

Jeżeli Wykonawca w formularzu oferty nie wpisze żadnej wartości dotyczącej oferowanego czasu wsparcia technicznego Zamawiający przyjmie że Wykonawca proponuje minimalny możliwy czas wsparcia technicznego tj 30 dni i Wykonawca w tym kryterium otrzyma 0 punktów.

Zaproponowanie terminu wsparcia technicznego w przedziale od 31 do 90 dni będzie podlegałopunktacji według poniższego wzoru:

Czas udzielonego wsparcia technicznego

badanej oferty

Liczba punktów = ------------------------------------------------------------------------- x 10

Najdłuższy Czas udzielonego wsparcia technicznego

ofert nie podlegających odrzuceniu

Liczba punktów w kryterium termin dostawy wynosi maksymalnie 10 punktów

Zamawiający uzna za najkorzystniejszą ofertę Wykonawcy, jeśli Wykonawca ten nie będzie podlegać wykluczeniu a jego oferta nie będzie podlegać odrzuceniu, który otrzyma największą liczbę punków wyliczoną zgodnie ze wzorem:

P = P1 + P2 + P3 + P4

gdzie:

P – łączna liczba punktów dla ocenianej oferty

P1 – liczba punktów przyznana ofercie ocenianej w kryterium Cena

P2 – liczba punktów przyznana ofercie ocenianej w kryterium Termin dostawy

P3 – liczba punktów przyznana ofercie ocenianej w kryterium Termin gwarancji

P4 – liczba punktów przyznana ofercie ocenianej w kryterium Wsparcie techniczne/serwis techniczny

Punkty będą zaokrąglane do dwóch miejsc po przecinku lub z większą dokładnością jeżeli przy zastosowaniu wymienionego zaokrąglenia nie występuje różnica w liczbie przyznanych punktów wynikająca z małej różnicy zaoferowanych cen. Jeśli nie będzie można wybrać najkorzystniejszej oferty z uwagi na to, że dwie lub więcej ofert przedstawia taki sam bilans punktów, Zamawiający spośród tych ofert wybiera ofertę z niższą ceną.

Cena ofertowa brutto musi uwzględniać wszelkie koszty jakie Wykonawca poniesie w związku z realizacją przedmiotu zamówienia.

W toku badania i oceny ofert Zamawiający może żądać od Wykonawcy wyjaśnień dotyczących treści złożonej oferty, w tym zaoferowanej ceny.

Zamawiający udzieli zamówienia Wykonawcy, którego oferta zostanie uznana za najkorzystniejszą.

1. **INFORMACJE O FORMALNOŚCIACH, JAKIE POWINNY BYĆ DOPEŁNIONE PO WYBORZE OFERTY W CELU ZAWARCIA UMOWY W SPRAWIE ZAMÓWIENIA PUBLICZNEGO**
2. Zamawiający zawiera umowę w sprawie zamówienia publicznego w terminie nie krótszym niż 5 dni od dnia przesłania zawiadomienia o wyborze najkorzystniejszej oferty.
3. Zamawiający może zawrzeć umowę w sprawie zamówienia publicznego przed upływem terminu, o którym mowa w ust. 1, jeżeli w postępowaniu o udzielenie zamówienia prowadzonym w trybie podstawowym złożono tylko jedną ofertę.
4. W przypadku wyboru oferty złożonej przez Wykonawców wspólnie ubiegających się o udzielenie zamówienia Zamawiający zastrzega sobie prawo żądania przed zawarciem umowy w sprawie zamówienia publicznego umowy regulującej współpracę tych Wykonawców.
5. Wykonawca będzie zobowiązany do podpisania umowy w miejscu i terminie wskazanym przez Zamawiającego.
6. **WYMAGANIA DOTYCZĄCE ZABEZPIECZENIA NALEŻYTEGO WYKONANIA UMOWY**
   * + 1. Zamawiający wymaga wniesienia zabezpieczenia należytego wykonania umowy.
       2. Zabezpieczenie służy pokryciu roszczeń z tytułu niewykonania lub nienależytego wykonania umowy.
       3. Zabezpieczenie wnosi się przed zawarciem umowy.
       4. Zabezpieczenie może być wnoszone, według wyboru wykonawcy, w jednej lub w kilku następujących formach:

1) pieniądzu;

2) poręczeniach bankowych lub poręczeniach spółdzielczej kasy oszczędnościowo-kredytowej, z tym że zobowiązanie kasy jest zawsze zobowiązaniem 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.

* + - 1. Zabezpieczenie wnoszone w pieniądzu wykonawca wpłaca przelewem na rachunek bankowy wskazany przez zamawiającego.
      2. W przypadku wniesienia wadium w pieniądzu wykonawca może wyrazić zgodę na zaliczenie kwoty wadium na poczet zabezpieczenia.
      3. Jeżeli zabezpieczenie wniesiono w pieniądzu, zamawiający przechowuje je na oprocentowanym rachunku bankowym. Zamawiający zwraca zabezpieczenie wniesione w pieniądzu z odsetkami wynikającymi z umowy rachunku bankowego, na którym było ono przechowywane, pomniejszone o koszt prowadzenia tego rachunku oraz prowizji bankowej za przelew pieniędzy na rachunek bankowy wykonawcy.
      4. W trakcie realizacji umowy wykonawca może dokonać zmiany formy zabezpieczenia na jedną lub kilka form, o których mowa w art. 450 ust. 1 ustawy z dnia 11.09.2019r. Prawo zamówień publicznych (Dz.U.z 2022r., poz. 1710).
      5. Zmiana formy zabezpieczenia jest dokonywana z zachowaniem ciągłości zabezpieczenia i bez zmniejszenia jego wysokości.
      6. Wysokość zabezpieczenia ustala się w stosunku procentowym do ceny całkowitej podanej w ofercie albo maksymalnej wartości nominalnej zobowiązania zamawiającego wynikającego z umowy, jeżeli w ofercie podano cenę jednostkową lub ceny jednostkowe.
      7. Zabezpieczenie ustala się w wysokości nieprzekraczającej 5% ceny całkowitej podanej w ofercie albo maksymalnej wartości nominalnej zobowiązania zamawiającego wynikającego z umowy.

1. **INFORMACJE O TREŚCI ZAWIERANEJ UMOWY ORAZ MOŻLIWOŚCI JEJ ZMIANY**
2. Wybrany Wykonawca jest zobowiązany do zawarcia umowy w sprawie zamówienia publicznego na warunkach określonych we Wzorze Umowy, stanowiącym **Załącznik nr 4 do SWZ**.
3. Zakres świadczenia Wykonawcy wynikający z umowy jest tożsamy z jego zobowiązaniem zawartym w ofercie.
4. Zamawiający przewiduje możliwość zmiany zawartej umowy w stosunku do treści wybranej oferty w zakresie uregulowanym w art. 454-455 p.z.p. oraz wskazanym we Wzorze Umowy, stanowiącym **Załącznik nr 4 do SWZ**.
5. Zmiana umowy wymaga dla swej ważności, pod rygorem nieważności, zachowania formy pisemnej.
6. **POUCZENIE O ŚRODKACH OCHRONY PRAWNEJ PRZYSŁUGUJĄCYCH WYKONAWCY**
7. Środki ochrony prawnej określone w niniejszym dziale przysługują wykonawcy, uczestnikowi konkursu oraz innemu podmiotowi, jeżeli ma lub miał interes w uzyskaniu zamówienia lub nagrody w konkursie oraz poniósł lub może ponieść szkodę w wyniku naruszenia przez zamawiającego przepisów ustawy p.z.p.
8. Środki ochrony prawnej wobec ogłoszenia wszczynającego postępowanie o udzielenie zamówienia lub ogłoszenia o konkursie oraz dokumentów zamówienia przysługują również organizacjom wpisanym na listę, o której mowa w art. 469 pkt 15 p.z.p. oraz Rzecznikowi Małych i Średnich Przedsiębiorców.
9. Odwołanie przysługuje na:
   * + - 1. niezgodną z przepisami ustawy czynność Zamawiającego, podjętą w postępowaniu o udzielenie zamówienia, w tym na projektowane postanowienie umowy;
         2. zaniechanie czynności w postępowaniu o udzielenie zamówienia do której zamawiający był obowiązany na podstawie ustawy;
10. Odwołanie wnosi się do Prezesa Izby. Odwołujący przekazuje kopię odwołania zamawiającemu przed upływem terminu do wniesienia odwołania w taki sposób, aby mógł on zapoznać się z jego treścią przed upływem tego terminu.

5. Odwołanie wobec treści ogłoszenia lub treści SWZ wnosi się w terminie 5 dni od dnia zamieszczenia ogłoszenia w Biuletynie Zamówień Publicznych lub treści SWZ na stronie internetowej.

6. Odwołanie wnosi się w terminie:

1) 5 dni od dnia przekazania informacji o czynności zamawiającego stanowiącej podstawę jego wniesienia, jeżeli informacja została przekazana przy użyciu środków komunikacji elektronicznej,

2) 10 dni od dnia przekazania informacji o czynności zamawiającego stanowiącej podstawę jego wniesienia, jeżeli informacja została przekazana w sposób inny niż określony w pkt 1).

* + - 1. Odwołanie w przypadkach innych niż określone w pkt 5 i 6 wnosi się w terminie 5 dni od dnia, w którym powzięto lub przy zachowaniu należytej staranności można było powziąć wiadomość o okolicznościach stanowiących podstawę jego wniesienia
      2. Na orzeczenie Izby oraz postanowienie Prezesa Izby, o którym mowa w art. 519 ust. 1 ustawy p.z.p., stronom oraz uczestnikom postępowania odwoławczego przysługuje skarga do sądu.

1. W postępowaniu toczącym się wskutek wniesienia skargi stosuje się odpowiednio przepisy ustawy z dnia 17 listopada 1964 r. - Kodeks postępowania cywilnego o apelacji, jeżeli przepisy niniejszego rozdziału nie stanowią inaczej.
2. Skargę wnosi się do Sądu Okręgowego w Warszawie - sądu zamówień publicznych, zwanego dalej "sądem zamówień publicznych".
3. Skargę wnosi się za pośrednictwem Prezesa Izby, w terminie 14 dni od dnia doręczenia orzeczenia Izby lub postanowienia Prezesa Izby, o którym mowa w art. 519 ust. 1 ustawy p.z.p., przesyłając jednocześnie jej odpis przeciwnikowi skargi. Złożenie skargi w placówce pocztowej operatora wyznaczonego w rozumieniu ustawy z dnia 23 listopada 2012 r. - Prawo pocztowe jest równoznaczne z jej wniesieniem.
4. Prezes Izby przekazuje skargę wraz z aktami postępowania odwoławczego do sądu zamówień publicznych w terminie 7 dni od dnia jej otrzymania.
5. **WYKAZ ZAŁĄCZNIKÓW DO SWZ**

Załącznik nr 1 – Opis Przedmiotu Zamówienia

Załącznik nr 2 – Formularz ofertowy

Załącznik 2a – Formularz rzeczowy

Załącznik nr 3 – oświadczenie dotyczące przesłanek wykluczenia z postępowania i spełniania warunków udziału w postępowaniu

Załącznik nr 4 - Wzór umowy.

Załącznik nr 5- Oświadczenie dotyczące przynależności do grupy kapitałowej.

Załącznik nr 6 - wykaz dostaw

Załącznik nr 7 – Zobowiązanie podmiotu udostępniającego zasoby

9/ZP/RZPWE/2023 ZAŁĄCZNIK NR 1 DO SWZ – OPIS PRZEDMIOTU ZAMÓWIENIA

**OPIS PRZEDMIOTU ZAMÓWIENIA**

**1. Serwer**

Zamawiający wymaga dostarczenia **Serwerów wirtualizacyjnych (3 szt.)** spełniających następujące parametry minimalne:

|  |  |  |
| --- | --- | --- |
| L.p. | Nazwa parametru | Wymagane minimalnie parametry techniczne |
| 1 | **Obudowa** | Do instalacji w szafie Rack 19”, wysokość nie więcej niż 1U, z zestawem szyn do mocowania w szafie i wysuwania do celów serwisowych. |
| 2 | **Procesor** | Architektura x86, maksymalny TDP dla procesora – 120W. Minimalna ilość rdzeni dla procesora – 12, zegar min 2.1GHz. Wsparcie dla procesorów do 40 rdzeni o mocy do 270W. Wynik testu SPECrate2017\_int nie może być gorszy niż 166 baseline |
| 3 | **Liczba procesorów** | 2 |
| 4 | **Płyta główna** | Płyta główna dedykowana do pracy w serwerach, wyprodukowana przez producenta serwera z możliwością zainstalowania do dwóch procesorów wykonujących 64-bitowe instrukcje AMD64 lub EM64T |
| 5 | **Pamięć operacyjna** | Zainstalowane minimum 384GB pamięci RAM o częstotliwości 3200MHz w kościach 32GB. Minimum 32 sloty na pamięć. Możliwość rozbudowy do 1024GB RAM bez zmiany kości, w konfiguracji dwuprocesorowej. Możliwość instalacji pamięci nieulotnych Intel Optane PM200. |
| 6 | **Zabezpieczenie pamięci** | memory mirroring, ECC, SDDC, ADDDC |
| 7 | **Procesor Graficzny** | Zintegrowana karta graficzna z minimum 16MB pamięci osiągająca rozdzielczość 1920x1200 przy 60 Hz.  1 port VGA z tyłu serwera, możliwość instalacji opcjonalnej 1 port VGA na przednim panelu serwera. |
| 8 | **Rozbudowa dysków** | Serwer musi mieć możliwość instalacji do 8 dysków 2.5”. Możliwość instalacji dysków bez wyłączania serwera, dyski typu Hot Swap. Możliwość jednoczesnej instalacji dysków twardych typu SAS, SATA, SSD. W obecnym postępowaniu nie jest wymagana powyższa funkcjonalność  Zainstalowane minimum:  dwa nośniki flash o pojemności min 32GB standardu M2, skonfigurowane w RAID 1, niezajmujących zatok dyskowych serwera, |
| 9 | **Kontrolery RAID** | Możliwość instalacji kontrolerów 12 Gb SAS/SATA z obsługą RAID 0, 1, 10, 5, 50, 6, 60 z pamięcią cache minimum 2 GB flash-backed cache. W obecnym postępowaniu nie jest wymagana powyższa funkcjonalność |
| 10 | **Zasilacz** | Minimum dwa redundantne zasilacze o mocy minimum 750W z certyfikatem minimum Platinium. |
| 11 | **Interfejsy sieciowe** | Jeden port RJ-45 o przepustowości 1GbE dedykowany dla karty zarządzającej.  Jedna karta czteroportowa 10Gb RJ45. Nie zajmująca slotów PCI. Jedna karta dwuportowa 10Gb/25Gb SFP28 z zainstalowanymi modułami 10G SFP+ |
| 12 | **Dodatkowe sloty I/O** | Obudowa z obsługą do 3 slotów PCIe x16 Gen4. Zainstalowane dwa sloty PCI x16 Gen4. Dodatkowy port na kartę OCP nie zajmujący slotów PCI. |
| 13 | **Dodatkowe porty** | 5x USB 3.1, z tego minimum 1 port na przednim panelu, 3 porty minimum na tylnym panelu, oraz 1 port wewnątrz serwera. 1x USB 2,0 na przednim panelu, umożliwiający również przeprowadzenie diagnostyki serwera. |
| 14 | **Chłodzenie** | Redundatne wentylatory N+1 |
| 15 | **Zarządzanie** | Zintegrowany z płytą główną serwera, niezależny od systemu operacyjnego, sprzętowy kontroler zdalnego zarządzania Monitoring statusu i zdrowia systemu Logowanie zdarzeń Umożliwiający Update systemowego firmware Umożliwiający zdalną konfigurację serwera Monitoring i możliwość ograniczenia poboru prądu  Zdalne włączanie/wyłączanie/restart  Przekierowanie kosnoli szeregowej przez IPMI  Zrzut ekranu w momencie zawieszenia system  Zdalny dostęp do serwera  Możliwość zdalnej instalacji systemu operacyjnego  Alerty Syslog  Przekierowanie konsoli szeregowej przez SSH  Wyświetlanie danych aktualnych I historycznych dla użycia energii I temperatury serwera  Możliwość mapowania obrazów ISO z lokalnego dysku operatora  Możliwość mapowania obrazów ISO przez HTTPS, SFTP, CIFS oraz NFS  Możliwość jednoczesnej pracy do 6 użytkowników przez wirtualną konsol  Wspierane protokoły/interfejsy: IPMI v2.0, SNMP v3, CIM, DCMI v1.5, REST API |
| 16 | **Funkcje zabezpieczeń** | Hasło włączania, hasło administratora, moduł TPM (wspierający TPM 2.0). Możliwość użycia funcji Secure Boot. Opcjonalnie przednia obudowa zamykana na klucz. Opcjonalny czujnik otwarcia obudowy. |
| 17 | **Urządzenia hot swap** | Dyski twarde, zasilacze, wentylatory. |
| 18 | **Diagnostyka** | Możliwość przewidywania awarii dla procesorów, regulatorów napięcia, pamięci, dysków wewnętrznych, wentylatorów, zasilaczy, a także nietypowych temperatur serwera i komponentów wewnętrznych. |
| 19 | **Systemy operacyjne** | Wsparcie dla systemów VMware ESXi, SUSE Linux, Redhat Linux, Windows 2019, 2022 |
| 20 | **Wymagania środowiskowe** | Serwer musi umożliwiać pracę w zakresie temperatur 10-45 st C. Klasa Ashrae4. |
| 21 | **Gwarancja** | 36 miesięcy gwarancji producenta.  Możliwość rozszerzenia serwisu o serwis z lepszym SLA (np. 8 lub 12h) – również jako serwis producenta. |
| 22 | **Oprogramowanie do zarządzania serwerem** | Serwer musi mieć możliwość wyposażenia w oprogramowanie do zarządzania, wyprodukowane przez producenta serwera. |

**2. Macierz dyskowa**

Zamawiający wymaga dostarczenia **Macierzy dyskowej (1 szt.)** spełniającej następujące parametry minimalne:

|  |  |  |
| --- | --- | --- |
| L.p. | Nazwa parametru | Wymagane minimalnie parametry techniczne |
| 1 | **Obudowa** | Macierz musi być dostarczona ze wszystkimi komponentami do instalacji w szafie rack 19''. |
| 2 | **Pojemność:** | Macierz musi zostać dostarczona w konfiguracji zawierającej minimum: 7 dysków SSD o pojemności minimum 3.84TB każdy.  Minimalne pojemności dysków, które macierz musi wspierać dyski:  -SSD:800GB; 1,6TB; 3,84TB; 7,68TB; 15.3TB - SAS: 1,2TB 10k rpm; 1,8T 10k rpm. Macierz musi mieć możliwość rozbudowy do minimum 190 dysków hot-swap. |
| 3 | **Kontroler** | Dwa kontrolery macierzy wyposażone w przynajmniej 8GB cache każdy. W przypadku awarii zasilania dane nie zapisane na dyski, przechowywane w pamięci muszą być zabezpieczone za pomocą podtrzymania bateryjnego przez 72 godziny lub jako zrzut na pamięć flash. Zawartość cache musi być mirrorowana (kopia lustrzana) między kontrolerami. |
| 4 | **Interfejsy** | Oferowana macierz musi posiadać minimum:  - 8 portów 10/25Gb iSCSI obsadzonych wkładkami 10Gb SFP+,  - 4 porty SAS 12 Gb/s do komunikacji z półkami rozszerzeń  - 2 porty RJ-45 10/100/1000 Mb Ethernet typu out-of-band management.  Macierz musi pozwalać na wymianę portów 10/25Gb iSCSI na porty min 16/32GB FC bez potrzeby wymiany kontrolera macierzy. |
| 5 | **RAID** | Kontrolery macierzy muszą umożliwiać konfigurację dysków w RAID: 0, 1, 5, 6, 10. Dodatkowo macierz musi posiadać mechanizm tworzenia wirtualnej przestrzeni na minimum 120 dyskach macierzy wraz z wyliczaniem parzystości oraz podwójnej parzystości w celu zabezpieczenia danych. Mechanizm ten musi być przygotowany do optymalizacji procesów odtwarzania dysków pojemnościowych. |
| 6 | **Obsługiwane protokoły** | Macierz musi obsługiwać protokół iSCSI. |
| 7 | **Inne wymagania** | Macierz musi posiadać wsparcie dla systemów:  Microsoft Windows Server; Red Hat Enterprise Linux (RHEL); SUSE Linux Enterprise Server (SLES); VMware vSphere  Macierz musi posiadać funkcjonalność wykonywania minimum 128 kopii migawkowych typu copy-on-write, z możliwością rozbudowy do 512.  Macierz musi posiadać funkcjonalność klonowania danych i replikacji asynchronicznej. Ta funkcjonalność nie jest objęta niniejszym postępowaniem.  Macierz musi umożliwiać dynamiczną zmianę rozmiaru wolumenów logicznych bez przerywania pracy macierzy i bez przerywania dostępu do danych znajdujących się na danym wolumenie.  Macierz musi posiadać wsparcie dla funkcjonalności Thin provisioning.  Macierz musi posiadać funkcjonalność partycjonowania macierzy na odseparowane od siebie logicznie systemy, na których rezydują osobne dyski logiczne dla heterogenicznych systemów. Licencja na macierzy musi pozwalać na wykonanie do 512 partycji.  Macierz musi pochodzić od tego samego producenta co serwery rack objęte niniejszym zapytaniem.  Macierz musi posiadać funkcjonalność thin provisioning.  Macierz musi pozwalać na dynamiczną migrację pomiędzy poziomami RAID.  Macierz musi posiadać możliwość integracji z Active Directory w zakresie definicji i mapowania grup i użytkowników pod kątem autentykacji.  Macierz musi posiadać oprogramowanie pozwalające na integrację z VMware vCenter.  Macierz musi zapewniać możliwość szyfrowania danych przy użyciu dysków typu FIPS SSD.  Wszystkie licencje (z wyłączeniem replikacji synchronicznej) na funkcjonalności muszą być dostarczone na maksymalną pojemność macierzy. |
| 8 | **Gwarancja i serwis** | 3 lat serwisu producenta z czasem reakcji w następny dzień roboczy.  Dostarczone rozwiązanie musi posiadać również 3 lata subskrypcji dla dostarczonego wraz z macierzą oprogramowania, dostęp do portalu serwisowego producenta, dostęp do wiedzy i informacji technicznych dotyczących oferowanego urządzenia. |

**3. Licencja oprogramowania do wirtualizacji serwerów wraz z licencją**

Zamawiający wymaga dostarczenia Oprogramowania do wirtualizacji serwerów, konsoli zarządzania zaoferowanym oprogramowaniem wraz z licencją (1 szt.) spełniających następujące parametry minimalne.

**Oprogramowanie do wirtualizacji serwerów:**

* 1. Zaoferowane oprogramowanie do wirtualizacji musi być instalowane bezpośrednio na sprzęcie fizycznym i nie może być ono częścią innego systemu operacyjnego.
  2. W zaoferowanym oprogramowaniu warstwa wirtualizacji nie może dla własnych celów alokować więcej niż 200MB pamięci operacyjnej RAM serwera fizycznego.
  3. Zaoferowane oprogramowanie do wirtualizacji zainstalowane na serwerze fizycznym musi potrafić obsłużyć i wykorzystać procesory fizyczne tego serwera wyposażone w 768 logicznych wątków, 24TB pamięci fizycznej RAM tego serwera oraz 16 procesorów fizycznych tego serwera.
  4. Zaoferowane oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z ilością od 1 do 768 procesorów wirtualnych.
  5. Zaoferowane oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością przydzielenia do 24 TB pamięci operacyjnej RAM.
  6. Zaoferowane oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością przydzielenia od 1 do 10 wirtualnych kart sieciowych dla każdej z nich. Dodatkowo, oprogramowanie musi posiadać możliwość utworzenia maszyny wirtualnej bez przydzielonej wirtualnej karty sieciowej.
  7. Zaoferowane oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 32 porty szeregowe, 3 porty równoległe i 20 urządzeń USB.
  8. Zaoferowane oprogramowanie musi wspierać następujące systemy operacyjne: Windows XP, Windows Vista, Windows 2000, Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows Server 2016, Windows Server 2019, Windows 7, Windows 8, SLES 12, SLES 11, SLES 10, SLES 9,RHEL 8, REHL 7, RHEL 6, RHEL 5, RHEL 4, RHEL 3, RHEL Atomic 7, Solaris 11, Solaris 10, Debian, CentOS, FreeBSD, Asianux, Ubuntu, SCO OpenServer, SCO Unixware, Mac OS X, Photon OS, eCommStation 1/2/2.1, Oracle Linux , CoreOS, NeoKylin, Amazon Linux 2.
  9. W celu osiągnięcia maksymalnego współczynnika konsolidacji, zaoferowane oprogramowanie musi umożliwiać przydzielenie łącznie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera, na którym maszyny te są posadowione.
  10. Rozwiązanie musi umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie dostępne na zasobach dyskowych.
  11. Zaoferowane oprogramowanie musi zapewniać sprzętowe wsparcie dla wirtualizacji zagnieżdżonej, w szczególności w zakresie możliwości zastosowania trybu XP mode w Microsoft Windows 7 a także instalacji wszystkich funkcjonalności w tym Microsoft Hyper-V pakietu Microsoft Windows Server 2012 na maszynie wirtualnej.
  12. Zaoferowane oprogramowanie musi umożliwiać integrację z rozwiązaniami antywirusowymi firm trzecich w zakresie skanowania maszyn wirtualnych z poziomu warstwy wirtualizacji bez ingerencji w systemy operacyjne maszyn wirtualnych (bezagentowość).

1. Zaoferowane oprogramowanie musi zapewniać zdalny i lokalny dostęp administracyjny do wszystkich serwerów fizycznych poprzez protokół SSH, z możliwością nadawania uprawnień do takiego dostępu nazwanym użytkownikom bez konieczności wykorzystania konta „root”.
2. Zaoferowane oprogramowanie do wirtualizacji musi zapewnić możliwość powielania maszyn wirtualnych wraz z ich pełną konfiguracją i danymi.
3. Zaoferowane oprogramowanie do wirtualizacji musi zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy z możliwością konieczności zachowania stanu pamięci pracującej maszyny wirtualnej.
4. Konsola zarządzająca zaoferowanego oprogramowania musi posiadać możliwość przydzielania i konfiguracji uprawnień z możliwością integracji z usługami katalogowymi, minimalnie z: Microsoft Active Directory i Open LDAP oraz umożliwiać federacyjne zarządzanie tożsamością w oparciu o Microsoft Active Directory Federation Services (ADFS).
5. Zaoferowane oprogramowanie musi zapewniać możliwość dodawania zasobów w czasie pracy maszyny wirtualnej, w szczególności w zakresie ilości procesorów, pamięci operacyjnej i przestrzeni dyskowej.
6. Zaoferowane oprogramowanie musi posiadać funkcjonalność tworzenia wirtualnego przełącznika (virtual switch) umożliwiającego tworzenie sieci wirtualnej w obszarze hosta (hypervisora wirtualizacyjnego) i pozwalającego połączyć tym przełącznikiem maszyny wirtualne w obszarze jednego hosta, a także na zewnątrz sieci fizycznej. Pojedynczy przełącznik wirtualny powinien mieć możliwość konfiguracji minimum 4000 portów.
7. Pojedynczy wirtualny przełącznik w zaoferowanym oprogramowaniu, w celu zapewnienia bezpieczeństwa połączenia ethernetowego w razie awarii fizycznej karty sieciowej, musi posiadać możliwość przyłączania do niego minimum dwóch fizycznych kart sieciowych.
8. Wirtualne przełączniki w zaoferowane oprogramowaniu muszą posiadać funkcjonalność obsługi wirtualnych sieci lokalnych (VLAN).
9. Zaoferowane oprogramowanie musi zapewniać możliwość konfigurowania polityk separacji sieci w warstwie trzeciej, tak aby zapewnić oddzielne grupy wzajemnej komunikacji pomiędzy maszynami wirtualnymi.
10. Zaoferowane oprogramowanie musi umożliwiać wykorzystanie technologii przepustowości sieci komputerowych do 200GbE, w tym agregację połączeń fizycznych do minimalizacji czasu przenoszenia maszyny wirtualnej pomiędzy serwerami fizycznymi.
11. Zaoferowane oprogramowanie do wirtualizacji musi obsługiwać przełączenie ścieżek LAN (bez utraty komunikacji) w przypadku awarii jednej ze ścieżek.
12. Zaoferowane oprogramowanie musi zapewnić możliwość zdefiniowania alertów informujących o przekroczeniu wartości progowych.
13. Zaoferowane oprogramowanie, w przypadku działania pod zarządcą klastra VMware vCenter, musi zapewniać możliwość replikacji maszyn wirtualnych z dowolnej pamięci masowej w tym z dysków wewnętrznych serwerów fizycznych na dowolną pamięć masową w tym samym lub oddalonym ośrodku przetwarzania. Replikacja musi gwarantować współczynnik RPO (ang Recovery Point Objective) na poziomie minimum 5 minut.
14. Zaoferowane oprogramowanie do wirtualizacji musi obsługiwać przełączenie ścieżek SAN (bez utraty komunikacji) w przypadku awarii jednej ze ścieżek.
15. Zaoferowane oprogramowanie, w przypadku działania pod zarządcą klastra VMware vCenter, musi mieć możliwość przenoszenia maszyn wirtualnych pomiędzy serwerami fizycznymi bez przerywania pracy usług na przenoszonych maszynach wirtualnych. Wymaga się wsparcia natywnego szyfrowania ruchu sieciowego dla maszyn wirtualnych podczas ich przenoszenia między serwerami fizycznymi.
16. Zaoferowane oprogramowanie, w przypadku działania pod zarządcą klastra VMware vCenter, oraz w środowisku z więcej niż pojedynczym wirtualizatorem, musi umożliwiać automatyczne, ponowne uruchomienie maszyn wirtualnych w przypadku awarii jednego z wirtualizatorów na kolejnym, działającym w tym samym klastrze wirtualizatorze (funkcjonalność HA) (ang. high availability).
17. Zaoferowane oprogramowanie, w przypadku działania pod zarządcą klastra VMware vCenter w środowisku z minimalnie dwoma wirtualizatorami oraz w przypadku potrzeby wgrania aktualizacji do warstwy wirtualizacji, musi posiadać możliwość w przypadku wywołania startu aktualizacji, automatycznego przeniesienia bezprzerwowego działających maszyn wirtualnych do innego wirtualizatora nie objętego aktualizacją, przed rozpoczęciem samej aktualizacji.
18. Zaoferowane oprogramowanie musi posiadać co najmniej 2 niezależne mechanizmy wzajemnej komunikacji między serwerami z zainstalowanym wirtualizatorem oraz z serwerem zarządzającym, gwarantujące właściwe działanie mechanizmów wysokiej dostępności na wypadek izolacji sieciowej serwerów fizycznych lub partycjonowania sieci.
19. Zaoferowane oprogramowanie, w przypadku działania pod zarządcą klastra VMware vCenter, w środowisku z minimum dwoma wirtualizatorami, musi zapewniać pracę bez przestojów dla wybranych maszyn wirtualnych (o maksymalnie dwóch procesorach wirtualnych), niezależnie od systemu operacyjnego oraz aplikacji, podczas awarii wirtualizatora, bez utraty danych i dostępności danych na maszynach wirtualnych objętych ochroną.
20. Zaoferowane oprogramowanie do wirtualizacji musi zapewniać możliwość stworzenia dysku maszyny wirtualnej o wielkości 62 TB.
21. Zaoferowane oprogramowanie musi posiadać wbudowany interfejs programistyczny (API) zapewniający pełną integrację zewnętrznych rozwiązań wykonywania kopii zapasowych z istniejącymi mechanizmami warstwy wirtualizacyjnej.
22. Producent zaoferowanego oprogramowania do wirtualizacji musi wspierać rozwiązania do automatyzacji procesów oraz wirtualizacji sieci (SDN, ang. software defined network).
23. Zaoferowane oprogramowanie musi wspierać mechanizmy zaawansowanego uwierzytelniania do systemu operacyjnego wirtualnej maszyny za pomocą technologii Smart Card Reader.
24. Zaoferowane oprogramowanie musi wspierać TPM 2.0. Minimalne wymaganie Zamawiającego dla TPM oznacza, że TPM zapewnia mechanizm gwarantujący, że serwer fizyczny, na którym zainstalowane jest zaoferowane oprogramowanie, uruchomił się z włączoną opcją Secure Boot. Po potwierdzeniu, że SecureBoot jest włączone, system gwarantuje, poprzez weryfikację podpisu cyfrowego, że hypervisor uruchomił się w niezmienionej formie.
25. Wirtualizator w zaoferowanym oprogramowaniu musi mieć możliwość włączenia funkcji “Microsoft virtualization-based security”, tzw. Microsoft VBS dla systemów operacyjnych maszyn wirtualnych opartych o system operacyjny Microsoft Windows 10 oraz Microsoft Windows Server 2016.
26. Zaoferowane oprogramowanie musi posiadać certyfikację FIPS-140-2 min. dla modułu jądra wirtualizatora odpowiedzialnego za szyfrowanie danych.
27. Zaoferowane oprogramowanie musi posiadać funkcjonalność wirtualnego TPM 2.0 dla maszyn wirtualnych z zainstalowanym Microsoft Windows 10 oraz Microsoft Windows 2016. Zamawiający wymaga aby z punktu widzenia maszyny wirtualnej z systemem operacyjnym Microsoft Windows 10 lub Microsoft Windows 2016 wirtualny TPM widziany był jako standardowy TPM, gdzie można przechowywać bezpiecznie wrażliwe dane np. certyfikaty. Zawartość wirtualnego TPM musi być przechowywana w pliku przynależnym do maszyny wirtualnej oraz musi być szyfrowana.
28. Zaoferowane oprogramowanie musi posiadać funkcjonalność szybkiego uruchamiania wirtualizatora po przeprowadzonym procesie jego aktualizacji. Zamawiający wymaga, aby w procesie aktualizacji wirtualizatora, jeśli wymagany jest jego restart, funkcjonalność szybkiego uruchamiania powodowała eliminację czasochłonnej fazy inicjalizacji serwera fizycznego.
29. Zaoferowane oprogramowanie musi posiadać możliwość aktualizacji i kontroli wersji oprogramowania do wirtualizacji w ramach klastra serwerów z poziomu centralnej konsoli zarządzającej. Dodatkowo centralna konsola zarządzająca musi posiadać funkcjonalność aktualizacji firmware komponentów serwera fizycznego (dyski, kontrolery, karty sieciowe) z poziomu konsoli zarządzającej wirtualizatora. Konsola zarządzająca musi mieć możliwość automatycznej weryfikacji, czy zainstalowane komponenty serwera posiadają rekomendowaną wersję sterowników i firmware, eliminując ryzyko pracy na nieaktualnych wersjach. Taka funkcjonalność powinna być dostępna dla minimum dwóch producentów serwerów obecnych na rynku.
30. Zaoferowane oprogramowanie musi posiadać wsparcie dla natywnych dysków 4K.
31. Zaoferowane oprogramowanie musi wspierać protokół precyzyjnej synchronizacji czasu PTP (ang. Precision Time Protocol).
32. Zaoferowane oprogramowanie, w przypadku działania pod zarządcą klastra VMware vCenter, musi posiadać mechanizm, który ogranicza dostęp do indywidualnego zarządzania warstwą wirtualizacji na serwerach fizycznych w ramach klastra serwerów w celu utwardzenia/hardening (maksymalnego zwiększenia bezpieczeństwa dostępu) systemu wirtualizacji.
33. Zaoferowane oprogramowanie musi mieć funkcjonalność migracji w trybie rzeczywistym dysków działających maszyn wirtualnych z jednego podsystemu dyskowego do innego bez konieczności przerywania pracy maszyny wirtualnej, której dysk jest migrowany.
34. Licencjonowanie zaoferowanego oprogramowania lub zapewnienie udzielenia licencji na zaoferowane oprogramowanie spełniające wymagania Standardowe musi posiadać możliwość swobodnego przeniesienia praw do użytkowania na dowolny podmiot wymieniony w umowie ramowej i dowolny serwer fizyczny będący w posiadaniu Zamawiającego (bez ograniczeń licencji OEM). Licencje dostępne w modelu licencjonowania na procesor fizyczny.
35. Zaoferowane oprogramowanie musi posiadać certyfikację dla pakietu NVIDIA AI Enterprise, natywnego dla chmury zbioru zoptymalizowanych aplikacji AI i frameworków przeznaczonych dla kompleksowego rozwiązania AI.
36. Zaoferowane oprogramowanie musi umożliwiać włączenie najnowszej generacji procesorów graficznych NVIDIA do swojego środowiska wirtualnego i skorzystanie z takich funkcji jak Multi-Instance GPU (MIG), pozwalające na współdzielenie cykli GPU przez wielu użytkowników.
37. Zaoferowane oprogramowanie umożliwia uruchamianie poufnych kontenerów w serwerach opartych na procesorach EPYC ™ firmy AMD.
38. Zaoferowane oprogramowanie zapewnia podstawowe funkcje serwera zarządzania kluczami (KMS), które upraszcza włączenie szyfrowania i zaawansowanych funkcji bezpieczeństwa.
39. Zaoferowane oprogramowanie obejmuje walidację FIPS, a także zaktualizowane przewodniki audytów.

**Konsola zarządzania dostarczonym oprogramowaniem do wirtualizacji serwerów**

**Zamawiający wymaga dostarczenia oprogramowania spełniającego poniższe funkcjonalności:**

* 1. Zaoferowane oprogramowanie musi posiadać konsolę graficzną do zarządzania maszynami wirtualnymi i do konfigurowania innych funkcjonalności. min: zasobów dyskowych oraz zasobów sieci komputerowej. Konsola graficzna powinna działać jako zainstalowana aplikacja na maszynie wirtualnej. Dodatkowo wymaga się aby maszyna z aplikacją była wstępnie skonfigurowana i dostępna jako tzw. Virtual appliance. Instalacja w/w virtual appliance nie może wiązać się z potrzebą dostawy dodatkowego oprogramowania takiego jak np. system operacyjny lub baza danych.
  2. Zaoferowane oprogramowanie musi posiadać wbudowany serwer ściany ogniowej (ang. firewall) dający możliwość konfiguracji blokady lub akceptacji ruchu pomiędzy konsolą zarządzającą a serwerami oraz serwerami wirtualnymi na nich posadowionymi, przy założeniu blokowania całego ruchu a nie poszczególnych portów.
  3. Zaoferowane oprogramowanie musi mieć możliwość konfiguracji uwierzytelniania użytkowników logujących się do niego w oparciu o minimum: domenę Microsoft Active Directory, Microsoft Active Directory over LDAP oraz Open LDAP.
  4. Zaoferowane oprogramowanie musi posiadać konsole graficzną, która musi być dostępna poprzez dedykowanego klienta (za pomocą przeglądarek, minimum Microsoft IE i Mozilla Firefox) lub poprzez konsolę graficzną, która zbudowana jest z wykorzystaniem języka HTML5.
  5. Zaoferowane oprogramowanie musi posiadać funkcjonalność zcentralizowanego zarządzania hostami opartymi na rozwiązaniu VMware vSphere.
  6. Zaoferowane oprogramowanie musi posiadać natywne mechanizmy do wykonywania kopii zapasowej swojej konfiguracji. Dodatkowo wymaga się możliwości ustawienia harmonogramu wykonywania kopii zapasowej. Wymaga się aby kopie zapasowe wspierały protokoły: FTPS, HTTPS, SCP, FTP oraz HTTP.
  7. Zaoferowane oprogramowanie, poprzez rozszerzenie o dodatkową licencję oferowaną przez tego samego producenta musi posiadać wbudowaną funkcjonalność zarządzania wirtualną przestrzenią dyskową SDS (ang. Software Defined Storage).
  8. Zaoferowane oprogramowanie musi posiadać interfejs graficzny do prowadzenia prac administracyjnych w zakresie swojej konfiguracji oraz monitoringu (możliwość monitorowania obciążenia min. vCPU, vRAM, vHDD, sieci, bazy danych). Interfejs graficzny powinien być wykonany w standardzie HTML5.
  9. Licencjonowanie zaoferowanego oprogramowania lub zapewnienie udzielenia licencji na zaoferowane oprogramowanie spełniające wymagania Minimalne musi posiadać możliwość swobodnego przeniesienia praw do użytkowania na dowolny podmiot wymieniony w umowie ramowej i dowolny serwer fizyczny będący w posiadaniu Zamawiającego (bez ograniczeń licencji OEM). Licencje dostępne w modelu licencjonowania na procesor fizyczny (nielimitowana ilość rdzeni procesora).
  10. Zaoferowane oprogramowanie zawiera możliwość automatyzacji instalacji wielu konsoli zarządzania poprzez użycie schematów konfiguracji.
  11. Zaoferowane oprogramowanie umożliwia aktualizowanie wielu wirtualizatorów równocześnie.
  12. Rozwiązanie musi pozwalać na wykorzystanie łącz o szybkości 25 GbE, 40 GbE i 100 GbE do bezawaryjnego przenoszenia maszyn wirtualnych między wirtualizatorami.
  13. Rozwiązanie musi zapewniać natywne mechanizmy wysokiej dostępności HA (ang. high availability) w niezawodnej architekturze Active-Passive-Witness dla wszystkich składowych komponentów centralnej konsoli graficznej zarządzającej platformą wirtualną.
  14. Zaoferowane oprogramowanie, w przypadku zarządzania serwerami opartymi o VMware vSphere, musi prezentować poziom zbalansowania mocy obliczeniowej w klastrze opartym o w/w wirtualizatory.
  15. Dostęp przez przeglądarkę do konsoli graficznej w zaoferowanym oprogramowaniu musi być skalowalny tj. powinien umożliwiać rozdzielenie komponentów na wiele instancji w przypadku zapotrzebowania na dużą liczbę jednoczesnych dostępów administracyjnych do środowiska.
  16. Licencjonowanie zaoferowanego oprogramowania lub zapewnienie udzielenia licencji na zaoferowane oprogramowanie spełniające wymagania Standardowe musi posiadać możliwość swobodnego przeniesienia praw do użytkowania na dowolny podmiot wymieniony w umowie ramowej i dowolny serwer fizyczny będący w posiadaniu Zamawiającego (bez ograniczeń licencji OEM). Licencje dostępne w modelu licencjonowania na procesor fizyczny (nielimitowana ilość rdzeni procesora).

**Licencje na oprogramowanie do wirtualizacji**

Zamawiający wymaga dostarczenia licencji na dostarczone oprogramowanie, które umożliwi uruchomienie wirtualizatora wykorzystującego 3 serwery fizyczne, z których każdy wyposażony jest w 2 procesory oraz wykorzystywanie konsoli zarządzania oprogramowaniem do wirtualizacji o wyżej opisanych cechach.

**4. Zapasowa macierz dyskowa**

Zamawiający wymaga dostarczenia **Zapasowej macierzy dyskowej (1 szt.)** spełniającej następujące parametry minimalne:

|  |  |  |
| --- | --- | --- |
| L.p. | Nazwa parametru | Wymagane minimalnie parametry techniczne |
| 1 | **Obudowa** | Rack 2U (maks.) |
| 2 | **Procesor** | Czterordzeniowy procesor o taktowaniu 2,2 GHz osiągający w teście PassMark na luty 2023 co najmniej 4 580 punktów |
| 3 | **Sprzętowy mechanizm szyfrowania** | Tak (AES-NI) |
| 4 | **Pamięć RAM** | min. 2 GB pamięci ECC SODIMM z możliwością rozszerzenia do  min. 32 GB |
| 5 | **Przestrzeń dyskowa** | Wymaga się aby serwer NAS był wyposażony w maks. 8 kieszeni na dyski twarde typu hot-swap przy czym macierz musi się składać z jednostki głównej oraz półki rozszerzającej podłączanej za pomocą portu eSATA. |
| 6 | **Dyski twarde** | Urządzenie musi być wyposażone w 8 dysków twardych SATA SSD 2.5” o pojemności min. 3 TB każdy. Średni czas do awarii (MTBF) musi wynosić min. 1.5 mln godzin a parametr TBW min. 2 194 TB danych.  Wymogiem jest dostarczenie dysków klasy korporacyjnej, które zapewnią odpowiednią wydajność oraz niezawodność a całość sprzętu pochodziła od tego samego producenta co macierz główna zapewniając pełną kompatybilność na poziomie oprogramowania układowego. |
| 7 | **Porty zewnętrzne** | Minimum:  • 2 porty USB 3.2.1  • 1 port eSATA (jako gniazdo rozszerzenia) |
| 8 | **Porty sieciowe** | Minimum:  • 4 porty 1GbE RJ45 (z obsługą funkcji Link Aggregation / przełączania awaryjnego)  • 1 port 10GbE RJ45 zrealizowany za pomocą dodatkowej, dedykowanej karty sieciowej tego samego producenta co urządzenie główne  • 2 porty 10GbE SFP+ zrealizowane za pomocą dodatkowej, dedykowanej karty sieciowej tego samego producenta co urządzenie główne |
| 9 | **Funkcja Wake on LAN/WAN** | Tak |
| 10 | **Gniazdo rozszerzeń PCIe 2.0** | Min. 1x 4-liniowe gniazdo x8 gen. 3 |
| 11 | **Wentylator obudowy** | Min. 3 wentylatory (40 × 40 × 20 mm) |
| 12 | **Obsługiwane protokoły sieciowe** | Min. SMB1 (CIFS), SMB2, SMB3, NFSv3, NFSv4, NFSv4.1, NFS Kerberized sessions, iSCSI, HTTP, HTTPs, FTP, SNMP, LDAP, CalDAV |
| 13 | **Obsługiwane systemy plików** | Min.:  • Wewnętrzny: Btrfs, ext4  • Zewnętrzny: Btrfs, ext4, ext3, FAT, NTFS, HFS+, exFAT |
| 14 | **Zarządzanie pamięcią masową** | Maksymalny rozmiar pojedynczego wolumenu: 108 TB  • Minimalny liczba wewnętrznych wolumenów: 64  • Minimalny liczba obiektów iSCSI Target: 128  • Minimalny liczba jednostek iSCSI LUN: 256  • Obsługa klonowania/migawek jednostek iSCSI LUN |
| 15 | **Obsługiwane typy macierzy RAID** | Min. SHR, Basic, JBOD, RAID 0, RAID 1, RAID 5, RAID 6, RAID 10 |
| 16 | **Funkcja udostępniania plików** | • Minimalna liczba kont użytkowników: 2 048  • Minimalna liczba grup użytkowników: 256  • Minimalna liczba folderów współdzielonych: 512  • Minimalna liczba jednoczesnych połączeń CIFS/AFP/NFS/FTP: 500\*  \*Liczba jednoczesnych połączeń może zostać zwiększona do 2 000 po zainstalowaniu co najmniej 8 GB pamięci RAM. |
| 17 | **Uprawnienia** | Uprawnienia listy kontroli dostępu systemu Windows® (ACL) i aplikacji |
| 18 | **Wirtualizacja** | Obsługa VMware vSphere with VAAI, Microsoft Hyper-V®, Citrix®, OpenStack® |
| 19 | **Usługa katalogowa** | Integracja z usługami Windows® AD, logowanie użytkowników domeny przez protokoły SMB/NFS/AFP/FTP lub aplikację File Station, integracja z LDAP |
| 20 | **Bezpieczeństwo** | Zapora, szyfrowany folder współdzielony, szyfrowanie SMB, FTP przez SSL/TLS, SFTP, rsync przez SSH, automatyczne blokowanie logowania, obsługa Let's Encrypt, HTTPS (dostosowywane mechanizmy szyfrowania) |
| 21 | **Obsługiwane przeglądarki** | Google Chrome®, Firefox®, Microsoft Edge®, Safari® 13 i nowsze oraz Safari (iOS 13.0 i nowsze) na urządzeniach iPad, Chrome (Android™ 11.0 i nowsze) na tabletach |
| 22 | **Oprogramowanie** | Urządzenie musi umożliwiać utworzenie przestrzeni dyskowej w oparciu o nowoczesny system plików, który będzie zapewniał obsługę migawek, generowania sum kontrolnych CRC a także lustrzanych kopii metadanych aby zapewnić całkowitą integralność danych biznesowych.  Dodatkowo wspomniany system musi wspierać ustawienie limitu dla folderów współdzielonych oraz szybkie klonowanie całych folderów współdzielonych  • Oprogramowanie zarządzające serwerem NAS musi zapewnić darmowe, kompleksowe rozwiązanie do tworzenia kopii zapasowych przeznaczone dla heterogenicznych środowisk IT, umożliwiające zdalne zarządzanie i monitorowanie ochrony komputerów, serwerów i maszyn wirtualnych na jednym, centralnym, przyjaznym dla administratora interfejsie. Ponadto gromadzone dane na urządzeniu mają mieć możliwość replikacji jako lokalne kopie zapasowe, sieciowe kopie zapasowe i kopie zapasowe danych w chmurach publicznych przy użyciu darmowego narzędzia instalowanego z Centrum Pakietów  • Wymaga się zapewnienia darmowej aplikacji do realizacji chmury prywatnej bez opłat cyklicznych, która będzie posiadała wygodną konsolę administratora zarządzaną z GUI a także agenty na urządzenia PC/MAC oraz aplikację mobilną na Android/iOS. Usługa powinna umożliwiać udostępnianie zasobów serwera NAS, synchronizację i tworzenie kopii zapasowych podłączonych urządzeń a także wspierać algorytm Intelliversioning. Ponadto omawiana usługa powinna umożliwiać pracę z dokumentami biurowymi (edytor tekstowy, arkusz kalkulacyjny, pokaz slajdów) i wpierać wersjonowanie oraz edycję tworzonych plików office w czasie rzeczywistym.  • Urządzenie musi umożliwiać pracę w trybie klastra wysokiej dostępności (HA) aby zapewnić nieprzerwany, natychmiastowy dostęp do zasobów bez widocznych zmian w użytkowaniu (konfiguracja jako jeden spójny system). Wszystkie dane z powodzeniem zapisane na serwerze aktywnym będą na bieżąco kopiowane do serwera pasywnego zapewniając replikację w czasie rzeczywistym i dostęp do danych oraz usług w przypadku uszkodzenia jednostki aktywnej dając gwarancję ciągłości pracy.  Utworzenie klastra HA ma się opierać o 2 identyczne urządzenia |
| 23 | **Konserwacja** | Konserwację urządzenia należy przeprowadzać przy użyciu dodatkowych, wygodnych w użyciu przesuwnych szyn rack |
| 24 | **Gwarancja** | 3 lata na urządzenia główne  • 3 lata na dodatkową półkę rozszerzającą  • 5 lat na dyski twarde SSD  • 5 lat na dodatkowe karty sieciowe  • 1 rok na dodatkowe akcesoria montażowe w postaci przesuwnych szyn rack |

**5. Serwer NAS przeznaczony do archiwizacji danych**

Zamawiający wymaga dostarczenia **Serwera NAS przeznaczonego do archiwizacji danych (1 szt.)** spełniającego następujące parametry minimalne:

|  |  |  |
| --- | --- | --- |
| L.p. | Nazwa parametru | Wymagane minimalnie parametry techniczne |
| 1 | **Obudowa** | Rack 2U (maks.) |
| 2 | **Procesor** | Czterordzeniowy procesor o taktowaniu 2,2 GHz osiągający w  teście PassMark na luty 2023 co najmniej 4 580 punktów |
| 3 | **Sprzętowy mechanizm szyfrowania** | Tak (AES-NI) |
| 4 | **Pamięć RAM** | min. 2 GB pamięci ECC SODIMM z możliwością rozszerzenia do  min. 32 GB |
| 5 | **Przestrzeń dyskowa** | Wymaga się aby serwer NAS był wyposażony w maks. 8 kieszeni na dyski twarde typu hot-swap przy czym macierz musi się składać z jednostki głównej oraz półki rozszerzającej podłączanej za pomocą portu eSATA. |
| 6 | **Dyski twarde** | Urządzenie musi być wyposażone w 8 dysków twardych SATA SSD 3.5” o pojemności min. 3 TB każdy. Średni czas do awarii (MTBF) musi wynosić min. 1 mln godzin. Dyski muszą być przystosowane do działania w trybie ciągłym 24/7 w macierzach dyskowych NAS. Dyski muszą posiadać funkcjonalność obniżającą pobór energii elektrycznej podczas okresów niskiej aktywności dysku. |
| 7 | **Porty zewnętrzne** | Minimum:  • 2 porty USB 3.2.1  • 1 port eSATA (jako gniazdo rozszerzenia) |
| 8 | **Porty sieciowe** | Minimum:  • 4 porty 1GbE RJ45 (z obsługą funkcji Link Aggregation / przełączania awaryjnego)  1 port 10GbE RJ45 zrealizowany za pomocą dodatkowej, dedykowanej karty sieciowej tego samego producenta co urządzenie główne |
| 9 | **Funkcja Wake on LAN/WAN** | Tak |
| 10 | **Gniazdo rozszerzeń PCIe 2.0** | Min. 1x 4-liniowe gniazdo x8 gen. 3 |
| 11 | **Wentylator obudowy** | Min. 3 wentylatory (40 × 40 × 20 mm) |
| 12 | **Obsługiwane protokoły sieciowe** | Min. SMB1 (CIFS), SMB2, SMB3, NFSv3, NFSv4, NFSv4.1, NFS Kerberized sessions, iSCSI, HTTP, HTTPs, FTP, SNMP, LDAP, CalDAV |
| 13 | **Obsługiwane systemy plików** | Min.:  • Wewnętrzny: Btrfs, ext4  • Zewnętrzny: Btrfs, ext4, ext3, FAT, NTFS, HFS+, exFAT |
| 14 | **Zarządzanie pamięcią masową** | • Maksymalny rozmiar pojedynczego wolumenu: 108 TB  • Minimalny liczba wewnętrznych wolumenów: 64  • Minimalny liczba obiektów iSCSI Target: 128  • Minimalny liczba jednostek iSCSI LUN: 256  • Obsługa klonowania/migawek jednostek iSCSI LUN |
| 15 | **Obsługiwane typy macierzy RAID** | Min. SHR, Basic, JBOD, RAID 0, RAID 1, RAID 5, RAID 6, RAID 10 |
| 16 | **Funkcja udostępniania plików** | • Minimalna liczba kont użytkowników: 2 048  • Minimalna liczba grup użytkowników: 256  • Minimalna liczba folderów współdzielonych: 512  • Minimalna liczba jednoczesnych połączeń CIFS/AFP/NFS/FTP: 500\*  \*Liczba jednoczesnych połączeń może zostać zwiększona do 2 000 po zainstalowaniu co najmniej 8 GB pamięci RAM. |
| 17 | **Uprawnienia** | Uprawnienia listy kontroli dostępu systemu Windows® (ACL) i aplikacji |
| 18 | **Wirtualizacja** | Obsługa VMware vSphere with VAAI, Microsoft Hyper-V®, Citrix®, OpenStack |
| 19 | **Usługa katalogowa** | Integracja z usługami Windows® AD, logowanie użytkowników domeny przez protokoły SMB/NFS/AFP/FTP lub aplikację File Station, integracja z LDAP |
| 20 | **Bezpieczeństwo** | Zapora, szyfrowany folder współdzielony, szyfrowanie SMB, FTP przez SSL/TLS, SFTP, rsync przez SSH, automatyczne blokowanie logowania, obsługa Let's Encrypt, HTTPS (dostosowywane mechanizmy szyfrowania) |
| 21 | **Obsługiwane przeglądarki** | Google Chrome®, Firefox®, Microsoft Edge®, Safari® 13 i nowsze oraz Safari (iOS 13.0 i nowsze) na urządzeniach iPad, Chrome (Android™ 11.0 i nowsze) na tabletach |
| 22 | **Oprogramowanie** | Urządzenie musi umożliwiać utworzenie przestrzeni dyskowej w oparciu o nowoczesny system plików, który będzie zapewniał obsługę migawek, generowania sum kontrolnych CRC a także lustrzanych kopii metadanych aby zapewnić całkowitą integralność danych biznesowych.  Dodatkowo wspomniany system musi wspierać ustawienie limitu dla folderów współdzielonych oraz szybkie klonowanie całych folderów współdzielonych  • Oprogramowanie zarządzające serwerem NAS musi zapewnić darmowe, kompleksowe rozwiązanie do tworzenia kopii zapasowych przeznaczone dla heterogenicznych środowisk IT, umożliwiające zdalne  zarządzanie i monitorowanie ochrony komputerów, serwerów i maszyn wirtualnych na jednym, centralnym, przyjaznym dla administratora interfejsie. Ponadto gromadzone dane na urządzeniu mają mieć możliwość replikacji jako lokalne kopie zapasowe, sieciowe kopie zapasowe i kopie zapasowe danych w chmurach publicznych przy użyciu darmowego narzędzia instalowanego z Centrum Pakietów  • Wymaga się zapewnienia darmowej aplikacji do realizacji chmury prywatnej bez opłat cyklicznych, która będzie posiadała wygodną konsolę administratora zarządzaną z GUI a także agenty na urządzenia PC/MAC oraz aplikację  mobilną na Android/iOS. Usługa powinna umożliwiać udostępnianie zasobów serwera NAS, synchronizację i tworzenie kopii zapasowych podłączonych urządzeń a także wspierać algorytm Intelliversioning. Ponadto omawiana  usługa powinna umożliwiać pracę z dokumentami biurowymi (edytor tekstowy, arkusz kalkulacyjny, pokaz slajdów) i wpierać wersjonowanie oraz edycję tworzonych plików office w czasie rzeczywistym.  Urządzenie musi umożliwiać pracę w trybie klastra wysokiej dostępności (HA) aby zapewnić nieprzerwany, natychmiastowy dostęp do zasobów bez widocznych zmian w użytkowaniu (konfiguracja jako jeden spójny system).  Wszystkie dane z powodzeniem zapisane na serwerze aktywnym będą na bieżąco kopiowane do serwera pasywnego zapewniając replikację w czasie rzeczywistym i dostęp do danych oraz usług w przypadku uszkodzenia  jednostki aktywnej dając gwarancję ciągłości pracy.  Utworzenie klastra HA ma się opierać o 2 identyczne urządzenia. |
| 23 | **Konserwacja** | Konserwację urządzenia należy przeprowadzać przy użyciu  dodatkowych, wygodnych w użyciu przesuwnych szyn rack |
| 24 | **Gwarancja** | 3 lata na urządzenia główne  • 3 lata na dodatkową półkę rozszerzającą  • 1 rok na dodatkowe akcesoria montażowe w postaci  przesuwnych szyn rack |

**6. Zasilacz awaryjny UPS**

Zamawiający wymaga dostarczenia **Zasilacza awaryjnego UPS (1 szt.)** spełniającego następujące parametry minimalne:

|  |  |  |
| --- | --- | --- |
| L.p. | Nazwa parametru | Wymagane minimalnie parametry techniczne |
| 1 | **Charakterystyka podstawowa** | |
|  | Technologia wykonania UPS | Online podwójna konwersja |
|  | Możliwość rozbudowy o kolejne UPS (praca równoległa) | Wymagana |
|  | Moc pozorna (VA) | 10000 |
|  | Moc rzeczywista (W) | 9000 |
|  | Kształt fali na wyjściu(praca na baterii) | Pełna fala sinusoidalna |
|  | Kompatybilność z zasilaczami z aktywnym PFC | Wymagana |
|  | Ochrona przed przeciążeniem | Wymagana(minimum bezpiecznik i wewnętrzny ogranicznik prądu) |
|  | Filtr EMI/RFI | Wymagany |
|  | Układ przeciwprzepięciowy (Dżule) | Wymagany, minimum 440 |
| 2 | **Charakterystyka wejścia/wyjścia** | |
|  | Nominalne napięcie wejściowe (V) | 230 |
|  | Obsługiwany zakres napięcia wejściowego (V) | 115 ~ 270 |
|  | Częstotliwość wejściowa(Hz) | 50+/-5 ; 60+/-6 |
|  | Wykrywanie częstotliwości wejściowej | Wymagane automatyczne |
|  | Napięcie przy pracy na baterii (V) | 208 +/-1% ; 220 +/-1%; 230 +/-1%; 240 +/-1% |
|  | Częstotliwość przy pracy baterii (Hz) | 50+/-0.1% ; 60+/-0.1% |
| 3 | **Charakterystyka gniazd** | |
|  | Rodzaj złącza wejściowego | Złącze typu terminal block |
|  | Rodzaj złącza wyjściowego | Złącze typu terminal block |
| 4 | **Charakterystyka baterii** | |
|  | Typowy czas przełączenia na baterie (ms) | 0 ms |
|  | Bateria | Wymagana praca z zewnętrznymi modułami baterii |
|  | Ilość obsługiwanych modułów baterii | Do 15 |
|  | Zarządzanie | |
|  | Sygnalizacja | Wymagane alarmy dźwiękowe oraz wyświetlacz LCD |
|  | Alarmy dźwiękowe | minimum Tryb baterii , Niski poziom baterii , Przeciążenie , Przeładowanie , Przegrzanie |
|  | Konfiguracja wybranych parametrów | Przez wyświetlacz LCD, minimum ustawienia trybu pracy, baterii, ustawienia wejścia-wyjścia |
|  | Port komunikacyjny USB | Wymagany |
|  | Port wyłącznika awaryjnego EPO | Wymagany |
|  | Dołączone oprogramowanie do zarządzania | Wymagane, obsługa platform Windows, Linux, Vmware |
|  | Zarządzanie przez sieć | Wymagane dostarczenie karty zarządzającej HTTPS/SNMP, umożliwiającej m.in. kontrolę i monitoring stanu i kondycji zasilacza UPS, parametrów zasilania na wejściu i wyjściu, powiadamianie o zdarzeniach związanych z zasilaniem, możliwość zaplanowania automatycznego włączenia, wyłączenia lub restartu zasilacza UPS, log zdarzeń. |
| 5 | **Cechy fizyczne** | |
|  | Obudowa | Wymagana możliwośc instalacji w szafie RACK lub ustawienia jako Tower |
|  | Konstrukcja obudowy | Metalowa |
|  | Szyny/uchwyty rack | Wymagane |
|  | Rozmiary (szer. x wys. x gł.) (mm) | Nie większe niż 438 x 130.5 x 680 |
|  | Waga | maksiumum 20 kg |
| 6 | **Dane środowiskowe** | |
|  | Temperatura robocza (°C) | 0 ~ 40 |
|  | Względna wilgotność robocza (bez kondensacji) (%) | 0 ~ 90 |
| 7 | **Pozostałe** | |
|  | Certyfikaty | CE, RoHS |
|  | Gwarancja | minimum 2 lata |

**7. Oprogramowanie do wykonywania kopii bezpieczeństwa**

|  |  |
| --- | --- |
| Nazwa Parametru | Wymagane minimalne parametry techniczne |
| Licencje backup dla oferowanych urządzeń zgodnie z ilością CPU oferowanych urządzeń - na 35 serwerów wirtualnych | • Oprogramowanie musi być produktem przeznaczonym do obsługi środowisk DataCenter. Oferowany produkt musi znajdować się w kwadracie liderów Gartner Magic Quadrant for Data Center Backup and Recovery Solutions oraz na ogólnie dostępnej liście referencyjnej Gartner: <https://www.gartner.com/reviews/market/data-center-backupand-recovery-solutions> i spełniać minimalne wymaganie: - minimalna liczba referencji 150, - minimalna ocena z referencji 4,5,  • Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 5.5, 6.0, 6.5, 6.7 and 7.0. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej  • Oprogramowanie musi współpracować z hostami zarządzanymi przez VMware vCenter oraz pojedynczymi hostami.  • Oprogramowanie musi współpracować z hostami zarządzanymi przez System Center Virtual Machine Manager, klastrami hostów oraz pojedynczymi hostami.  • Oprogramowanie musi zapewniać tworzenie kopii zapasowych wszystkich systemów operacyjnych maszyn wirtualnych wspieranych przez vSphere  • Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux.  • Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej  • Oprogramowanie musi tworzyć “samowystarczalne” archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków  • Oprogramowanie musi pozwalać na tworzenie kopii zapasowych w trybach: Pełny, pełny syntetyczny, przyrostowy i odwrotnie przyrostowy (tzw. reverse-inremental)  • Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji  • Oprogramowanie musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć jedną wirtualną pulę pamięci na kopie zapasowe. Wymagane jest wsparcie dla co najmniej trzech pamięci masowych w takiej puli.  • Oprogramowanie musi pozwalać na rozszerzenie lokalnej przestrzeni backupowej poprzez integrację z Microsoft Azure Blob, Amazon S3 oraz z innymi kompatybilnymi z S3 macierzami obiektowymi. Proces migracji danych powinien być zautomatyzowany. Jedynie unikalne bloki mogą być przesyłane w celu oszczędności pasma oraz przestrzeni na przechowywane dane. Funkcjonalność ta nie może mieć wpływu na możliwości odtwarzania danych.  • Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu.  • Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny  wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania  • Oprogramowanie musi mieć możliwość uruchamiania dowolnych skryptów przed i po zadaniu backupowym lub przed i po wykonaniu zadania snapshota.  • Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL oraz Oracle (w tym odtwarzanie point-in-time)  • Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji  • Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji  • Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania  • Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.  • Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej  • Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta musi być dostępna na wszystkich wspieranych platformach wirtualizacyjnych • Oprogramowanie musi automatycznie wykrywać i usuwać snapshoty-sieroty (orphaned snapshots), które mogą zakłócić poprawne wykonanie backupu. Proces ten nie może wymagać interakcji administratora  • Oprogramowanie musi posiadać wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją VMware.  • Oprogramowanie musi wspierać kopiowanie backupów na taśmy wraz z pełnym śledzeniem wirtualnych maszyn  • Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son)  • Oprogramowanie musi umieć korzystać z protokołu DDBOOST w przypadku, gdy repozytorium backupów jest umiejscowione na Dell EMC DataDomain. Funkcjonalność musi wspierać łącze sieciowe lub FC.  • Oprogramowanie musi umieć korzystać z protokołu Catalyst (w tym Catalyst Copy) w przypadku, gdy repozytorium backupów jest umiejscowione na HPE StoreOnce. Funkcjonalność musi wspierać łącze sieciowe lub FC.  • Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016 lub 2019 z systemem pliku ReFS jako repozytorium backupu. Podobna funkcjonalność musi być zapewniona dla repozytoriów opartych o linuxowy system plików XFS.  • Oprogramowanie musi mieć możliwość replikacji włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere, pomiędzy hostami ESXi, włączając asynchroniczną replikacją ciągłą. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji.  • Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik  • Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding)  • Oprogramowanie musi dawać możliwość tworzenia backupów ad-hoc z konsoli jak i z klienta webowego vSphere  • Oprogramowanie musi przetwarzać wiele wirtualnych dysków jednocześnie (parallel processing)  • Oprogramowanie musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware niezależnie od rodzaju storage’u użytego do przechowywania kopii zapasowych.  • Dodatkowo dla środowiska vSphere powyższa funkcjonalność umożliwi uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna)    • Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja musi odbywać się mechanizmami wbudowanymi w hypervisor. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie musi realizować taką migrację swoimi mechanizmami  • Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSpehre  • Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków  • Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack  • Oprogramowanie musi umożliwić odtworzenie plików na maszynę operatora lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie będzie ograniczona wielkością i liczbą przywracanych plików  • Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy VIX API dla platformy VMware  • Oprogramowanie musi wspierać odtwarzanie plików z następujących systemów plików: o Linux (ext2, ext3, ext4, ReiserFS, JFS, XFS, Btrfs ) o Mac (HFS, HFS+) o Windows (NTFS, FAT, FAT32, ReFS)  • Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM oraz Windows Storage Spaces.  • Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej.  • Oprogramowanie musi wspierać granularne odtwarzanie dowolnych obiektów i dowolnych atrybutów Active Directory włączając hasło, obiekty Group Policy, partycja konfiguracji AD, rekordy DNS zintegrowane z AD, Microsoft System Objects, certyfikaty CA oraz elementy AD Sites.  • Licencje muszą być wieczyste i posiadać wykupione wsparcie na okres 1 roku |

**8. Licencje systemu operacyjnego**

Zamawiający wymaga dostarczenia następujących licencji systemu operacyjnego:

* Licencja Windows Server 2022 Datacenter Academic na 72 rdzenie procesora w paczkach po 2 licencje
* Licencja Windows Server 2022 User CAL Academic - 10 szt.
* Licencja Windows Server 2022 External Connector - 2 szt.

**9. Licencje oprogramowanie serwera bazy danych**

Zamawiający wymaga dostarczenia następujących licencji oprogramowania serwera bazy danych:

* Licencja SQL Server Standard Core Academic na 16 rdzeni procesora w paczkach po 2 licencje wraz z Software Assurance na 3 lata

**10. System zarządzania infrastrukturą sieciową**

Zamawiający wymaga dostarczenia zestawów stanowisk zarządzania infrastrukturą w liczbie 4 sztuk o minimalnych następujących parametrach:

**Monitory**

|  |  |  |
| --- | --- | --- |
| L.p. | Nazwa parametru | Wymagane minimalnie parametry techniczne |
| 1 | **Charakterystyka podstawowa** | |
|  | Wyświetlacz | LCD z podświetleniem LED, matryca aktywna TFT |
|  | Wielkość przekątnej | 27 cali |
|  | typ panelu | IPS |
|  | wspołczynnk kształtui | 16:9 |
|  | rozdzielczość natywna | QHD 2560x1440 75Hz |
|  | jasność | 350 cd/m2 |
|  | współczynnik kontrastu | 1000:1 |
|  | kąty widzenia | 178 H / 178 V |
|  | powłoka dodatkowa | anti-glare |
| 2 | **Interfejsy** | |
|  | audio | mikrofon z redukcją szumów |
|  | głośniki | 5 wat |
|  | złącza | HDMI, DisplayPort, USB 3.2 |
| 3 | **Mechaniczne** | |
|  | Regulacja pozycji ekranu | wysokość, pivot (obrót), odchylenie |
| 4 | **Pozostałe** | |
|  | Certyfikaty | EnergyStar |

**Stacje zarządzania:**

|  |  |
| --- | --- |
| Procesor: | 12 rdzeni, 16 wątków, osiągający w trybie turbo 4,4GHz, 12MB cache, typowe TDP – 28W, ze zintegrowaną kartą graficzną, osiągający wynik minimum 17300 punktów w teście PassMark – CPU Benchmarks (na dzień 22.03.2023) opublikowany na stronie <https://www.cpubenchmark.net/cpu_list.php> |
| Pamięć RAM | Minimum 16GB (DDR4, 3200MHz, so-dimm), możliwośc rozbudowy do 64GB, |
| Płyta główna | Dostępne złącza zewnętrzne:  Przód - 2x USB 3.2, 1x audio  Tył - 2x USB 4 type C, 1x USB 3.2, 1x USB 2.0, 1x RJ45, 2x HDMI 2.1, 1x port zasilania |
| Dysk | Zainstalowany dysk SSD w formacie m2 nvme, minimum o pojemności 500 GB, prędkości odczytu minimum 3500MB/s i zapisu minimum 2300MB/s, możliwośc zainstalowania drugiego dysku w obudowie |
| Napęd DVD | Nie jest wymagany |
| Karta graficzna | Zintegrowana, obsługująca do 4 ekranów, osiągająca wynik minimum 2690 punktów w teście PassMark – CPU Benchmarks (na dzień 22.03.2023) opublikowany na stronie <https://www.videocardbenchmark.net/high_end_gpus.html> |
| Multimedia | Wbudowana karta dźwiękowa zintegrowana z płytą główną |
| Łączność | LAN 10/100/1000 Mbps z portem RJ45  Karta bezprzewodowa w standardzie Wi-Fi 6E AX211(Gig+)  Bluetooth wersja minimum 5.3 |
| Obudowa | Możliwość zabezpieczenia poprzez złącze kesingtonlock  Możliwośc zawieszenia komputera zgodnie ze standardem VESA (uchwyt dołączony w zestawie)  Wymiary maksymalne obudowy 12x12x6 cm |
| Zasilacz | Zewnętrzny o mocy maksymalnej 90W  Zasilacz dołączony do zestawu |
| Klawiatura, mysz | Myszka USB 1000dpi, klawiatura USB (układ klawiszy US) – obie oznaczone trwałym logo producenta komputera |
| Właściwości specjalne | Windows AutoPilot ready  Zapisana trwale w BIOS informacja dotycząca nazwy producenta, numeru seryjnego i modelu komputera  Zintegrowany moduł TPM minimum 2.0 |
| System operacyjny | Windows 11 Pro 64-bit lub równoważny  Klucz systemu musi być zapisany trwale w BIOS i umożliwiać instalację systemu operacyjnego z nośnika lub napędu lub zdalnie bez potrzeby ręcznego wpisywania klucza licencyjnego.  Na sprzęcie powinien być umieszczony symbol legalności systemu operacyjnego w formie naklejki/hologramu potwierdzający jego autentyczność |
| Certyfikaty producenta | CE, ISO 9001, ISO 14001 |
| Gwarancja | 12 miesięcy  Gwarancja musi być realizowana przez producenta lub autoryzowanego serwis partnera producenta.  Możliwość sprawdzenia konfiguracji oraz okresu gwarancji na stronie producenta po podaniu numeru seryjnego sprzętu.  Możliwość wydłużenia gwarancji u producenta na okres do 5 lat w trakcie jej trwania. |
| Wymagania dodatkowe: | Sprzęt fabrycznie nowy, oryginalnie zapakowany, bez śladów użytkowania, oznaczony logo producenta.  Możliwość pobrania sterowników oraz obrazu systemu ze strony producenta po podaniu numeru seryjnego.  Sprzęt wyprodukowany w Europie, nie wcześniej niż w 2023 roku. |

**11. Klaster przełączników centralnych (core)**

Zamawiający wymaga dostarczenia **przełączników centralnych zestawionych w 2 klastry, po 2 przełączniki na każdy klaster (w sumie 4 urządzenia)** przełączniki spełniające następujące parametry minimalne:

Wymaga się aby urządzenie jak i zainstalowane zasilacze oraz wentylatory były objęte wieczystą gwarancją producenta realizowaną w systemie door-to-door  przez serwis producenta.

Urządzenie powinno być objęte 90 dniową pomocą techniczną telefoniczną świadczoną przez producenta urządzenia. Dodatkowo producent winien zapewnić pomoc w formie czat pracujący minimum 8 godzin dziennie w dni robocze w języku polskim przez cały okres gwarancji.

Urządzenie powinno być objęte usługą szybkiej wymiany w wypadku awarii wysłanie sprawnego urządzenia nie później niż na następny dzień roboczy przez cały okres gwarancji.

W celu realizacji warunków gwarancji oraz zachowania pełnej kompatybilności wszystkie urządzenia sieciowe aktywne w tym moduły SFP oraz SFP+ będące przedmiotem postępowania winny pochodzić od jednego producenta.

Wymaga się aby urządzenie posiadało następujące porty, protokoły oraz spełniało następujące funkcje:

* Liczba portów 24 porty 10GBaseT oraz 4 porty SFP+
* Chłodzenie od przodu do tyłu obudowy
* Tablica MAC min. 16K
* Tablica ARP/NDP min. 888
* Bufor 32Mb
* MTBF min. 247 tys. godzin
* Wydajność min. 357 Mp/s
* Przepustowość min. 480 Gb/s
* Port USB
* Port miniUSB
* Port zarządzania Out-of-band;
* Web GUI
* HTTPs
* CLI
* Telnet
* SSH
* SNMP
* MIB RSPAN
* Radius
* TACACS+
* DiffServ
* Możliwość limitowania przepustowości do 1 Kbps w oparciu o harmonogram
* IPv4/IPv6 Multicast filtering
* IGMPv3 MLDv2 Snooping
* ASM & SSM
* IGMPv1,v2 Querier
* Auto-VoIP
* Auto-iSCSI
* Policy-based routing (PBR)
* LLDP-MED
* Spanning Tree
* Green Ethernet
* STP
* MTP
* RSTP
* PV(R)STP
* BPDU/STRG Root Guard
* EEE (802.3az)
* GVRP/GMRP
* Q in Q,
* Private VLAN
* DOT1X
* MAB
* Captive Portal
* DHCP Snooping
* Dynamic ARP
* Inspection
* IP Source Guard
* CPU min 800 Mhz
* Min 1GB RAM
* Min 256MB Flash
* Min ilość obsługiwanych VLAN 4K
* DHCP Server min 2K rezerwacji
* sFlow
* Minimalna liczba przełączników w stosie: 8
* Możliwość łączenia w stos za pomocą interfejsów 10Gb/s
* Możliwość łączenia przełączników w stos w konfiguracji: pierścień, podwójny pierścień, mesh
* Non-stop forwarding (NSF)
* Distributed Link Aggregation (LAGs across the stack)
* Double VLAN Tagging (QoQ)
* PIM-DM (Multicast Routing - dense mode)
* PIM-DM (IPv6)
* PIM-SM (Multicast Routing - sparse mode)
* PIM-SM (IPv6)
* RIPv1
* RIPv2
* OSPFv2
* RFC 2328
* RFC 1583
* OSPFv3
* OSPFv2 min. sąsiadów 400
* OSPFv3 min. sąsiadów 400
* OSPFv3 min. sąsiadów na interfejs 100
* UDLD
* LLPF
* DHCPv6 Snooping
* wysyłanie alertów na email
* MMRP
* Ilość ACL min. 100
* Ilość reguł na listę min. 1023 na wejściu i 511 na wyjściu
* CE: EN 55032:2012+AC:2013/CISPR 32:2012, EN 61000-3-2:2014,
* Class A, EN 61000-3-3:2013, EN 55024:2010
* VCCI : VCCI-CISPR 32:2016, Class A
* RCM: AS/NZS CISPR 32:2013 Class A
* FCC: 47 CFR FCC Part 15, Class A, ANSI C63.4:2014
* ISED: ICES-003:2016 Issue 6, Class A, ANSI C63.4:2014
* BSMI: CNS 13438 Class A

**12. Przełącznik dostępowy**

Zamawiający wymaga dostarczenia przełączników dostępowych **(2 szt.)** spełniających następujące parametry minimalne:

Wymaga się aby urządzenie jak i zainstalowane zasilacze oraz wentylatory były objęte wieczysta gwarancją producenta realizowaną w systemie door-to-door  przez serwis producenta.

Urządzenie powinno być objęte 90 dniową pomocą techniczną telefoniczną świadczoną przez producenta urządzenia. Dodatkowo producent winien zapewnić pomoc w formie czat pracujący minimum 8 godzin dziennie w dni robocze w języku polskim przez cały okres gwarancji.

Urządzenie powinno być objęte usługą szybkiej wymiany w wypadku awarii  wysłanie sprawnego urządzenia nie później niż na następny dzień roboczy przez cały okres gwarancji.

W celu realizacji warunków gwarancji oraz zachowania pełnej kompatybilności wszystkie urządzenia sieciowe aktywne w tym moduły SFP oraz SFP+ będące przedmiotem postępowania winny pochodzić od jednego producenta.

Wymaga się aby urządzenie posiadało następujące porty, protokoły oraz spełniało następujące funkcje:

* Ilość portów 52 porty PoE+ 1GBaseT, 2 x SFP+ oraz 2 x 10GBaseT niezależne
* Chłodzenie od przodu do tyłu obudowy
* Redundantny wewnętrzny zasilacz
* Budżet mocy PoE przy zastosowaniu zasilacza 550W: 480W
* Tablica MAC min. 16K
* Tablica ARP/NDP min. 2K
* Bufor 16Mb
* MTBF min. 673207 godzin
* Wydajność min. 130,9 Mp/s
* Przepustowość min. 176 Gb/s
* Port USB
* Port miniUSB
* Port zarządzania Out-of-band;
* Web GUI
* HTTPs
* CLI
* Telnet
* SSH
* SNMP
* MIB RSPAN
* Radius
* TACACS+
* DiffServ
* Możliwość limitowania przepustowości do 1 Kbps w oparciu o harmonogram
* IPv4/IPv6 Multicast filtering
* IGMPv3 MLDv2 Snooping
* ASM & SSM
* IGMPv1,v2 Querier
* Auto-VoIP
* Auto-iSCSI
* Policy-based routing (PBR)
* LLDP-MED
* Spanning Tree
* Green Ethernet
* STP
* MTP
* RSTP
* PV(R)STP
* BPDU/STRG Root Guard
* EEE (802.3az)
* GVRP/GMRP
* Q in Q,
* Private VLAN
* DOT1X
* MAB
* Captive Portal
* DHCP Snooping
* Dynamic ARP
* Inspection
* IP Source Guard
* CPU min 800 Mhz
* Min 1GB RAM
* Min 256MB Flash
* Min ilość obsługiwanych VLAN 4K
* DHCP Server min 2K rezerwacji
* sFlow
* Minimalna ilość przełączników w stosie: 8
* Możliwość łączenia w stos przełączników z dominującymi portami 10Gb/s oraz 1Gb/s
* Możliwość łączenia w stos za pomocą interfejsów 10Gb/s
* Możliwość łączenia przełączników w stos w konfiguracji: pierścień, podwójny pierścień, mesh
* Non-stop forwarding (NSF)
* Distributed Link Aggregation (LAGs across the stack)
* Ilość interfejsów IP 128
* Double VLAN Tagging (QoQ)
* PIM-DM (Multicast Routing - dense mode)
* PIM-DM (IPv6)
* PIM-SM (Multicast Routing - sparse mode)
* PIM-SM (IPv6)
* RIPv1
* RIPv2
* OSPFv2
* RFC 2328
* RFC 1583
* OSPFv3
* OSPFv2 min. sąsiadów 400
* OSPFv3 min. sąsiadów 400
* OSPFv3 min. sąsiadów na interfejs 100
* UDLD
* LLPF
* DHCPv6 Snooping
* wysyłanie alertów na email
* MMRP
* Ilość ACL min. 100
* Ilość reguł na listę min. 1023 na wejściu i 511 na wyjściu
* Zasilacz z certyfikatem 80+
* CE mark, commercial
* FCC Part 15 Class A
* VCCI Class A
* Class A EN 55022
* (CISPR 22) Class A
* Class A C-Tick
* EN 50082-1
* EN 55024
* CSA certified (CSA 22.2 #950)
* UL listed (UL 1950)/cUL IEC 950/EN 60950

**13. Router UTM**

Zamawiający wymaga dostarczenia **Routera UTM (1 szt.)** spełniającego następujące parametry minimalne:

# Wymagania Ogólne

System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall’a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu.

System wspiera protokoły 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 – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji.
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.
4. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.

# Interfejsy, Dysk, Zasilanie:

1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów:

* 10 portami Gigabit Ethernet RJ-45.

1. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
2. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN’y w oparciu o standard 802.1Q.
3. System jest wyposażony w zasilanie AC.

# Parametry wydajnościowe:

1. W zakresie Firewall’a obsługa nie mniej niż 1.4 mln. jednoczesnych połączeń oraz 32 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.7 Gbps.
4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 6 Gbps.
5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1.3 Gbps.
6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 750 Mbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 650 Mbps.

# Funkcje Systemu Bezpieczeństwa:

W ramach systemu ochrony są 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.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są 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. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.
12. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system.
13. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).

# Polityki, Firewall

1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System realizuje 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.

1. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
2. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP.
3. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.
4. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.
5. Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu.

* Amazon Web Services (AWS).
* Microsoft Azure.
* Cisco ACI.
* Google Cloud Platform (GCP).
* OpenStack.
* VMware NSX.
* Kubernetes.

# Połączenia VPN

1. Rozwiązanie umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:

* Wsparcie dla IKE v1 oraz v2.
* Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM).
* Obsługa protokołu Diffie-Hellman grup 19, 20.
* Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh.
* 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.
* Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat.
* Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.
* Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu.
* Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth.
* Mechanizm „Split tunneling” dla połączeń Client-to-Site.

1. Rozwiązanie umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia:

* Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie rozwiązanie zapewnia stronę komunikacyjną działającą w oparciu o HTML 5.0.
* Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.
* Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.

# Routing i obsługa łączy WAN

W zakresie routingu rozwiązanie zapewnia obsługę:

1. Routingu statycznego.
2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP).
3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM.
4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu.
5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu.
6. BFD (Bidirectional Forwarding Detection).
7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.

# Funkcje SD-WAN

1. Rozwiązanie umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.
2. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).

# Zarządzanie pasmem

1. Rozwiązanie Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. Rozwiązanie daje możliwość określania pasma dla poszczególnych aplikacji.
3. Rozwiązanie pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.
4. Rozwiązanie zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.

# Ochrona przed malware

1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.
3. Rozwiązanie umożliwia skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości.
4. Rozwiązanie umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.
5. Rozwiązanie dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
7. Rozwiązanie współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w chmurze.
8. Rozwiązanie zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
9. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.
10. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.

# Ochrona przed atakami

1. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. Rozwiązanie chroni przed atakami na aplikacje pracujące na niestandardowych portach.
3. Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
4. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur.
5. Rozwiązanie zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
6. Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty).
7. Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http.
8. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
9. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.

# Kontrola aplikacji

1. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur.
6. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).
7. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).

# Kontrola WWW

1. Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
3. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard.
4. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex).
6. Filtr WWW daje możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.
7. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.
8. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.
9. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.

# Uwierzytelnianie użytkowników w ramach sesji

1. System Firewall umożliwia 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.

1. System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.
2. System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.
3. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

# Zarządzanie

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów.
3. Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.
5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.
8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).
9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.

# Logowanie

1. Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
2. W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
3. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.
4. Możliwość włączenia logowania per reguła w polityce firewall.
5. System zapewnia możliwość logowania do serwera SYSLOG.
6. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.

# Certyfikaty

Poszczególne elementy systemu bezpieczeństwa posiadają następujące certyfikacje:

* ICSA lub EAL4 dla funkcji Firewall.

# Testy wydajnościowe oraz funkcjonalne

1. Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta oraz wykonane testy.

# Serwisy i licencje

Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje:

b)     Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 36 miesięcy.

# Gwarancja oraz wsparcie

1. Gwarancja: Rozwiązanie jest objęte serwisem gwarancyjnym producenta przez okres 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (advanced hardware replacement). W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

# Opisy do wymagań ogólnych

1. Zaleca się, aby w przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), został uzyskany dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.
2. Zaleca się, aby został uzyskany dokument - oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż produkt pochodzi z autoryzowanego kanału sprzedaży, np. poprzez oświadczenie o posiadanym statusie autoryzacyjnym.

**14. Usługi informatyczne**

I. Montaż dostarczonych urządzeń.

Wszystkie urządzenia powinny zostać zamontowane w szafach rack w serwerowniach wskazanych przez Zamawiającego. Serwerownie znajdują się w siedzibie Zamawiającego i mają tworzyć dwa główne węzły sieci, połączone ze sobą za pomocą światłowodu.

W ramach wdrożenia Wykonawca dostarczy komplet okablowania typu patchcord i komplet wkładek SFP niezbędny do prawidłowego działania całego rozwiązania. Okablowanie należy ułożyć w sposób zorganizowany i gwarantujący jego możliwie długą trwałość z wykorzystaniem paneli porządkujących.

Interfejsy sieciowe urządzeń sieciowych, serwerów i macierzy umożliwiające zarzadzanie urządzeniami muszą znajdować się w wydzielonej podsieci, do której nie mogą mieć dostępu użytkownicy. Dostęp sieciowy należy zrealizować zgodnie z zasadą minimalnego dostępu.

Wszystkie dostarczone urządzenia oraz systemy muszą tworzyć kompletne i działające rozwiązanie. Koncepcję konfiguracji poszczególnych elementów należy opracować we współpracy z Zamawiającym i wdrożyć po uzyskaniu jego akceptacji.

Przed montażem urządzeń należy sporządzić plan instalacji fizycznej uwzględniający wszystkie urządzenia, propozycję ich lokalizacji w szafach rack, nazewnictwa i adresacji IP.

Po zakończeniu prac należy dostarczyć dokumentację powykonawczą zawierającą:

* schemat fizyczny i logiczny sieci,
* dokumentację woluminów dyskowych,
* dokumentację konfiguracji klastra HA serwerów wirtualizacji,
* dokumentację adresacji IP,
* rejestr haseł.

Po zakończeniu prac Wykonawca zapewni Zamawiającemu zdalne wsparcie techniczne w zakresie dostarczonego rozwiązania przez okres nie mniej 30 dni pracy techników. Wsparcie techniczne rozumiane jest jako konsultacje telefoniczne, mailowe oraz pomoc zdalna.

Po zakończeniu prac Wykonawca sporządzi protokół, na podstawie którego Zamawiający dokona odbioru prac w zakresie montażu i uruchomienia infrastruktury.

II. Zadania dotyczące sieci LAN.

1. Przygotowanie koncepcji i wdrożenie zasad ochrony UTM (np. IPS, antywirus, antyspam, deszyfracja SSL) dla poszczególnych podsieci VLAN po akceptacji przez Zamawiającego.
2. Wdrożenie klastrów przełączników centralnych (stack) w serwerowniach z wykorzystaniem połączenia światłowodowego dostarczonego przez Zamawiającego.
3. Wdrożenie przełączników dystrybucyjno-dostępowych.
4. Połączenie przełączników dystrybucyjno-dostępowych z przełącznikami centralnymi w sposób gwarantujący redundancję połączeń.
5. Opracowanie koncepcji podziału sieci na podsieci (VLAN) gwarantującego bezpieczeństwo funkcjonowania i spójność adresacji IP dla usług, wraz z określeniem zasad dostępu i miejscem ich terminacji (router UTM, przełączniki centralne).
6. Integracja aktualnej infrastruktury sieciowej z przełącznikami dostarczonymi w projekcie.

III. Zadania dotyczące serwerów.

1. Połączenie serwerów z macierzą za pomocą dedykowanych połączeń i interfejsów iSCSI.
2. Wdrożenie klastra HA serwerów wirtualizacji składającego się z 3 serwerów oraz macierzy dyskowej zgodnie z przyjętą koncepcją.
3. Wdrożenie zapasowej macierzy dyskowej w drugiej serwerowni i połączenie jej z serwerownią główną z wykorzystaniem połączenia światłowodowego dostarczonego przez Zamawiającego.
4. Wdrożenie replikacji serwerów wirtualnych na zapasową macierz dyskową za pomocą dedykowanych do tego interfejsów sieciowych serwera.

IV. Kopie zapasowe.

1. Podłączenie serwera NAS we wskazanej przez Zamawiającego serwerowni.
2. Macierz NAS nie może być dostępna z sieci użytkowników i powinna być szczególnie chroniona ze względu na bezpieczeństwo kopii zapasowych.
3. Opracowanie koncepcji wykonywania kopii zapasowych serwerów wirtualnych działających w rozwiązaniu klastrowym HA serwerów wirtualizacji.

V. Migracja obecnego systemu maszyn wirtualnych na nowe dostarczone rozwiązanie.

1. Opracowanie optymalnej koncepcji migracji serwerów wirtualnych z obecnego systemu wirtualizacji vSphere 6.0   
   (około 7 TB danych) do nowo dostarczonego klastra HA serwerów wirtualizacji, wraz z oszacowaniem czasu trwania całej operacji oraz planowanych przerw w dostępie do systemów i uzyskanie akceptacji koncepcji u Zamawiającego.
2. Migracja serwerów wirtualnych Windows Server zgodnie z przyjętą koncepcją w terminie do 30 dni od zakończenia prac wdrożeniowych, tj. montażu i uruchomienia infrastruktury oraz odbioru protokołem wykonanych prac   
   wdrożeniowych

VI. Monitoring sieci.

Wraz z urządzeniami należy dostarczyć i wdrożyć w działającej infrastrukturze sieciowo-serwerowej system monitorowania pracy dostarczonych urządzeń sieciowych, serwerów fizycznych, macierzy dyskowych i uruchomionych serwerów wirtualnych, spełniający minimum:

1. Dostęp do systemu przez przeglądarkę internetową, przy czym dostęp do serwisu webowego powinien być ograniczony do działu IT Zamawiającego oraz dostępu zdalnego VPN dla członków konkretnej grupy zabezpieczeń Active Directory.
2. Dostęp do systemu powinien odbywać się za pomocą logowania na stronie WWW, a konta poszczególnych użytkowników powinny być związane z konkretnymi uprawnieniami (administrator, technik, przeglądający).
3. System powinien posiadać widok ukazujący listę zdarzeń, na które powinni zareagować członkowie działu IT z podziałem na błędy i ostrzeżenia.
4. System powinien posiadać widok ukazujący ogólny stan działania infrastruktury sieciowo-serwerowej.
5. System powinien umożliwiać monitorowanie co najmniej następujących parametrów:

* serwery fizyczne: ogólny stan komponentów sprzętowych serwera, dostępność (ping), wykorzystanie CPU, RAM i dysków, stan zapory sieciowej, stan instalacji aktualizacji Windows;
* serwery wirtualne: dostępność (ping), wykorzystanie CPU, RAM i dysków, stan zapory sieciowej, stan instalacji aktualizacji Windows;
* macierze dyskowe: dostępność (ping), ogólny stan komponentów sprzętowych;
* przełączniki sieciowe: dostępność (ping),
* router UTM: dostępność (ping), wykorzystanie CPU i RAM, wersję firmware.

9/ZP/RZPWE/2023 ZAŁĄCZNIK NR 2 DO SWZ – FORMULARZ OFERTOWY

**FORMULARZ OFERTOWY**

Nazwa Wykonawcy/Wykonawców w przypadku oferty wspólnej: ...............................................................................................

Adres: ....................................................................................

tel. .........…………................……………………………………………..…

FAX. ………………………………………………………………………………..

REGON: …………………................……………………………………………

NIP: …………………………………................…………………………………

Adres e-mail na który Zamawiający ma przesyłać korespondencję …………………………………

* 1. Odpowiadając na zaproszenie do wzięcia udziału w postępowaniu prowadzonym w trybie podstawowym bez negocjacji o wartości zamówienia nie przekraczającej progów unijnych o jakich stanowi art. 3 ustawy z 11 września 2019 r. - Prawo zamówień publicznych (Dz. U. z 2022 r. poz. 1710 ze zm.) – dalej p.z.p. **na dostawę infrastruktury serwerowej na potrzeby RZPWE**

Oferujemy wykonanie przedmiotu zamówienia łącznie za cenę brutto:........................................ PLN, słownie: ..................................................................................................................**,**

**w tym:** Migracja serwerów wirtualnych Windows Server wynosi brutto…………………………….. słownie:…………………………………………………………………………**.**

* 1. Deklarujemy, że I etap zamówienia wykonamy w terminie: (proszę wpisać liczbę tygodni):……………………………(minimalny czas dostawy 10 tygodni, maksymalny czas dostawy 20 tygodni)
  2. Deklarujemy czas udzielenia gwarancji na dostarczony sprzęt:

– grupa I: poz. 1 – serwer, poz. 2 – macierz dyskowa, poz. 4 - Zapasowa macierz dyskowa, poz. 5 Serwer NAS przeznaczony do archiwizacji danych - (proszę wpisać liczbę miesięcy):……………………………( minimalny okres 36 miesięcy, maksymalny czas 60 miesięcy)

grupa II: poz. 6 – zasilacz awaryjny UPS, poz. 10 – system zarządzania infrastrukturą sieciową - (proszę wpisać liczbę miesięcy):……………………………( minimalny okres 12 miesięcy, maksymalny czas 60 miesięcy)

* 1. Deklarujemy, że udzielę okresu wsparcia technicznego/serwisu technicznego (proszę podać liczbę dni): …………………………. (minimalny czas wsparcia technicznego/serwisu technicznego to 30 dni, maksymalny czas wsparcia technicznego/serwisu technicznego to 90 dni)
  2. Oświadczamy, że zapoznaliśmy się ze specyfikacją warunków zamówienia (w tym wzorem umowy) i nie wnosimy do niej żadnych zastrzeżeń oraz przyjmujemy warunki w niej zawarte.
  3. Akceptujemy termin wykonania zamówienia i warunki płatności opisane we wzorze umowy.
  4. Oświadczamy, że nie podlegamy wykluczeniu z postępowania na podstawie art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego (Dz. U. poz. 835).
  5. Oświadczamy, że uzyskaliśmy wszelkie informacje niezbędne do prawidłowego przygotowania i złożenia niniejszej oferty.
  6. Oświadczamy, że jesteśmy związani ofertą przez okres 30 dni, który rozpoczyna się wraz z upływem terminu składania ofert.
  7. W przypadku przyznania nam zamówienia, zobowiązujemy się do zawarcia umowy w miejscu i terminie wskazanym przez zamawiającego.
  8. Oferta została złożona na …….… stronach podpisanych i kolejno ponumerowanych od nr ………………. do nr ……………...
  9. STATUS PRZEDSIĘBIORCY. Wyłącznie do celów statystycznych Urzędu Zamówień Publicznych, należy zaznaczyć jedną z poniższych opcji: Wykonawca jest mikro / małym / średnim przedsiębiorcą:……………………..(wpisać właściwe) tj. zatrudnia mniej niż 250 osób i jego roczny obrót nie przekracza 50 milionów euro lub roczna suma bilansowa nie przekracza 43 milionów euro.
  10. Zamówienie zrealizujemy sami / przy udziale podwykonawców\*, którzy będą wykonywać następujące zakresy zamówienia:

**Zakres I** ……………………………………………………………………………………………… realizowany przez (nazwa lub imię i nazwisko oraz dane kontaktowe podwykonawcy - jeżeli są znane)………………………………………………………………..

**Zakres II** ……………………………………………………………………………………………… realizowany przez (nazwa lub imię i nazwisko oraz dane kontaktowe podwykonawcy - jeżeli są znane)………………………………………………………………

* 1. Zgodnie z art. 117 ust. 4 ustawy Pzp, wykonawcy wspólnie ubiegający się o udzielenie zamówienia w treści formularza ofertowego wskazują, które usługi/dostawy/roboty budowlane wykonają poszczególni wykonawcy (jeżeli dotyczy):

……………………………………………………………………………...………………………

1. Integralną część oferty stanowią następujące dokumenty:

A ) …………………………………………………………………………………………………………….

B ) …………………………………………………………………………………………………………….

C ) …………………………………………………………………………………………………………….

1. Oświadczam, że wypełniłem obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO (rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1). wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu. (W przypadku gdy wykonawca nie przekazuje danych osobowych innych niż bezpośrednio jego dotyczących lub zachodzi wyłączenie stosowania obowiązku informacyjnego, stosownie do art. 13 ust. 4 lub art. 14 ust. 5 RODO treści oświadczenia wykonawca nie składa (usunięcie treści oświadczenia np. przez jego wykreślenie).

…………………………………………. ………………………………………………………….……………………………

/miejscowość i data/ /Imię Nazwisko i podpis przedstawiciela wykonawcy/ \*\*

\* - niepotrzebne skreślić

\*\* - podpis osoby lub osób figurujących w rejestrach uprawnionych do zaciągania zobowiązań w imieniu wykonawcy lub we właściwym upoważnieniu

9/ZP/RZPWE/2023 ZAŁĄCZNIK NR 2a DO SWZ – formularz rzeczowy

**FORMULARZ RZECZOWY**

**1. Serwer – 3 szt.**

|  |  |  |
| --- | --- | --- |
| L.p. | Nazwa parametru | parametry techniczne, typ, model, producent oferowanego sprzętu |
| 1 | **Typ obudowy, model producenta, wysokość U** |  |
| 2 | **Liczba i model procesora** |  |
| 3 | **Typ, ilość i rodzaj pamięci operacyjnej** |  |
| 4 | **Konfiguracja i ilość dysków, w tym konf.RAID** |  |
| 5 | **Zasilanie, zasilacze** |  |
| 6 | **Interfejsy sieciowe** |  |
| 7 | **Porty** |  |
| 8 | **Chłodzenie** |  |
| 9 | **System zarządzania** |  |
| 10 | **Funkcje zabezpieczeń** |  |
| 11 | **Urządzenia hot swap** |  |
| 12 | **Funkcje diagnostyki** |  |
| 13 | **Gwarancja** |  |

**2. Macierz dyskowa – 1 szt.**

|  |  |  |
| --- | --- | --- |
| L.p. | Nazwa parametru | parametry techniczne, typ, model, producent oferowanego sprzętu |
| 1 | **Typ obudowy, producent, dokładne oznaczenie modelu** |  |
| 2 | **Liczba, modele dysków** |  |
| 3 | **Interfejsy sieciowa** |  |
| 4 | **Wsparcie RAID** |  |
| 5 | **Gwarancja i serwis** |  |

**3. Licencja oprogramowania do wirtualizacji (**Zamawiający wymaga dostarczenia Oprogramowania do wirtualizacji serwerów wraz z konsolą zarządzania zaoferowanym oprogramowaniem)

**Oprogramowanie do wirtualizacji serwerów – proszę opisać dokładny, jednoznaczny** typ licencji, model, producent oferowanego oprogramowania:

…..

**4. Zapasowa macierz dyskowa – 1 szt.**

|  |  |  |
| --- | --- | --- |
| L.p. | Nazwa parametru | parametry techniczne, typ, model, producent oferowanego sprzętu |
| 1 | **Typ obudowy, producent, dokładne oznaczenie modelu** |  |
| 2 | **Pamięć RAM** |  |
| 3 | **Przestrzeń dyskowa (ilość zatok), w tym modele dysków** |  |
| 4 | **Porty komunikacyjne oraz sieciowe** |  |
| 5 | **Wentylator obudowy** |  |
| 6 | **Obsługiwane protokoły sieciowe** |  |
| 7 | **Obsługiwane typy macierzy RAID** |  |
| 8 | **Współpraca z systemami wirtualizacji** |  |
| 9 | **Gwarancja** |  |

**5. Serwer NAS do archiwizacji danych – 1 szt.**

|  |  |  |
| --- | --- | --- |
| L.p. | Nazwa parametru | parametry techniczne, typ, model, producent oferowanego sprzętu |
| 1 | **Typ obudowy, producent, dokładne oznaczenie modelu** |  |
| 2 | **Pamięć RAM** |  |
| 3 | **Przestrzeń dyskowa (ilość zatok), w tym modele dysków** |  |
| 4 | **Porty komunikacyjne oraz sieciowe** |  |
| 5 | **Wentylator obudowy** |  |
| 6 | **Obsługiwane protokoły sieciowe** |  |
| 7 | **Obsługiwane typy macierzy RAID** |  |
| 8 | **Współpraca z systemami wirtualizacji** |  |
| 9 | **Gwarancja** |  |

**6. Zasilacz awaryjny UPS- 1 szt.**:

|  |  |  |
| --- | --- | --- |
| L.p. | Nazwa parametru | parametry techniczne, typ, model, producent oferowanego sprzętu |
|  | **Typ obudowy, producent, dokładne oznaczenie modelu:** | |
| 1 | **Charakterystyka podstawowa** | |
|  | Technologia wykonania UPS |  |
|  | Możliwość rozbudowy o kolejne UPS (praca równoległa) |  |
|  | Moc pozorna (VA) |  |
|  | Moc rzeczywista (W) |  |
|  | Kształt fali na wyjściu(praca na baterii) |  |
|  | Kompatybilność z zasilaczami z aktywnym PFC |  |
|  | Ochrona przed przeciążeniem |  |
|  | Filtr EMI/RFI |  |
|  | Układ przeciwprzepięciowy (Dżule) |  |
| 2 | **Charakterystyka wejścia/wyjścia** | |
|  | Nominalne napięcie wejściowe (V) |  |
|  | Obsługiwany zakres napięcia wejściowego (V) |  |
|  | Częstotliwość wejściowa(Hz) |  |
|  | Wykrywanie częstotliwości wejściowej |  |
|  | Napięcie przy pracy na baterii (V) |  |
|  | Częstotliwość przy pracy baterii (Hz) |  |
| 3 | **Charakterystyka gniazd** | |
|  | Rodzaj złącza wejściowego |  |
|  | Rodzaj złącza wyjściowego |  |
| 4 | **Charakterystyka baterii** | |
|  | Typowy czas przełączenia na baterie (ms) |  |
|  | Bateria |  |
|  | Ilość obsługiwanych modułów baterii |  |
| 6 | **Zarządzanie** | |
|  | Sygnalizacja |  |
|  | Alarmy dźwiękowe |  |
|  | Konfiguracja wybranych parametrów |  |
|  | Port komunikacyjny USB |  |
|  | Port wyłącznika awaryjnego EPO |  |
|  | Dołączone oprogramowanie do zarządzania |  |
|  | Zarządzanie przez sieć |  |
| 7 | **Cechy fizyczne** | |
|  | Obudowa - typ |  |
|  | Konstrukcja obudowy |  |
|  | Szyny/uchwyty rack |  |
|  | Rozmiary (szer. x wys. x gł.) (mm) |  |
|  | Waga |  |
| 8 | **Dane środowiskowe** | |
|  | Temperatura robocza (°C) |  |
|  | Względna wilgotność robocza (bez kondensacji) (%) |  |
| 7 | **Pozostałe** | |
|  | Certyfikaty |  |
|  | Gwarancja |  |

**7. Oprogramowanie do wykonywania kopii bezpieczeństwa**

|  |  |
| --- | --- |
| Nazwa Parametru | parametry techniczne, typ, model, producent oferowanego oprogramowania, funkcjonalności |
| Licencje backup dla oferowanych urządzeń zgodnie z ilością CPU oferowanych urządzeń - na 35 serwerów wirtualnych |  |

**8. Licencje systemu operacyjnego**

Zamawiający wymaga dostarczenia następujących licencji systemu operacyjnego:

* Licencja Windows Server 2022 Datacenter Academic na 72 rdzenie procesora w paczkach po 2 licencje
* Licencja Windows Server 2022 User CAL Academic - 10 szt.
* Licencja Windows Server 2022 External Connector - 2 szt.

**9. Licencje oprogramowanie serwera bazy danych**

Zamawiający wymaga dostarczenia następujących licencji oprogramowania serwera bazy danych:

* Licencja SQL Server Standard Core Academic na 16 rdzeni procesora w paczkach po 2 licencje wraz z Software Assurance na 3 lata

**10. System zarządzania infrastrukturą sieciową – 4 zestawy**

**Monitory**

|  |  |  |
| --- | --- | --- |
| L.p. | Nazwa parametru | Wymagane minimalnie parametry techniczne |
|  | **Typ obudowy, producent, dokładne oznaczenie modelu:** | |
| 1 | **Charakterystyka podstawowa** | |
|  | Wielkość przekątnej |  |
|  | typ panelu |  |
|  | współczynnik kształtu |  |
|  | rozdzielczość natywna |  |
|  | jasność |  |
|  | współczynnik kontrastu |  |
|  | kąty widzenia |  |
|  | powłoka dodatkowa |  |
| 2 | **Interfejsy** | |
|  | audio |  |
|  | głośniki |  |
|  | złącza |  |
| 3 | **Mechaniczne** | |
|  | Regulacja pozycji ekranu |  |
| 4 | **Pozostałe** | |
|  | Gwarancja |  |

**Stacje zarządzania:**

|  |  |
| --- | --- |
| Nazwa Parametru | parametry techniczne, typ, model, producent oferowanego oprogramowania, funkcjonalności |
| **Typ obudowy, producent, dokładne oznaczenie modelu:** |  |
| Procesor: |  |
| Pamięć RAM |  |
| Porty połączeniowe |  |
| Dysk |  |
| Napęd DVD |  |
| Karta graficzna |  |
| Porty sieciowe i komunikacyjne |  |
| Obudowa |  |
| Zasilacz |  |
| Klawiatura, mysz |  |
| System operacyjny |  |
| Certyfikaty producenta |  |
| Gwarancja |  |

**11.Klaster przełączników centralnych (core) - przełączniki centralne zestawionych w 2 klastry, po 2 przełączniki na każdy klaster (w sumie 4 urządzenia)**, proszę opisać parametry techniczne, typ, model, producent, funkcjonalności:

**….**

**12. Przełącznik dostępowy – 2 szt.,** proszę podać dokładny model i producenta oraz opisać parametry techniczne, funkcjonalności:

**….**

**13. Router UTM – 1 szt.,**

|  |  |  |
| --- | --- | --- |
| L.p. |  | proszę opisać parametry techniczne, typ, model, producent, funkcjonalności: |
| 1. | **Producent, dokładne oznaczenie modelu:** |  |
| 2. | Interfejsy sieciowe |  |
| 3. | Parametry wydajnościowe: |  |
| 4. | Obsługa VPN |  |
| 5. | Wsparcie producenta (zakres i okres): |  |
| 6. | Gwarancja: |  |

ZAŁĄCZNIK NR 3 DO SWZ – OŚWIADCZENIE WYKONAWCY

9/ZP/RZPWE/2023

**OŚWIADCZENIE WYKONAWCY**

**składane na podstawie art. 125 ust. 1 ustawy z dnia 11 września 2019 r.  
Prawo zamówień publicznych (dalej jako: Pzp)**

**DOTYCZĄCE PODSTAW WYKLUCZENIA *Z* POSTĘPOWANIA**

|  |  |
| --- | --- |
| Wykonawca [firma][[1]](#footnote-1): |  |
| Adres siedziby: |  |
| Nr KRS / CEiDG |  |
| NIP: |  |
| Imię i nazwisko osoby uprawnionej do reprezentowania Wykonawcy / podstawa do reprezentacji |  |
| Podanie podstawy uprawnienia do reprezentowania Wykonawcy |  |

Na potrzeby postępowania o udzielenie zamówienia publicznego w trybie podstawowym bez negocjacji o wartości zamówienia nie przekraczającej progów unijnych o jakich stanowi art. 3 ustawy z 11 września 2019 r. - Prawo zamówień publicznych (Dz. U. z 2022 r. poz. 1710 ze zm.) – dalej p.z.p, **na dostawę infrastruktury serwerowej na potrzeby RZPWE,** oświadczam, że:

1. spełniam warunki udziału w postępowaniu określone przez Zamawiającego w Specyfikacji Warunków Zamówienia –składam swoją ofertę.
2. w celu wykazania spełniania warunków udziału w postępowaniu, określonych przez Zamawiającego w Specyfikacji Warunków Zamówienia, polegam na zasobach następującego/ych podmiotu/ów (jeżeli dotyczy):

……………………………………………………………………...……………………………………………………………………………………………………………….

w następującym zakresie:

……………………………………………………………………………………………...………………………………………………………………………………………

(wskazać podmiot i określić odpowiedni zakres dla wskazanego podmiotu).

1. nie podlegam wykluczeniu z postępowania na podstawie art. 108 ust. 1 i 109 ust. 1 pkt. 4 ) ustawy Pzp;
2. nie podlegam wykluczeniu z postępowania na podstawie art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego (Dz.U. poz. 835).
3. zachodzą w stosunku do mnie podstawy wykluczenia z postępowania na podstawie art. …… ustawy Pzp[[2]](#footnote-2)
4. jednocześnie oświadczam, że w związku z ww. okolicznością z pkt 2 na podstawie art. 110 ust. 2 ustawy Pzp podjąłem następujące środki naprawcze

…………………………………………………………………………………………………

…………………………………………………………………………………………………

…………………………………………………………………………………………………

**OŚWIADCZENIE DOTYCZĄCE PODWYKONAWCY NIEBĘDĄCEGO PODMIOTEM, NA KTÓREGO ZASOBY POWOŁUJE SIĘ WYKONAWCA**

Oświadczam, że w stosunku do następującego/-ych podmiotu/-tów, będącego/-ych podwykonawcą/-ami: ………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………

*(należy podać pełną nazwę/firmę, adres, a także w zależności od podmiotu: NIP/PESEL, KRS/CEiDG)*,

nie zachodzą podstawy wykluczenia z postępowania o udzielenie zamówienia.

Oświadczam, że w stosunku do podmiotu:

…………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………….

*(należy podać pełną nazwę/firmę, adres, a także w zależności od podmiotu: NIP/PESEL, KRS/CEiDG)*

zachodzą podstawy wykluczenia z postępowania na podstawie art. …………. ustawy Pzp

*(podać mającą zastosowanie podstawę wykluczenia)*

Jednocześnie oświadczam, że w związku z ww. okolicznością, na podstawie art. 110 ust. 2 ustawy Pzp podjęte zostały następujące środki naprawcze:

…………………………………………………………………………………………..…………………...........…………………………………………………………………………………………………..…………………...........…………………………………………………………………………………………………..…………………...........………………………………………………………………….

**OŚWIADCZENIE DOTYCZĄCE PODANYCH INFORMACJI:**

Oświadczam, że wszystkie informacje podane w powyższych oświadczeniach są aktualne i zgodne   
z prawdą oraz zostały przedstawione z pełną świadomością konsekwencji wprowa­dzenia Zamawiającego w błąd przy przedstawianiu informacji.

Miejscowość …………….….…., dnia ……..………… ........................................................

*(podpis osoby/(-ób) uprawnionej do reprezentowania Wykonawcy)*

ZAŁĄCZNIK NR 4 DO SWZ- WZÓR UMOWY

**UMOWA NR 9/ZP/RZPWE/2023**

**zawarta w dniu …………………... r.**

pomiędzy:

Województwem Opolskim z siedzibą: 45-082 Opole, ul. Piastowska 14, NIP: 7543077565, Regionalnym Zespołem Placówek Wsparcia Edukacji

reprezentowanym przez: **.........................................** – Dyrektora Regionalnego Zespołu Placówek Wsparcia Edukacji,

zwanym dalej **Zamawiającym**,

a

…………………………………………………………………………………………………………………………………………................……………………………………………………………………………………………………………………………………………………...................................................……………

reprezentowaną/reprezentowanym\* przez:

………………………………………………………………,

zwanym dalej **Wykonawcą**,

wyniku udzielenia zamówienia publicznego w trybie podstawowym bez negocjacji o wartości zamówienia nie przekraczającej progów unijnych o jakich stanowi art. 3 ustawy z 11 września 2019 r. Prawo Zamówień Publicznych (Dz.U z 2022 poz. 1710 ze zm.) zostaje zawarta umowa o następującej treści:

**§ 1**

* + - 1. Przedmiotem zamówienia jest **dostawa infrastruktury serwerowej na potrzeby Regionalnego Zespołu Placówek Wsparcia Edukacji.**
      2. Szczegółowy opis przedmiotu zamówienia stanowi załącznik nr 1 do umowy.

**§ 2**

1. **Całkowita wartość umowy wynika z oferty Wykonawcy i wynosi brutto:........................................ PLN, słownie:......................................................................................................., w tym: Migracja serwerów wirtualnych Windows Server zgodnie z przyjętą koncepcją wynosi brutto…………………………….. słownie:…………………………………………………**
2. **Termin realizacji przedmiotu umowy:** 
   * + 1. **Etap I: dostawa, montaż, konfiguracja/wdrożenie i uruchomienie infrastruktury serwerowej: …………………….tygodni od dnia podpisania umowy,**
       2. **Etap II: Migracja serwerów wirtualnych Windows Server: do 30 dni od dnia od zakończenia prac wdrożeniowych, tj. montażu i uruchomienia infrastruktury oraz odbioru protokołem wykonanych prac wdrożeniowych**
3. **Termin gwarancji na przedmiot zamówienia:**
4. **Grupa I (poz. 1,2,4,5) ....................... miesięcy**
5. **Grupa II: (poz. 6 i 10) ....................... miesięcy**
6. **Wsparcie techniczne od dnia protokołu odbioru potwierdzającego realizację przedmiotu umowy (etap I)................dni**
7. Całkowita wartość umowy obejmuje wszelkie koszty związane z realizacją zamówienia i nie może ulec zwiększeniu przez cały okres realizacji umowy.

**§ 3**

1. Osoby wyznaczone do kontaktów w sprawie realizacji umowy:
2. po stronie Wykonawcy: **…………………………**, tel.: **…………………………..**, e-mail: **……………………………..**
3. po stronie Zamawiającego: **……………………………..** tel.: **………………..…..**, e-mail: **……………………**
4. Zmiany osób, o których mowa w ust. 1, nie stanowią zmiany umowy w rozumieniu § 7 i nie wymagają aneksu, a jedynie pisemnego poinformowania drugiej Strony o zaistniałej sytuacji.

**§ 4**

* 1. Płatność za przedmiot umowy nastąpi na rachunek bankowy Wykonawcy w ciągu 30 dni od daty otrzymania przez Zamawiającego prawidłowo wystawionej faktury, z zastrzeżeniem zdania 2. Płatność następuje nie wcześniej niż po podpisaniu przynajmniej przez jedną osobę ze strony Zamawiającego i przez osobę ze strony Wykonawcy, o których mowa w § 3 ust. 1, protokołu odbioru sporządzonego po każdym etapie realizacji przedmiotu umowy, tj. bez zastrzeżeń zgodnie z ceną podaną w formularzu ofertowym Wykonawcy. Wykonawca ma prawo wystawić dwie faktury, po zrealizowaniu każdego z dwóch etapów. Etap I: dostawa, montaż, konfiguracja/wdrożenie i uruchomienie infrastruktury serwerowej. Etap II: Migracja serwerów wirtualnych Windows Server zgodnie z przyjętą koncepcją.
  2. NIP Zamawiającego: 7543077565 (Województwo Opolskie).
  3. Odbiorcą jest Regionalny Zespół Placówek Wsparcia Edukacji w Opolu, ul. Głogowska 27, 45-315 Opole.
  4. Wykonawca zobowiązany jest wystawiać faktury wg wzoru:

|  |  |
| --- | --- |
| Nabywca:  Województwo Opolskie  ul. Piastowska 14  45-082 Opole  NIP: 7543077565 | Odbiorca:  Regionalny Zespół Placówek Wsparcia Edukacji  ul. Głogowska 27  45-315 Opole |

* 1. Bank i nr rachunku bankowego Wykonawcy: wg faktury.
  2. Za dzień zapłaty faktury uważa się datę obciążenia rachunku bankowego Zamawiającego.
  3. Za zwłokę w zapłaceniu faktury Wykonawca ma prawo do naliczenia odsetek ustawowych.
  4. Niezależnym od Zamawiającego warunkiem zrealizowania przelewu na konto Wykonawcy w terminie, o którym mowa w ust. 1, jest dostępność środków pieniężnych na jego projektowym rachunku bankowym. Dostępność ta uzależniona jest od transferów środków z Instytucji Pośredniczącej. Uregulowanie należności nastąpi niezwłocznie po otrzymaniu przez Zamawiającego środków i z tego tytułu Wykonawca nie będzie dochodził ewentualnego roszczenia o odsetki powstałe w wyniku nieterminowej zapłaty wynagrodzenia.
  5. Zamawiający nie wyraża zgody na przelew wierzytelności przez Wykonawcę na rzecz osoby trzeciej z tytułu wynagrodzenia należnego na podstawie niniejszej umowy, z wyjątkiem przelewu wierzytelności na rzecz banku, w związku z zabezpieczeniem kredytu bankowego udzielonego Wykonawcy na realizację niniejszej umowy, na co Wykonawca musi uzyskać pisemną zgodę Zamawiającego.

**§ 5**

1. Za odstąpienie od umowy przez Wykonawcę z przyczyn od niego zależnych, Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 20% wartości umowy, o której mowa w § 2 ust. 1.
2. W przypadku zwłoki Wykonawcy w kompletnej dostawie przedmiotu umowy w terminie, o którym mowa w § 2 ust. 2, Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 0,5 % wartości umowy zł za każdy dzień zwłoki, w sumie jednak nie więcej niż 20% wartości umowy, o której mowa w § 2 ust. 1.
3. Zamawiający zapłaci Wykonawcy karę umowną z tytułu odstąpienia od umowy z przyczyn od niego zależnych w wysokości 20% wartości umowy, o której mowa w § 2 ust. 1, nie dotyczy sytuacji określonych w § 7 ust. 6.
4. Kary umowne stają się wymagalne następnego dnia po zajściu zdarzenia wywołującego obowiązek ich zapłaty.
5. Wykonawca wyraża zgodę na potrącenie wymagalnych kar umownych z wystawionych faktur.
6. Niezależnie od kar umownych, Zamawiający zastrzega sobie prawo dochodzenia odszkodowania na zasadach ogólnych do wysokości rzeczywiście poniesionej szkody.
7. Niezależnie od powyższego w razie obciążenia Zamawiającego obowiązkiem zapłaty kary administracyjnej, sądowej bądź kontraktowej, itp., ze względu na niewykonanie bądź nienależyte wykonanie zobowiązania przez Wykonawcę, Wykonawca zobowiązuje się przekazać Zamawiającemu sumę odpowiadającą kwocie nałożonej kary.
8. Niezależnie od zapisów powyższych Wykonawca na podstawie art. 473 kc, zobowiązuje się do naprawienia szkody powstałej w przypadku niewykonania bądź zaprzestania realizacji umowy z przyczyn nie dotyczących Zamawiającego – na skutek odstąpienia, rozwiązania bądź wypowiedzenia umowy przez Wykonawcę bądź Zamawiającego, także w przypadku wystąpienia po stronie Wykonawcy ważnej przyczyny uzasadniającej odstąpienie, rozwiązanie bądź wypowiedzenie i to niezależnie od rodzaju ważnej przyczyny dotyczącej Wykonawcy, a w szczególności w przypadku zaistnienia awarii sprzętu stosowanego do wykonania umowy

**§ 6**

* 1. Zamawiający wymaga wniesienia zabezpieczenia należytego wykonania umowy.
  2. Zabezpieczenie służy pokryciu roszczeń z tytułu niewykonania lub nienależytego wykonania umowy.
  3. Zabezpieczenie wnosi się przed zawarciem umowy.
  4. Zabezpieczenie może być wnoszone, według wyboru wykonawcy, w jednej lub w kilku następujących formach:

1) pieniądzu;

2) poręczeniach bankowych lub poręczeniach spółdzielczej kasy oszczędnościowo-kredytowej, z tym

że zobowiązanie kasy jest zawsze zobowiązaniem 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.

* 1. Zabezpieczenie wnoszone w pieniądzu wykonawca wpłaca przelewem na rachunek bankowy wskazany przez zamawiającego.
  2. W przypadku wniesienia wadium w pieniądzu wykonawca może wyrazić zgodę na zaliczenie kwoty wadium na poczet zabezpieczenia.
  3. Jeżeli zabezpieczenie wniesiono w pieniądzu, zamawiający przechowuje je na oprocentowanym rachunku bankowym. Zamawiający zwraca zabezpieczenie wniesione w pieniądzu z odsetkami wynikającymi z umowy rachunku bankowego, na którym było ono przechowywane, pomniejszone o koszt prowadzenia tego rachunku oraz prowizji bankowej za przelew pieniędzy na rachunek bankowy wykonawcy.
  4. W trakcie realizacji umowy wykonawca może dokonać zmiany formy zabezpieczenia na jedną lub kilka form, o których mowa w art. 450 ust. 1 ustawy z dnia 11.09.2019r. Prawo zamówień publicznych (Dz.U.z 2022r., poz. 1710).
  5. Zmiana formy zabezpieczenia jest dokonywana z zachowaniem ciągłości zabezpieczenia i bez zmniejszenia jego wysokości.
  6. Wysokość zabezpieczenia ustala się w stosunku procentowym do ceny całkowitej podanej w ofercie albo maksymalnej wartości nominalnej zobowiązania zamawiającego wynikającego z umowy, jeżeli w ofercie podano cenę jednostkową lub ceny jednostkowe.
  7. Zabezpieczenie ustala się w wysokości 5% ceny całkowitej podanej w ofercie albo maksymalnej wartości nominalnej zobowiązania zamawiającego wynikającego z umowy.

**§ 7**

* + 1. Zmiana treści lub uzupełnienie niniejszej umowy może nastąpić wyłącznie w granicach unormowania art. 455 ustawy Prawo zamówień publicznych za zgodą obu Stron i pod rygorem nieważności wymaga formy pisemnego aneksu, skutecznego po podpisaniu przez obie Strony.
    2. Zamawiający dopuszcza możliwość dokonania zmiany postanowień zawartej umowy w stosunku do treści oferty, w sytuacji gdy dotyczy ona zmiany:

nowe postanowienia są korzystne dla Zamawiającego,

Wykonawca zaproponuje nowszy technologicznie produkt spełniający parametry określone w opisie przedmiotu zamówienia,

zmiany stawki podatku VAT na towary sprzedawane w ramach rozstrzygniętego postępowania; zmiana ceny następuje nie wcześniej niż z dniem wejścia w życie aktu prawnego zmieniającego stawkę podatku VAT.

* + 1. Dostawca nie może zlecić wykonania przedmiotu umowy określonego w § 1 niniejszej umowy osobie trzeciej.
    2. Dostawca pod rygorem nieważności, nie może bez pisemnej zgody Zamawiającego zbyć wierzytelność z niniejszej umowy.
    3. W sprawach nieuregulowanych niniejszą Umową mają zastosowanie przepisy ustawy Prawo zamówień publicznych oraz przepisy Kodeksu Cywilnego, względnie inne regulacje prawne właściwe ze względu na przedmiot umowy.
    4. W razie zaistnienia istotnej zmiany okoliczności powodującej, że wykonanie umowy nie leży w interesie publicznym, czego nie można było przewidzieć w chwili zawarcia umowy, Zamawiający może odstąpić od umowy w terminie 30 dni od powzięcia wiadomości o tych okolicznościach. W przypadku takiego odstąpienia, nie stosuje się kar określonych w § 5 ust. 3 niniejszej umowy.

**§ 8**

1. W sprawach nieuregulowanych niniejszą umową stosuje się przepisy kodeksu cywilnego (Dz.U. z 2022r., poz. 1360) i ustawy z dn. 11.09.2019r. Prawo zamówień publicznych (Dz.U. z 2022r., poz.1710 z późn. zm.)
2. Umowę sporządzono w 2 egzemplarzach, po jednym dla każdej ze stron.
3. Ewentualne spory wynikłe z realizacji umowy strony poddają rozstrzygnięciu właściwemu rzeczowo sądowi w Opolu.

Załączniki do umowy:

* + - 1. Formularz ofertowy Wykonawcy z formularzem rzeczowym.

**ZAMAWIAJĄCY**  **WYKONAWCA**

9/ZP/RZPWE/2023 ZAŁĄCZNIK NR 5 DO SIWZ –

WZÓR OŚWIADCZENIA O PRZYNALEŻNOŚCI DO GRUPY KAPITAŁOWEJ

**OŚWIADCZENIE**

Skłądając ofertę w Postępowaniu o udzielenie zamówienia publicznego **na dostawę infrastruktury serwerowej na potrzeby RZPWE,**

działając w imieniu Wykonawcy:

*(podać nazwę i adres Wykonawcy)*

oświadczamy, że:

1) Wykonawca, którego reprezentuję nie przynależy do grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (Dz. U. z 2021 r., poz. 275) z innym wykonawcą, który złożył ofertę lub ofertę częściową w przedmiotowym postępowaniu\*,

2) Wykonawca, którego reprezentuję przynależy do grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (Dz. U. z 2021 r., poz. 275) wraz z wykonawcą, który złożył ofertę lub ofertę częściową w przedmiotowym postępowaniu tj. (podać nazwę i adres)\*:

*1/…………………………………………………………………………………….*

*2/ ………………………………………………………….……………………….*

**Uwaga:**

**- \*) niepotrzebne skreślić - należy wypełnić pkt 1) lub pkt 2)**

…………………………….. ………………………………

(miejscowość, data) (podpis wykonawcy)

ZAŁĄCZNIK NR 6 DO SWZ – WYKAZ DOSTAW

9/ZP/RZPWE/2023

**Wykonawca:**

……………………………………

……………………………………

……………………………………

*(pełna nazwa/firma, adres)*

Dot. zamówienia na Przedmiotem zamówienia jest dostawa **infrastruktury serwerowej na potrzeby RZPWE**

**WYKAZ DOSTAW**

**Składa tylko wykonawca wezwany na podstawie art. 274 ust. 1 ustawy prawo zamówień publicznych**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| L.p. | Przedmiot zamówienia | Cena (wartość wraz z podatkiem VAT)  w PLN | Data wykonania | | Podmiot, na rzecz którego dostawa została wykonana lub jest wykonywana |
|
| Początek (data) | Zakończenie  (data) |
|  |  |  |  |  |  |

W załączeniu dowody określające czy usługi wskazane w wykazie zostały wykonane lub są wykonywane należycie, przy czym dowodami, o których mowa, są referencje bądź inne dokumenty sporządzone przez podmiot na rzecz którego usługi zostały wykonane, a w przypadku świadczeń ciągłych są wykonywane, a jeżeli Wykonawca z przyczyn niezależnych od niego nie jest w stanie uzyskać tych dokumentów – oświadczenie Wykonawcy; w przypadku świadczeń ciągłych nadal wykonywanych referencje bądź inne dokumenty potwierdzające ich należyte wykonywanie powinny być wystawione w okresie ostatnich 3 miesięcy.

……….……*,* dnia ………….……. r.

………………………….........................................

*Podpis Wykonawcy lub osób uprawnionych do składania oświadczeń woli w imieniu Wykonawcy*

**Załącznik Nr 7 do SWZ – zobowiązanie innego podmiotu**

9/ZP/RZPWE/2023

…………………………………………………..

*(pieczęć firmowa/imię i nazwisko)*

**ZOBOWIĄZANIE DO UDOSTĘPNIENIA NIEZBĘDNYCH ZASOBÓW INNYCH PODMIOTÓW**

**NA OKRES KORZYSTANIA Z NICH PRZY WYKONYWANIU ZAMÓWIENIA**

W celu realizacji zadania, którego przedmiotem jest:

**„D**ostawa **infrastruktury serwerowej na potrzeby RZPWE**”

zobowiązuję/emy się do udostępnienia Wykonawcy następującego zasobu:

……………………………………………………………………………………………………………

……………………………………………………………………………………………………………

Oświadczamy, iż w przypadku zawarcia umowy między Zamawiającym a Wykonawcą w celu realizacji ww. zadania będziemy odpowiadać solidarnie z Wykonawcą za szkodę Zamawiającego niezależnie od tego, czy szkoda powstała wskutek nieudostępnienia ww. zasobów, i niezależnie od tego, czy za nieudostępnienie zasobów ponosimy winę. Tym samym godzimy się na takie rozszerzenie odpowiedzialności przewidzianej w art. 120 ustawy z dnia 11 września 2019r. Prawo zamówień publicznych.

opis udostępnianego zasobu:

……………………………………………………………………………………………………………………………………………………………………………………………………………………………………

………… , dnia

…………………………………………

pieczęć i podpis podmiotu zobowiązującego się do oddania zasobów

1. *W przypadku Wykonawców występujących wspólnie należy wpisać dane każdego z tych Wykonawców, a nadto wskazać tego z nich, który reprezentuje Wykonawców w Postępowaniu (tzw. Lider konsorcjum, pełnomocnik Wykonawców wspólnie ubiegających się o udzielenie zamówienia* [↑](#footnote-ref-1)
2. *podać mającą zastosowanie podstawę wykluczenia spośród* *wymienionych w art. 108 ust. 1 pkt 1, 2, 5 lub 6 ustawy Pzp. Jeśli nie dotyczy należy wykreślić całe zdanie.*  [↑](#footnote-ref-2)